

Federally Facilitated Marketplace (FFM)

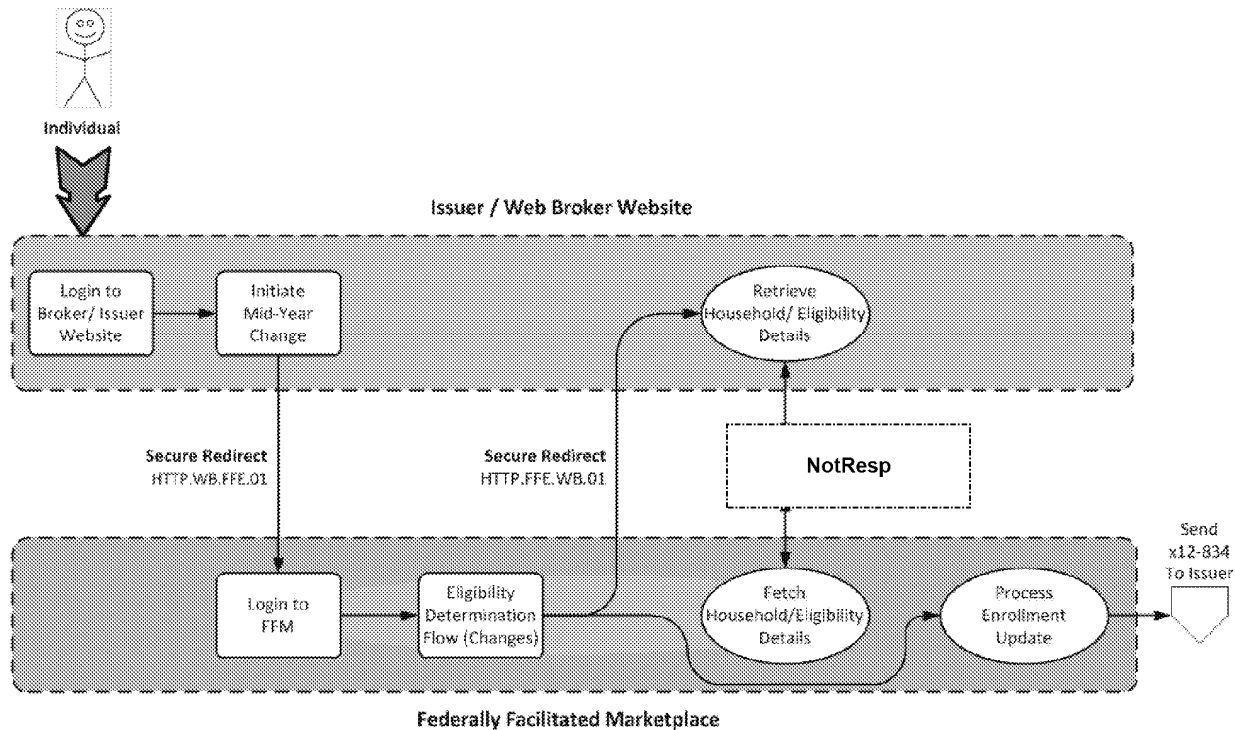
- b. FFM will generate x12-834 enrollment change transaction and transmit to the Issuer of the policy
- 24) For any existing enrollment groups from which all members have been removed
 - a. FFM will process a QHP disenrollment from the QHP (policy level)
 - b. FFM will generate an x12-834 cancellation/termination transaction for the QHP and transmit to the Issuer of the policy
- 25) For any existing enrollment groups for which the plan has been changed.
 - a. FFM will process a QHP disenrollment from the old QHP (policy level)
 - b. FFM will generate an x12-834 cancellation/termination transaction for the old QHP and transmit to the Issuer of the policy
 - c. FFM will process a QHP Initial Enrollment from the new QHP
 - d. FFM will generate an x12-834 initial enrollment transaction for the new QHP and transmit to the Issuer of the policy
- 26) For any new enrollment groups
 - a. FFM will process QHP enrollment into the new QHP
 - b. FFM will generate an x12-834 initial enrollment transaction for new QHP and transmit to Issuer
- 27) In all the above cases where FFM generates an x12-834 transaction
 - Note 1: The Agent/Broker information sent by the partner website as part of the enrollment transaction will be listed as the agent/broker on the x12-834 transaction for compensation purposes
 - Note 2: If a consumer returns to the FFM directly and performs their enrollment on the FFM, none of the partner websites through which they had previously visited the FFM will be included on the x12-834 transaction

Federally Facilitated Marketplace (FFM)

B.6 Scenario #4 - Reporting changes not impacting eligibility

Figure 8 - Reporting Changes not Impacting Eligibility illustrates the interactions between the Partner Website and FFM under this scenario.

Figure 8 - Reporting Changes not Impacting Eligibility



B.6.1 Scenario Overview

In this scenario, a consumer with a household previously enrolled in a QHP with APTC/CSR returns to report changes in their household income or other demographic information. The changes do not impact their eligibility for APTC/CSR and the information update is processed by the FFM and conveyed to the Issuer.

B.6.2 Sequence of Activities

On Partner Website

- 1) Consumer and/or members of their household are enrolled in a QHP.
- 2) Consumer may or may not have an account on the partner website. If the consumer has an account, they would login using their credentials for the partner website. Otherwise, they would create a new account with the partner website and be assigned a Partner Assigned Consumer ID.
- 3) Consumer indicates intent to enter changes to their demographic/household information for an FFM enrollment
- 4) Partner website transfers consumer to the FFM website. Information passed to the FFM includes:
 - a. Information Exchange System ID
 - b. Partner Assigned Consumer ID
 - c. FFE Assigned Consumer ID (If available)

Federally Facilitated Marketplace (FFM)

- d. Return URL
- e. Keep-alive URL

On FFM

- 5) Consumer already has an account with the FFM and will login using their FFM credentials
- 6) Consumer reviews their account/application details on the FFM and enters changes where applicable. Changes could include:
 - a. Changes in household income
 - b. Residency changes
 - c. Other Demographic changes
- 7) FFM verifies information entered by consumer with internal and external data sources
- 8) FFM determines eligibility for Medicaid, CHIP and APTC/CSR and determines no change in eligibility for any member of the household
- 9) FFM Updates the QHP enrollment with the new information
- 10) If applicable, FFM generates an x12-834 enrollment change transaction and transmits to Issuer(s) of QHP(s) in which the household is enrolled
- 11) FFM transfers consumer to the Return URL provided by partner website and passes back the Partner Assigned Consumer ID and FFE Assigned Consumer ID

On Partner Website

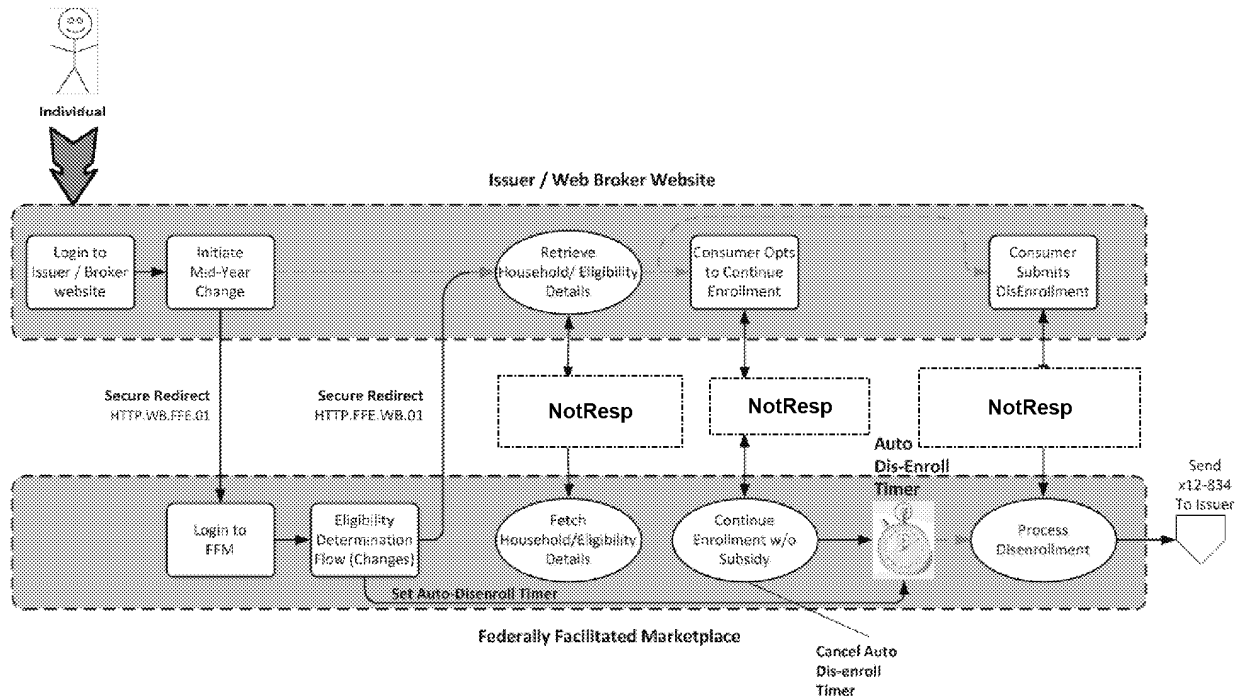
- 12) Partner website invokes the FFM Household/Eligibility web service using the FFE Assigned Consumer ID
- 13) Partner website receives following information from the FFM Household/Eligibility web service
 - a. Application Contact Information
 - b. List of members and demographic Information required for plan shopping and enrollment. This will only include members requesting health insurance coverage (including those referred to Medicaid/CHIP)
 - c. Eligibility information for each member of the household
 - i. Eligibility for Medicaid/CHIP
 - ii. Eligibility for APTC including Maximum Monthly APTC
 - iii. Eligibility for CSR and CSR Level
 - iv. Eligibility for Enrollment Period - Initial Enrollment Period (IEP), Annual Enrollment Period (AEP) or Special Enrollment Period (SEP).
 - v. Flag indicating if a member has gained or lost eligibility for QHP and or APTC/CSR
 - d. Enrollment status of members of the household.
- 14) Partner website confirms completion of change transaction

Federally Facilitated Marketplace (FFM)

B.7 Scenario #5 - Reporting changes leading to Disenrollment

Figure 9 - Reporting Changes Leading to Disenrollment illustrates the interactions between the Partner Website and FFM under this scenario.

Figure 9 - Reporting Changes Leading to Disenrollment



B.7.1 Scenario Overview

In this scenario, a consumer with a household previously enrolled in a QHP with APTC/CSR returns to report changes in their household income or other demographic information. The changes result in a loss of eligibility for QHP or APTC/CSR for one or more members (including cases where members of the household become eligible for Medicaid or CHIP). In this case the members who lose APTC/CSR will be subject to automatic disenrollment unless the consumer indicates their intent to continue enrollment in the QHP without APTC and CSR.

B.7.2 Sequence of Activities

On Partner Website

- 1) Consumer and/or members of their household are enrolled in a QHP.
- 2) Consumer may or may not have an account on the partner website. If they do not have an account on the partner website, they would create one. Otherwise, they would login using their credentials for the partner website.
- 3) Consumer indicates intent to enter changes to their demographic/household information for an FFM enrollment
- 4) Partner website transfers consumer to the FFM website. Information passed to the FFM includes:
 - a. Information Exchange System ID
 - b. Partner Assigned Consumer ID
 - c. FFE Assigned Consumer ID

Federally Facilitated Marketplace (FFM)

- d. Return URL
- e. Keep-alive URL

On FFM

- 5) Consumer already has an account with the FFM and will login using their FFM credentials
- 6) Consumer reviews their account/application details on the FFM and enters changes where applicable. Changes could include:
 - a. Addition or removal of household members
 - b. Changes in household income
 - c. Changes in availability of other health coverage (employer sponsored or other public programs)
 - d. Residency changes
 - e. Other Demographic changes
- 7) FFM verifies information entered by consumer with internal and external data sources
- 8) If FFM determines that one or more members of the household have lost eligibility QHP (based on eligibility criteria for QHP - Citizenship/Lawful presence, Residency or Incarceration status)
 - a. If not all members of an enrollment group lose eligibility for QHP
 - i. FFM will process a QHP enrollment change transaction to remove members that lost QHP eligibility
 - ii. FFM will generate an x12-834 enrollment change transaction and transmit to the Issuer of the policy
 - b. If all members of an enrollment group lose eligibility for QHP
 - i. FFM will process QHP disenrollment from QHP (policy level)
 - ii. FFM will generate an x12-834 cancellation/termination transaction for the QHP and transmit to the Issuer of the policy
- 9) If FFM determines that one or more members of the household have lost eligibility for APTC and CSR (due to gaining eligibility for Medicaid/CHIP or other eligibility criteria)
 - a. FFM will initiate an auto disenrollment timer for the members that lost APTC and CSR eligibility.
 - b. FFM will notify the consumer on the impending auto-disenrollment of members that lost eligibility. The notice will offer the consumer the following choices:
 - i. Consumer can indicate their intent to continue QHP enrollment for the members without APTC and CSR. This will cancel the auto disenrollment process.
 - ii. Consumer can voluntarily disenroll the members
 - iii. Take no action - Members will be automatically disenrolled by the FFM on the date indicated in the notice.
- 15) FFM transfers consumer to the Return URL provided by partner website and passes back the Partner Assigned Consumer ID and FFE Assigned Consumer ID
- 10)

On Partner Website

- 11) Partner website invokes the FFM Household/Eligibility web service using the FFE Assigned Consumer ID

Federally Facilitated Marketplace (FFM)

- 12) Partner website receives following information from the FFM Household/Eligibility web service
 - a. Application Contact Information
 - b. List of members and demographic Information required for plan shopping and enrollment. This will only include members requesting health insurance coverage (including those referred to Medicaid/CHIP)
 - c. Eligibility information for each member of the household
 - i. Eligibility for Medicaid/CHIP
 - ii. Eligibility for APTC including Maximum Monthly APTC
 - iii. Eligibility for CSR and CSR Level
 - iv. Eligibility for Enrollment Period - Initial Enrollment Period (IEP), Annual Enrollment Period (AEP) or Special Enrollment Period (SEP).
 - v. Flag indicating if a member has gained or lost eligibility for QHP and or APTC/CSR and the date for pending auto disenrollment (if applicable)
 - d. Enrollment status of members of the household.
- 13) Consumer is offered the opportunity to remove members who lost eligibility for APTC/CSR, from their QHP enrollments
 - a. If consumer chooses this option, the partner website will invoke the FFM Enrollment web service with information on the members that the consumer chose to remove from QHP enrollment.
- 14) Consumer is offered the opportunity to indicate their intent to continue QHP enrollments without APTC/CSR for members that lost eligibility
 - a. If consumer chooses this option, the partner website will invoke the FFM Enrollment web service with information on the members that the consumer chose to continue enrollment despite loss of APTC and CSR. FFM will cancel the Auto disenrollment timer.

On FFM (No consumer interaction)

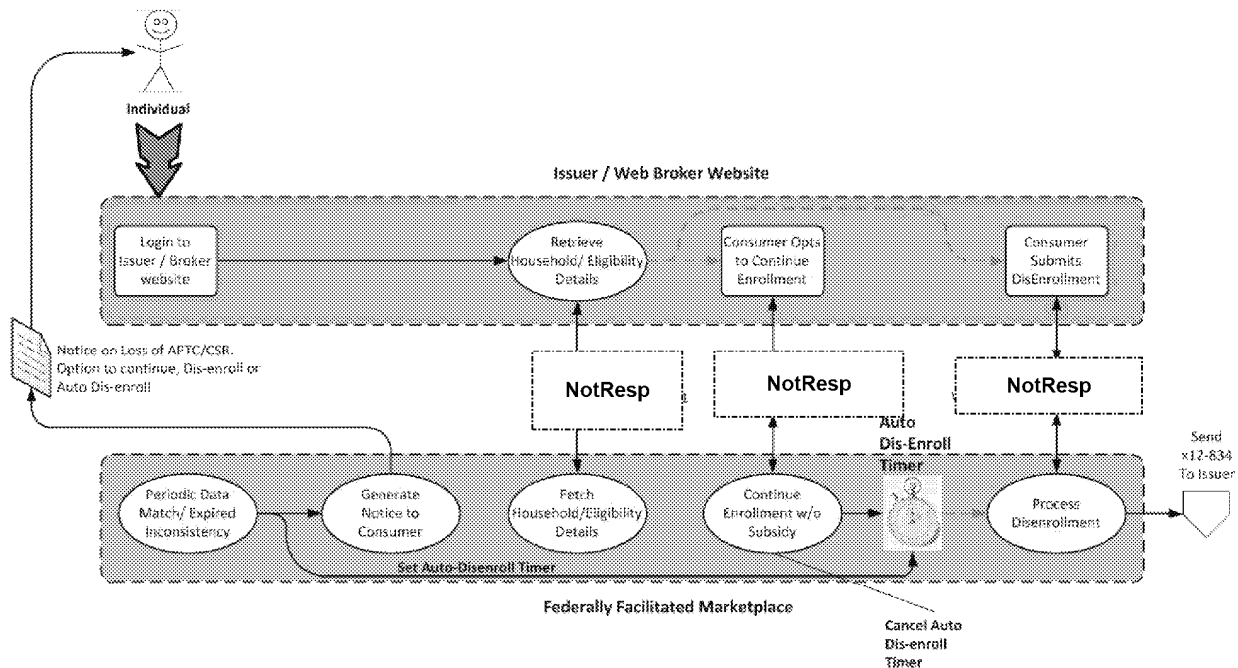
- 15) If the consumer chose to remove one or more members that lost eligibility for APTC/CSR from QHP enrollment
 - a. If not all members in an enrollment group are being removed
 - i. FFM will process a QHP enrollment change request to remove members
 - ii. FFM will generate an x12-834 enrollment change transaction and transmit to the Issuer of the policy
 - b. If all members in an enrollment group are being removed
 - i. FFM will process a disenrollment request (policy level)
 - ii. FFM will generate an x12-834 cancellation/termination transaction and transmit to the Issuer of the policy

Federally Facilitated Marketplace (FFM)

B.8 Scenario #6 - FFM Initiated Disenrollment

Figure 10 - FFM Initiated Disenrollment illustrates the interactions between the Partner Website and FFM under this scenario.

Figure 10 - FFM Initiated Disenrollment



B.8.1 Scenario Overview

In this scenario, the FFM re-determines eligibility for members receiving APTC/CSR as part of a periodic data match or on expiry of the period of reasonable opportunity to resolve verification inconsistencies. FFM will start a timer for automatic disenrollment of members who lost eligibility for APTC and CSR and notify the consumer accordingly. As part of the notice, the consumer will be presented the following options:

- Consumer can indicate their intent to continue QHP enrollment for the members without APTC and CSR. This will cancel the auto disenrollment process.
- Consumer can voluntarily Disenroll the members
- Take no action - Members will be automatically disenrolled by the FFM on the date indicated in the notice.

B.8.2 Sequence of Activities

On FFM (No Consumer Interaction)

- 1) Consumer and/or member of their household are enrolled in QHP(s) on the exchange
- 2) FFM determines loss of eligibility for APTC/CSR for one or more members of the household due to one of following reasons:
 - Periodic data match resulting in ineligibility
 - Expiry of period of reasonable opportunity for resolving verification inconsistencies

Federally Facilitated Marketplace (FFM)

- 3) FFM notifies consumer on loss of eligibility for APTC/CSR and offers them the following options:
 - Consumer can indicate their intent to continue QHP enrollment for the members without APTC and CSR. This will cancel the auto disenrollment process.
 - Consumer can voluntarily Disenroll the members
 - Take no action - Members will be automatically disenrolled by the FFM on the date indicated in the notice.

On Partner Website

- 4) Consumer already has an account with the partner website and will login using their credentials for the partner website
- 5) Partner website invokes the FFM Household/Eligibility web service using the FFE Assigned Consumer ID
- 6) Partner website receives following information from the FFM Household/Eligibility web service
 - a. Application Contact Information
 - b. List of members and demographic Information required for plan shopping and enrollment. This will only include members requesting health insurance coverage (including those referred to Medicaid/CHIP)
 - c. Eligibility information for each member of the household
 - i. Eligibility for Medicaid/CHIP
 - ii. Eligibility for APTC including Maximum Monthly APTC
 - iii. Eligibility for CSR and CSR Level
 - iv. Eligibility for Enrollment Period - Initial Enrollment Period (IEP), Annual Enrollment Period (AEP) or Special Enrollment Period (SEP).
 - v. Flag indicating if a member has gained or lost eligibility for QHP and or APTC/CSR and the date for pending auto disenrollment (if applicable)
 - d. Enrollment status of members of the household.
- 7) Consumer is offered the opportunity to remove members who lost eligibility for APTC/CSR, from their QHP enrollments
 - a. If consumer chooses this option, the partner website invokes the FFM Enrollment web service with information on members to be removed from QHP enrollment.
- 8) Consumer is offered the opportunity to indicate their intent to continue QHP enrollments without APTC/CSR for members that lost eligibility
 - a. If consumer chooses this option, the partner website invokes FFM Enrollment web service with information on the members that the consumer chose to continue enrollment despite loss of APTC and CSR. FFM will cancel the Auto disenrollment timer.

On FFM (No consumer interaction)

- 9) If the consumer chose to remove one or more members that lost eligibility for APTC/CSR from QHP enrollment
 - a. If not all members in an enrollment group are being removed
 - iii. FFM will process the QHP enrollment change transaction to remove members

Federally Facilitated Marketplace (FFM)

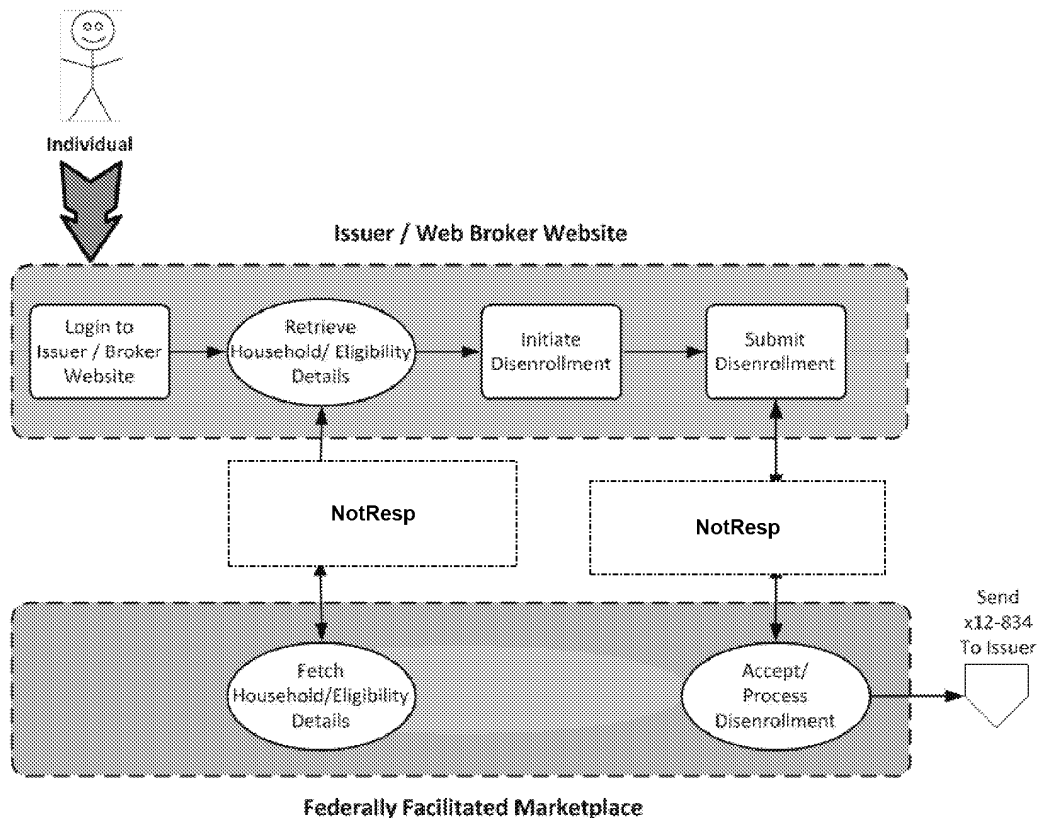
- iv. FFM will generate an x12-834 enrollment change transaction and transmit to the Issuer of the policy
- b. If all members in an enrollment group are being removed
 - v. FFM will process a disenrollment request (policy level)
 - vi. FFM will generate an x12-834 cancellation/termination transaction and transmit to the Issuer of the policy

Federally Facilitated Marketplace (FFM)

B.9 Scenario #7 - Voluntary Disenrollment by Consumer

Figure 11 - Voluntary Disenrollment illustrates the interactions between the Partner Website and FFM under this scenario.

Figure 11 - Voluntary Disenrollment



B.9.1 Scenario Overview

In this scenario, the consumer wishes to voluntarily disenroll one or more members of their household from QHP Enrollment(s). The consumer returns to the Partner Website and indicates their intent to disenroll. The partner website will capture the disenrollment request and send it to the FFM.

B.9.2 Sequence of Activities

On Partner Website

- 1) Consumer and/or members of their household are enrolled in a QHP on the exchange
- 2) Consumer already has an account with the partner website and will login using their credentials for the partner website
- 3) Consumer indicates intent to disenroll one or members of their household from a QHP
- 4) Consumer submits disenrollment request
- 5) Partner website invokes the FFM Enrollment Web service to perform the disenrollment request

Federally Facilitated Marketplace (FFM)

On FFM (No Consumer Interaction)

- 6) If the consumer chose to remove one or more members from QHP enrollment(s)
 - a. If not all members in an enrollment group are being removed
 - i. FFM will process a QHP enrollment change request to remove members
 - ii. FFM will generate an x12-834 enrollment change transaction and transmit to the Issuer of the policy
 - b. If all members in an enrollment group are being removed
 - i. FFM will process a disenrollment request (policy level)
 - ii. FFM will generate an x12-834 cancellation/termination transaction and transmit to the Issuer of the policy

HHS Notice of Proposed Rulemaking: Establishment of Exchanges and Qualified Health Plans

Clarifications and suggestions contained in the preamble are noted in *italics*.
Requests for comment are noted in *blue italics*.

Section	Summary	Questions/Comments
Part 155—Exchange Establishment Standards and Other Related Standards Under the Affordable Care Act		
Subpart A—General Provisions		
§155.20-Definitions	<p>Advance payments of the premium tax credit means payment of the tax credits provided on an advance basis to an eligible individual of a QHP through an Exchange.</p> <p>Agent or broker means a person or entity licensed by the State as an agent, broker or insurance producer.</p> <p>Annual open enrollment period means the period each year during which a qualified individual may enroll or change coverage in a QHP through the Exchange.</p> <p><u>Applicant means:</u></p> <p>(1) An individual who is seeking eligibility through an application to the Exchange for at least one of the following:</p> <p>(i) Enrollment in a QHP through the Exchange;</p> <p>(ii) Advance payments of the premium tax credit and cost-sharing reductions; or</p> <p>(iii) Medicaid, CHIP, and the BHP, if applicable.</p> <p>(2) An employer or employee seeking eligibility for enrollment in a QHP through the SHOP, where applicable.</p> <p>Benefit year means a calendar year for which a health plan provides coverage for health benefits.</p> <p>Code means the Internal Revenue Code of 1986.</p> <p>Cost sharing means any expenditure required by or on behalf of an enrollee with respect to essential health benefits; such term includes deductibles, coinsurance, copayments, or similar charges, but excludes premiums, balance billing amounts for non-network providers, and spending for non-covered services.</p> <p>Cost-sharing reductions means reductions in cost sharing for an eligible individual enrolled in a silver level plan in the Exchange or for an individual who is an Indian who is enrolled in a QHP in the Exchange.</p> <p>Eligible employer-sponsored plan means, with respect to any employee, a group health plan or group health insurance coverage offered by an employer to the employee which is –</p> <p>(1) A governmental plan; or</p> <p>(2) Any other plan or coverage offered in the small or large group market within a State.</p> <p>Such term shall include a grandfathered health plan offered in the group market.</p>	

Obtained via FOIA by Judicial Watch, Inc.

Section	Summary	Questions/Comments
	<p>Employer has the meaning given to the term in section 2791 of the PHS Act, except that such term must include employers with one or more employees. All persons treated as a single employer under subsection (b), (c), (m), or (o) of section 414 of the Code must be treated as one employer.</p> <p><i>The preamble states that "We note that coverage for only a sole proprietor, certain owners of S corporations, and certain relatives of each of the above would not constitute a group health plan under ERISA section 732(a)... and would not be entitled to purchase in the small group market under Federal law."</i></p>	
	Employer contributions means any financial contributions towards an employer sponsored health plan, or other eligible employer-sponsored benefit made by the employer including those made by salary reduction agreement that is excluded from gross income.	
	Enrollee means a qualified individual or qualified employee enrolled in a QHP.	
	Exchange means a governmental agency or non-profit entity that meets the applicable requirements of this part and makes QHPs available to qualified individuals and qualified employers. Unless otherwise identified, this term refers to State Exchanges, regional Exchanges, subsidiary Exchanges, and a Federally-facilitated Exchange.	
	Exchange service area means the area in which the Exchange is certified to operate.	
	Health plan means health insurance coverage and a group health plan. It does not include a group health plan or multiple employer welfare arrangement to the extent the plan or arrangement is not subject to State insurance regulation under section 514 of the Employee Retirement Income Security Act of 1974.	
	<i>The preamble notes that PPACA specified that a health plan does not include a group health plan or MEWA to the extent that it is not subject to state regulation, but that ERISA allows state regulation of MEWAs to the extent that such regulation does not conflict with ERISA. It requests comment on this inconsistency, as well as whether or not Toft-Hartley plans and church plans can participate in the Exchange.</i>	
	Individual market means the market for health insurance coverage offered to individuals other than in connection with a group health plan.	
	Initial enrollment period means the period during which a qualified individual may enroll in coverage through the Exchange for coverage during the 2014 benefit year.	
	Large employer means, in connection with a group health plan with respect to a calendar year and a plan year, an employer who employed an average of at least 101 employees on business days during the preceding calendar year and who employs at least 1 employee on the first day of the plan year. In the case of plan years beginning before January 1, 2016, a State may elect to define large employer by substituting "51 employees" for "101 employees."	
	Navigator means a private or public entity or individual that is qualified, and licensed, if appropriate, to engage in the activities and meet the requirements described in §155.210.	
	Plain language means language that the intended audience, including individuals with limited English proficiency, can readily understand and use because that language is concise, well organized, and follows other best practices of plain language writing.	
	Plan year means a consecutive 12 month period during which a health plan provides coverage for health benefits. A plan year may be a calendar year or otherwise.	

Obtained via FOIA by Judicial Watch, Inc.

Section	Summary	Questions/Comments
	<p>Qualified employee means an individual employed by a qualified employer who has been offered health insurance coverage by such qualified employer through the SHOP.</p> <p>Qualified employer means a small employer that elects to make, at a minimum, all fulltime employees of such employer eligible for one or more QHPs in the small group market offered through a SHOP. Beginning in 2017, if a State allows large employers to purchase coverage through the SHOP, the term "qualified employer" shall include a large employer that elects to make all full-time employees of such employer eligible for one or more QHPs in the large group market offered through the SHOP.</p> <p>Qualified health plan or QHP means a health plan that has in effect a certification that it meets the standards described in subpart C of part 156 issued or recognized by each Exchange through which such plan is offered pursuant to the process described in subpart K of part 155.</p> <p>Qualified health plan issuer or QHP issuer means a health insurance issuer that offers, pursuant to a certification from an Exchange, a QHP.</p> <p>Qualified individual means, with respect to an Exchange, an individual who has been determined eligible to enroll in a QHP in the individual market offered through the Exchange.</p> <p>SHOP means a Small Business Health Options Program operated by an Exchange through which a qualified employer can provide its employees and their dependents with access to one or more QHPs.</p> <p>Small employer means, in connection with a group health plan with respect to a calendar year and a plan year, an employer who employed an average of at least 1 but not more than 100 employees on business days during the preceding calendar year and who employs at least 1 employee on the first day of the plan year. In the case of plan years beginning before January 1, 2016, a State may elect to define small employer by substituting "50 employees" for "100 employees."</p> <p>Small group market means the health insurance market under which individuals obtain health insurance coverage (directly or through any arrangement) on behalf of themselves (and their dependents) through a group health plan maintained by a small employer (as defined in this section).</p> <p>Special enrollment period means a period during which a qualified individual or enrollee who experiences certain qualifying events may enroll in, or change enrollment in, a QHP through the Exchange outside of the initial and annual open enrollment periods.</p> <p>State means each of the 50 States and the District of Columbia.</p>	
Subpart B—General Standards Related to the Establishment of an Exchange by a State		
§155.100-Establishment of a State Exchange	Each state may establish an Exchange that facilitates the purchase of QHPs and provides for the establishment of a SHOP. Exchanges may be governmental agencies (either existing executive branch agencies or independent public agencies) or non-profit entities established by the state.	
§155.105-Approval of a State Exchange	Each State Exchange must be approved by the Secretary of HHS no later than January 1, 2013 in order to begin offering QHPs on January 1, 2014. The regulation interprets the term "fully operational" to mean that an Exchange is capable of beginning operations by October 1, 2013 to support the initial open enrollment period in <u>§155.410</u> .	

Section	Summary	Questions/Comments
	<p>Approval standards:</p> <ul style="list-style-type: none"> • Exchanges must be established consistent with the requirements of the regulation. • Exchanges must be capable of carrying out required functions: <ul style="list-style-type: none"> ○ Minimum Exchange functions ○ Enrollment functions ○ SHOP functions ○ QHP certification functions • Exchanges must be capable of complying with information requirements with respect to subsidies, in accordance with rules to be issued later. • Exchanges must agree to perform its duties related to the transitional reinsurance program and enter into a contract with one or more reinsurance entities to carry it out. • The entire geographic area of the state must be covered by one or more Exchanges. <p>Approval process:</p> <ul style="list-style-type: none"> • States must submit an Exchange Plan to HHS, which will detail how it will meet each of the approval standards above and include any agreements the State has entered into to carry out Exchange responsibilities. HHS will issue a template outlining the required components of the Exchange Plan. • HHS will conduct an operational readiness assessment, which will be coordinated with the ongoing grants monitoring process. Additional guidance on these assessments will be issued at a later date. • Each State must receive written approval or conditional approval of its Exchange Plan in order to be approved to operate. The approved Exchange Plan will constitute an agreement between the State and HHS. • Because work will be ongoing systems development and contracting work that extends past January 1, 2013, HHS will issue conditional approvals to states that are making progress and will have an Exchange that is operational by January 1, 2014, even if it cannot demonstrate complete readiness on January 1, 2013. • HHS is considering establishing a review process for Exchange Plans that is similar to Medicaid and CHIP for which there would be 90 days to review the plan and approve, deny or request comment on the plan. <i>HHS is seeking comments on this review process.</i> <p>Changes to the Exchange Plan</p> <ul style="list-style-type: none"> • A State must notify HHS before making significant changes to its Exchange Plan and must receive written approval of these changes. • <i>HHS is considering utilizing the state plan amendment process that is used for Medicaid and CHIP and is seeking comments on the subject.</i> 	
<p>\$155.106-Election to operate an Exchange after 2014</p>	<p>A state that does not have in place an approved or conditionally approved Exchange Plan and operational readiness assessment by January 1, 2013 may seek initial approval to operate an Exchange by following the process and meeting the standards outlined in <u>\$155.105</u> above. The Exchange Plan must be approved or conditionally approved prior to January 1 of the year before the first coverage sold through the Exchange would become effective. States must also work with</p>	

Section	Summary	Questions/Comments
	<p>HHS to develop a transition plan.</p> <p>A State-operated Exchange may cease operations and elect have the Federal government establish an Exchange in the State. The State must provide at least 12 months' notice to HHS prior to ceasing operations and work with HHS to develop and execute a transition plan.</p>	
<p>\$155.110-Entities eligible to carry out Exchange functions</p>	<p>Entities with whom the Exchange contracts to carry out one or more responsibilities must:</p> <ul style="list-style-type: none"> • Be incorporated under and subject to the laws of one or more States; • Have demonstrated experience on a State or regional basis in the individual and small group markets and in benefits coverage; and • Not be a health insurance issuer or be treated as a health insurance issuer. <p>The regulation specifically identifies State Medicaid agencies as entities eligible to contract with the Exchange.</p> <p><i>HHS is seeking comments on the extent to which it should impose conflict of interest requirements on contacted entities.</i></p> <p><i>HHS is seeking comments on how to construct a model for State-Federal partnership for carrying out Exchange responsibilities consistent with §1311(f)(3) and (d)(5) of the ACA.</i></p> <p>The Exchange must remain responsible for meeting all Federal requirements related to contracted functions.</p> <p>If the Exchange is established as an independent State agency or as a not-for-profit entity, it must have a clearly-defined governing board and operate under a formal, publicly-adopted operating charter or by-laws. The board must hold regular public meetings. A majority of the board must be free from conflicts of interest. A conflict of interest is defined as representing health insurers, agents, brokers, or other individuals licensed to sell health insurance. States may adopt more stringent or specific conflict of interest policies.</p> <p><i>HHS is seeking comments on the extent to which these categories of representatives with potential conflicts of interest should be specified and on the types of representatives who have potential conflicts of interest.</i></p> <p>A majority of board members must also have relevant experience in health benefits administration, health care finance, health plan purchasing, health care delivery system administration, public health, or health policy issues related to the small group and individual markets and the uninsured.</p> <p><i>HHS is seeking comment on the types of representatives that should be on Exchange board to ensure that consumer interests are well-represented and that the Exchange board has the necessary technical expertise.</i></p> <p>States may establish a separate governance structure for the SHOP Exchange. If it chooses to do so, the two governance entities must coordinate and share data. If a State opts to use a single governance structure for both, it must have adequate resources to assist individuals and small</p>	

Section	Summary	Questions/Comments
	<p>employers.</p> <p>HHS will periodically review the governance of Exchanges.</p> <p><i>HHS is requesting comment on the recommended frequency of reviews.</i></p>	
<p>§155.120-Non-interference with federal law and non-discrimination standards</p>	<p>Exchange rules may not conflict with, or prevent the application of, relevant HHS regulations. Nothing in the regulation shall be construed to preempt any state law that does not prevent the application of title I of PPACA.</p> <p>Exchanges may not be operated in any way that discriminates on the basis of race, color, national origin, disability, age, sex, gender identity, or sexual orientation.</p>	
<p>§155.130-Stakeholder consultation</p>	<p>Exchanges must consult, on an ongoing basis, with the following categories of stakeholders:</p> <ul style="list-style-type: none"> • Educated health care consumers; • Individuals and entities with experience facilitating enrollment in health coverage; • Advocates for enrolling hard-to-reach populations, including those with mental health or substance abuse disorders (HHS also encourages consultation with advocates for individuals with disabilities and those who need culturally and linguistically appropriate services); • Small businesses and self-employed individuals; • State Medicaid and CHIP agencies (HHS also encourages consultation with Medicaid and CHIP beneficiaries); • Federally-recognized tribes within the Exchange's geographic area; • Public health experts; • Health care providers; • Large employers; • Health insurance issuers; and • Agents and brokers. <p><i>HHS will provide additional guidance to tribes and States on consultation.</i></p>	
<p>§155.140-Establishment of a regional Exchange or subsidiary Exchange</p>	<p>A State may participate in a regional Exchange that spans two or more States, which need not be contiguous. The regional Exchange would submit a single Exchange plan, which will be evaluated and approved using the criteria outlined in §155.105.</p> <p>HHS encourages States to consider the following:</p> <ul style="list-style-type: none"> • How a regional Exchange would meet the Exchange requirements; • How a regional Exchange would cooperate with State Departments of Insurance; • How to provide a consistent level of consumer protections across the States; • Procedures for State withdrawal from the Exchange; and • Financing of the Exchange. <p>A State may establish multiple subsidiary Exchanges if each serves a distinct geographic area that is at least as large as a geographic rating area described in PHSA §2701(a).</p> <p><i>HHS is requesting comments regarding operational or policy concerns raised by subsidiary Exchanges that cover areas across State lines and the extent to which more</i></p>	

Obtained via FOIA by Judicial Watch, Inc.

Section	Summary	Questions/Comments
	<i>flexibility in the structure of subsidiary Exchanges should be allowed.</i>	
§155.150-Transition process for existing State health insurance Exchanges	<p>Regional and subsidiary Exchanges must meet all requirements for Exchanges, and perform the functions for a SHOP outlined in the regulations. If a regional or subsidiary Exchange maintains separate governance structures for individual and SHOP Exchanges, the geographic service areas must be identical.</p> <p>Unless determined to be non-compliant, an Exchange is presumed to be in compliance if:</p> <ul style="list-style-type: none"> • The Exchange was operating prior to January 1, 2010; and • The State has insured a percentage of its population that is not less than the percentage of the population projected to be covered nationally under PPACA when fully implemented. <p><i>HHS is requesting comments regarding how to make this determination. They are proposing to use the year 2016 as the benchmark for full implementation, and are considering different projections of national coverage in this year: CMS Actuary (93.6%) and CBO (95%).</i></p>	
§155.160-Financial support for continued operations	<p>Any state that is currently operating an Exchange that is presumed to be compliant must work with HHS to identify areas of non-compliance.</p> <p>A State must develop a plan to ensure its Exchange has sufficient funding to support ongoing operations beginning January 1, 2015.</p> <p>States may fund exchanges through user fees or assessments or by other methods, so long as those methods do not violate other State or Federal laws.</p> <p>Any user fees on health insurance issuers must be announced in advance of the plan year.</p> <p><i>HHS is requesting comments on whether it should otherwise limit how and when user fees may be assessed and whether they should be assessed on an annual basis.</i></p>	
Subpart C—General Functions of an Exchange		
§155.200-Functions of an Exchange	<p>An Exchange must perform the required functions set forth in <u>subparts E</u> (individual enrollment in QHPs), <u>H</u> (SHOP), and <u>K</u> (QHP certification).</p> <p>An Exchange must grant certifications of exemption from the individual mandate. Standards and eligibility criteria for exemptions will be included in future rulemaking.</p> <p>An Exchange must perform eligibility determinations for enrollment in a QHP, subsidies, Medicaid, CHIP and the Basic Health Plan if one is established by the State. Standards and eligibility criteria for these determinations will be addressed in future rulemaking.</p> <p>Each Exchange must establish a process for appeals of eligibility determinations, which will be addressed in future rulemaking.</p> <p>An Exchange must perform required functions related to oversight and financial integrity requirements in order to comply with PPACA §1313.</p>	

Obtained via FOIA by Judicial Watch, Inc.

Section	Summary	Questions/Comments
	<p>An Exchange must evaluate quality improvement strategies and oversee implementation of enrollee satisfaction surveys, assessment and ratings of health care quality and outcomes, information disclosures, and data reporting. These will be addressed in future rulemaking.</p> <p><i>HHS encourages States to consider supplemental standards or functionality for their Exchanges and requests comments regarding these and other functions that should be required of Exchanges.</i></p>	
<p>§155.205-Required consumer assistance tools and programs of an Exchange</p>	<p>An Exchange must establish a toll-free call center to respond to requests for assistance by consumers.</p> <p><i>HHS suggests that Exchanges consider operating the call center outside of normal business hours and adjusting staffing for expected call volumes. HHS believes the call center should be prepared to provide assistance on a broad range of issues, including:</i></p> <ul style="list-style-type: none"> • <i>Types of QHPs offered in the Exchange</i> • <i>Premiums, benefits, cost-sharing, and quality ratings associated with the QHPs offered</i> • <i>Categories of assistance available, including:</i> <ul style="list-style-type: none"> ◦ <i>Advance payments of premium tax credits</i> ◦ <i>Cost-sharing reductions</i> ◦ <i>Medicaid</i> ◦ <i>CHIP</i> • <i>The application process for enrollment in coverage through the Exchange and other programs, such as Medicaid and CHIP</i> <p><i>HHS also suggests that call centers be used as conduits to consumer assistance programs, Navigators, and other State consumer programs, where appropriate.</i></p> <p><i>HHS is seeking comment on ways to streamline and prevent duplication of effort by the Exchange call center and QHP issuers' customer call centers, but ensure that consumers have a variety of ways to learn about coverage options and receive assistance on other coverage issues.</i></p> <p>An Exchange must maintain an Internet web site that:</p> <ul style="list-style-type: none"> • Presents standardized comparative information on each available QHP, including: <ul style="list-style-type: none"> ◦ Premium and cost-sharing information ◦ Summary of benefits and coverage document <i>This could be made available through a link to the QHP web site, or the Exchange could require documents to be submitted in a manner that supports a searchable format.</i> <ul style="list-style-type: none"> ◦ Level of coverage provided (bronze, silver, gold, platinum, or catastrophic) ◦ Results of enrollee satisfaction surveys ◦ Quality ratings ◦ Medical loss ratio ◦ Transparency of coverage measures ◦ Provider directory 	

Section	Summary	Questions/Comments
	<p><i>HHS is requesting comments on the extent to which the Exchange Web site may satisfy the need to provide plan comparison functionality using HealthCare.gov.</i></p> <ul style="list-style-type: none"> • Provides meaningful access to information for individuals with limited English proficiency. Web sites must also be accessible to people with disabilities. <i>This requirement may be met by providing language assistance services, which may include translated information and "tag lines" directing individuals to translated materials and/or telephone numbers to call to reach interpreters for assistance.</i> • Publishes the following financial information: <ul style="list-style-type: none"> ○ Average cost of licensing required by the Exchange ○ Any regulatory fees required by the Exchange ○ Any other payments required by the Exchange ○ Administrative costs of the Exchange ○ Monies lost to fraud, waste and abuse • Provides contact information for Navigators and other consumer assistance services • Allows for eligibility determinations pursuant to §155.200(c) of this rule • Allows for enrollment in coverage in QHPs <p><i>HHS is considering a Web site requirement that would allow applicants and enrollees to store and access their personal account information and make changes, provided that the Web site complied with standards issued by HHS.</i></p> <p><i>HHS is also encouraging Exchanges to develop a feature whereby eligibility and enrollment experts, caseworkers, Navigators, agents and brokers, and other application assisters are able to maintain records of individuals they have assisted with the application process. They are requesting comments on this proposal.</i></p> <p>An Exchange must establish and make available electronically a calculator to assist individuals in comparing the costs of coverage in available QHPs after the application of subsidies.</p> <p><i>HHS is requesting comments on the extent to which States would benefit from a model calculator and suggestions for its design.</i></p> <p>An Exchange must provide a consumer assistance function (including but not limited to a Navigator program) that provides assistance services to consumers.</p> <p><i>If an Exchange receives complaints of race, color, national origin, disability, age, or sex discrimination, it may refer these individuals to the HHS Office of Civil Rights.</i></p> <p>An Exchange must conduct outreach and education activities separate from the implementation of the Navigator program.</p>	
§155.210-Navigator program standards	<p>Exchanges must award grant funds to public or private entities to serve as Navigators.</p> <p>Navigators must:</p> <ul style="list-style-type: none"> • Be capable of carrying out all required duties 	

Section	Summary	Questions/Comments
	<ul style="list-style-type: none"> • Demonstrate existing relationships, or the ability to readily establish relationships, with employers and employees, consumers (including the uninsured and underinsured), or self-employed individuals likely to be eligible to enroll in QHPs through the Exchange. • Meet any licensing, certification or other standards prescribed by the State or the Exchange, as appropriate • Be free of conflicts of interest during the term as a Navigator <p><i>HHS is requesting comments on whether it should propose additional requirements on Exchanges to make determinations regarding conflicts of interest</i></p> <p>The Exchange must select entities from at least two of the following categories to serve as Navigators:</p> <ul style="list-style-type: none"> • Community and consumer-focused nonprofit groups • Trade, industry and professional associations • Commercial fishing industry organizations, ranching and farming organizations • Chambers of commerce • Unions • Resource partners of the Small Business Administration • Licensed agents and brokers • Other public or private entities that meet the requirements of this section, which may include: <ul style="list-style-type: none"> ○ Indian tribes, tribal organizations, urban Indian organizations ○ State or local human service agencies <p><i>HHS is requesting comments on whether it should require that at least one of the two types of entities include a consumer-focused nonprofit organization, or whether it should require that Navigator grantees reflect a cross-section of stakeholders.</i></p> <p>Navigators may not be health insurance issuers or receive any consideration directly or indirectly from any health insurance issuer in connection with the enrollment of individuals or employers in a QHP.</p> <p><i>Such consideration includes any:</i></p> <ul style="list-style-type: none"> • Monetary or non-monetary commission • Kick-back • Salary • Hourly wage • Payment made directly or indirectly to the entity or individual from the QHP issuer. <p><i>This provision would not preclude a Navigator from receiving compensation from health insurance issuers in connection with enrolling individuals, small employers or large employers in non-QHPs. HHS is seeking comments on this issue and whether there are ways to manage any potential conflict of interest that might arise.</i></p> <p>A Navigator must carry out the following minimum duties:</p>	

Section	Summary	Questions/Comments
	<ul style="list-style-type: none"> Maintain expertise in eligibility, enrollment, and program specifications and conduct public education activities to raise public awareness of the Exchange Provide information and services in a fair and impartial manner, acknowledging other health programs <p><i>HHS is considering standards related to the content of information shared, referral strategies, and training requirements to include in grant award conditions and welcomes comments on the topic.</i></p> <ul style="list-style-type: none"> Facilitate enrollment in QHPs Provide referrals to any applicable office of health insurance consumer assistance or ombudsman or other appropriate State agency for any enrollee with a grievance, complaint or question regarding their health plan, coverage, or a determination under that plan Provide information in a manner that is culturally and linguistically appropriate <p><i>HHS is seeking comments regarding any specific standards it might issue on the provision of information in a culturally and linguistically appropriate manner.</i></p> <p><i>The Exchange may require that a Navigator meet additional standards and carry out additional duties as long as they are consistent with the above.</i></p> <p>An Exchange may not use Federal funds to support the Navigator program. However, if Navigators are permitted or required to address Medicaid or CHIP administrative functions, and these functions are performed under a contract or agreement that specifies a method for identifying costs attributable to these programs, the Medicaid and CHIP agencies may claim federal funding for a share of these costs.</p> <p><i>HHS is considering a requirement that Exchanges ensure that the Navigator program is operational on the first day of the initial open enrollment period (October 1, 2013) and is seeking comments on this requirement.</i></p>	
<p>§155.220-Ability of States to permit agents and brokers to assist qualified individuals, qualified employers, or enrolling in QHPs</p>	<p>An Exchange may allow agents and brokers to enroll qualified individuals, employers and employees in QHPs and assist them in applying for subsidies.</p> <p>It may also display information regarding agents and brokers on its web site or in other materials.</p> <p><i>Some web-based or other entities with experience in health plan enrollment are seeking to assist in QHP enrollment in several ways, including:</i></p> <ul style="list-style-type: none"> By contracting with an Exchange to perform outreach and enrollment functions; Acting independently of an Exchange to perform similar outreach and enrollment functions to the Exchange. 	

Section	Summary	Questions/Comments
	<p><i>To the extent that an Exchange contracts with such entities, it would remain responsible for ensuring that statutory and regulatory requirements pertinent to the contracted functions are met. In addition, HHS notes that subsidies are available only through the Exchange. HHS is seeking comments on the functions that such entities could perform, the potential scope of how these entities would interact with the Exchanges and what standards should apply to an entity performing functions in place of, or on behalf of, an Exchange. They also seek comments on the practical implications, costs, and benefits to an Exchange that coordinates with such entities, as well as any security- or privacy-related implications of such an arrangement.</i></p> <p>Standards in this section do not apply to agents or brokers serving as Navigators, who many not receive any financial compensation from an issuer for helping an individual or employer select a QHP.</p>	
<p>§155.230-General standards for Exchange notices</p>	<p>Any notice sent by an Exchange pursuant to these regulations must be in writing and include:</p> <ul style="list-style-type: none"> • Contact information for customer service resources; • An explanation of rights to appeal, if applicable; and • A citation to the specific regulation serving as the cause for notice <p>All applications, forms and notices must be provided in plain language and written in a manner that meets the needs of diverse populations by providing meaningful access to limited English proficient individuals and ensuring effective communication for people with disabilities.</p> <p><i>HHS is seeking comments regarding whether it should include requirements to provide information about the availability and steps to obtain oral interpretation services, information about the languages in which written materials are available, and the availability of materials in alternate formats for persons with disabilities, as well as other requirements they might consider to provide meaningful access to limited English proficient individuals and to ensure effective communication for people with disabilities.</i></p> <p>The Exchange must annually re-evaluate the appropriateness of the applications, forms, and notices and in consultation with HHS when changes are made.</p>	
<p>§155.240-Payment of premiums</p>	<p>In the individual market, an Exchange generally has 3 options with regard to payment of premiums:</p> <ul style="list-style-type: none"> • Take no part in payment of premiums, so that enrollees pay premiums directly to the QHP issuer; • Facilitate the payment of premiums by creating an electronic "pass-through" without directly retaining any of the payments; or • Establish a payment option where the Exchange collects premiums from enrollees and pays an aggregated sum to the QHP issuers. <p>An Exchange must allow an individual enrolled in a QHP to pay any applicable premium directly to the issuer, if he or she wishes, regardless of the option chosen above.</p> <p>An Exchange may also allow Indian tribes, tribal organizations and urban Indian organizations to pay the QHP premiums on behalf of qualified individuals, subject to terms and conditions established by the Exchange.</p>	

Section	Summary	Questions/Comments
	<p><i>HHS is seeking comment on whether and how an up-front group payment mechanism similar to what is currently used by some tribes to enroll members in Medicare Part D plans would work in an Exchange. Under this mechanism tribes offer a selection of plans to members from which they may choose, thus limiting their choices.</i></p> <p>An Exchange must accept payment of an aggregate premium by a qualified employer, pursuant to standards set forth in <u>§155.705(b)(4)</u>.</p> <p>An Exchange may facilitate the collection and payment of premiums through electronic means, though it must conform to any standards and protocols required under <u>§155.260</u> and <u>§155.270</u> and must ensure the integrity of the financial transactions.</p> <p><i>Premium collection by the Exchange does not make it liable for payment.</i></p> <p><i>HHS seeks comments concerning Exchange flexibility in establishing the premium payment process and what standards would be appropriate for the Federal government to establish in regulations to ensure fiduciary accountability in the case of an Exchange that collects premiums.</i></p>	
<p>§155.260-Privacy and security of information</p>	<p>An Exchange must apply appropriate security and privacy protections when collecting, using, disclosing or disposing of personally identifiable information it collects. Personally identifiable information is information that, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, can reasonably be used to distinguish or trace an individual's identity.</p> <p>The collection, use, and disclosure of personally identifiable information is limited to what is specifically required by:</p> <ul style="list-style-type: none"> • This section; • Other applicable law; • <u>Subpart E</u> of this regulation (dealing with enrollment of individuals in individual market QHPs); • Standards established in accordance with <u>§155.200(c)</u>; or • Section 1942(b) of the (Social Security) Act (dealing with information required for Medicaid and CHIP eligibility determinations). <p><i>Exchanges may not collect, use or disclose personally identifiable information if prohibited by another law. HHS invites comments as to whether and how it should restrict the method of disposal in this section as well.</i></p> <p><i>Each Exchange should conduct analysis of its operations and functions and determine its HIPAA status and must comply with HIPAA privacy requirements if it is a HIPAA covered entity. Regardless of this analysis, each Exchange must implement safeguards to ensure that any and all personally identifiable information received, used, stored, transferred, or prepared for disposal by an Exchange is subject to adequate privacy and security protections.</i></p> <p>Exchange security standards must be consistent with HIPAA security rules, and must be applied to sub-contractors through contractual requirements.</p>	

Section	Summary	Questions/Comments
	<p><i>HHS is considering requiring each Exchange to adopt privacy policies that conform to the Fair Information Practice Principles (FIPPs) and requests comments on their appropriateness in this context and the best means to integrate them into the privacy policies and operating procedures of individual Exchanges while allowing for adaptability to each Exchange's structure and operations.</i></p> <p>The privacy and security policies and procedures of an Exchange must be in writing and available to HHS and must identify any applicable laws that it will need to follow. Contractors and subcontractors must be covered by the same or higher privacy and security policies than are applicable to the Exchange.</p> <p><i>HHS is considering a requirement that each Exchange implement some form of authentication procedure for ensuring that all entities interacting with Exchanges are who they claim.</i></p> <p>An Exchange must participate in the data matching program with the state Medicaid and CHIP agencies. Data use agreements between the Exchange and these entities must prevent the unauthorized use or disclosure of personally identifiable information and prohibit the Exchange and agencies from seeking information that they do not reasonably expect to use.</p> <p>Exchanges must adopt privacy and security policies and procedures that meet the standards of the Internal Revenue Code that protect the confidentiality of tax returns and tax return information.</p>	
<p>§155.270-Use of standards and protocols for electronic transactions</p>	<p>Any person who knowingly and willfully uses or discloses personally identifiable information in violation of section 1411(g) of PPACA will be subject to civil money penalties of up to \$25,000 per disclosure and any other applicable penalties prescribed by law.</p> <p>To the extent an Exchange performs electronic transactions with a HIPAA covered entity, including State Medicaid programs and QHP issuers, the Exchange must use HIPAA standards and operating rules adopted by HHS pursuant to 45 CFR parts 160 and 162.</p> <p>HT enrollment standards and protocols developed pursuant to PHSA 3021 will be incorporated within Exchange IT systems as required under the Exchange cooperative agreements awarded pursuant to 1311(a) of PPACA.</p>	
<p>Subpart F—Exchange functions in the individual market: Enrollment in Qualified Health Plans</p> <p>§155.400-Enrollment of qualified individuals into QHPs</p>	<p>An Exchange must accept a QHP selection from an applicant who is determined eligible for enrollment in a QHP, notify the issuer of the applicant's selected QHP, and transmit information necessary to enable the QHP issuer to enroll the applicant.</p> <p>The Exchange must send QHP issuers enrollment information on a timely basis and must develop a process by which QHP issuers may acknowledge the receipt of this information.</p> <p><i>HHS will be issuing further guidance regarding the timing of transmission of enrollment information to QHP issuers. They encourage real-time processing and</i></p>	

Section	Summary	Questions/Comments
	<p><i>acknowledgement of enrollment and seek comments on whether they should require a specific frequency for enrollment transaction (e.g. real-time or daily, etc.)</i></p> <p>The Exchange must maintain records of enrollment, submit enrollment information to HHS, and reconcile enrollment files with QHP issuers at least monthly.</p>	
<p>§155.405-Single streamlined application</p>	<p>The Exchange must use a single streamlined application to collect information necessary for QHP enrollment, subsidies, and Medicaid, CHIP and the Basic Health Plan. HHS will create both a paper-based and web-based dynamic application.</p> <p>If the Exchange seeks to use an alternative application, it must be approved by HHS.</p> <p><i>HHS seeks comments on whether it should require that applicants not be required to answer questions that are not pertinent to the eligibility and enrollment process.</i></p> <p>The Exchange must accept applications from multiple sources, including:</p> <ul style="list-style-type: none"> • The applicant; • An authorized representative as defined by state law; or • Or someone acting responsibly for the applicant. <p>An individual must be able to file an application online, by telephone, by mail, or in person.</p> <p><i>HHS is soliciting comments on the requirement that individuals must be allowed to file an application in person.</i></p>	
<p>§155.410-Initial and annual open enrollment periods</p>	<p>Exchanges must adhere to the initial and annual open enrollment periods. Initial and annual open enrollment periods and special enrollment periods are the only times when an Exchange may permit a qualified individual to enroll in a QHP or change QHPs.</p> <p>The initial open enrollment period will be October 1, 2013 through February 28, 2014.</p> <p><i>HHS seeks comments on the duration of the initial open enrollment period.</i></p> <p>If the Exchange receives an application for coverage on or before December 22, 2013, the Exchange must ensure a coverage effective date of January 1, 2014. Applications received between the 1st and 22nd of any subsequent month must be processed to ensure an effective date of the 1st of the following month.</p> <p>If the Exchange receives an application for coverage between the 23rd and the last day of any month between December 2013 and February 2014, coverage must be effective either the first day of the following month or the first day of the second following month.</p> <p><i>The coverage effective date may not be set and enrollment information may not be sent from the Exchange to the QHP until an individual has been determined to be eligible to purchase coverage through the Exchange.</i></p> <p><i>Coverage in a QHP may only begin on the first day of a month. This was proposed in order to align with a statutory restriction that individuals may only receive subsidies if they are enrolled in a QHP on the first day of the month. HHS is seeking comment as to whether it should consider allowing at least twice-monthly effective dates for coverage or complete flexibility to allow for coverage to being any day for individuals who forgo</i></p>	

Section	Summary	Questions/Comments
	<p><i>subsidies until the first day of the next month.</i></p> <p>The Exchange must send written notification to enrollees about the annual open enrollment period.</p> <p><i>HHS is considering requiring that the notice be sent no later than 30 days before the start of the annual open enrollment period and requiring that it contain specified information, including:</i></p> <ul style="list-style-type: none"> <i>• The date annual enrollment begins and ends;</i> <i>• Where individuals may obtain information about available QHPs, including the Web site, call center and through Navigator assistance; and</i> <i>• Other relevant information.</i> <p><i>HHS is seeking comment on whether they should include such requirements.</i></p> <p>The annual open enrollment period will be from October 15 through December 7 of each year, starting in October 2014 for coverage beginning January 1, 2015.</p> <p><i>HHS considered an alternative annual open enrollment period from November 1 through December 15 of each year. They are seeking comment regarding the proposed and alternative annual open enrollment periods.</i></p> <p>The Exchange must ensure coverage is effective as of the first day of the following benefit year for a qualified individual who has made a QHP selection during the annual open enrollment period.</p> <p><i>HHS is seeking comment regarding whether they should require Exchanges to automatically enroll individuals who received subsidies and are then disenrolled from a QHP because the QHP is no longer offered if that individual does not make a new QHP selection.</i></p> <p><i>HHS is also seeking comment on whether they should require automatic enrollment of individuals into new QHPs when there are mergers between issuers or when one QHP offered by an issuer is no longer offered but there are other options available from the same issuer.</i></p> <p><i>HHS is also seeking comment on how far any automatic enrollment should extend.</i></p>	
<p>\$155,420-Special enrollment periods</p>	<p>The Exchange must allow a qualified individual or enrollee to enroll in a QHP or change from one QHP to another outside of the annual open enrollment period if such individual qualifies for a special enrollment period.</p> <p>For eligible individuals selecting coverage during a special enrollment period, the Exchange must ensure that their effective date of coverage is on the first day of the following month for all QHP selections made by the 22nd of the previous month, and on either the first day of the following month or the first day of the second following month for selections made between the 23rd and last day of the previous month. There is an exemption to this rule in the case of birth, adoption, or placement for adoption, for which coverage must be effective on the date of birth, adoption, or placement for adoption.</p>	

Section	Summary	Questions/Comments
	<p>Special enrollment periods will last for 60 days from the date of the triggering event unless the regulation specifically provides otherwise.</p> <p>All requests for special enrollment periods must be evaluated by the Exchange as part of the eligibility determination process.</p> <p>For purposes of special enrollment periods, a dependent is any individual who is or may become eligible for coverage under the terms of a QHP because of a relationship to an enrollee.</p> <p>Triggering Events:</p> <ul style="list-style-type: none"> Loss of other minimum essential coverage, defined as any event that triggers a loss of eligibility for other minimum essential coverage. <ul style="list-style-type: none"> <i>Examples would include</i> <ul style="list-style-type: none"> Decertification of a QHP outside of the annual open enrollment period; Legal separation or divorce ending eligibility of a spouse or step-child as a dependent; End of dependent status; Death of an individual enrolled in minimum essential coverage ending eligibility for covered dependents; Termination of employment or reduction in the number of hours required to maintain coverage; Relocation outside the service area of the QHP. Termination of employer contributions for a qualified individual or dependent who has coverage that is not COBRA continuation coverage; Exhaustion of COBRA continuation coverage; Reaching a lifetime limit on all benefits in a grandfathered plan; Termination of Medicaid or CHIP. <p>HHS is seeking comment on its limitation of the special enrollment period to only those who lose minimum essential coverage, as opposed to any coverage. This was done to avoid adverse selection.</p> <ul style="list-style-type: none"> Addition of a dependent through marriage, birth, adoption, or placement for adoption; <ul style="list-style-type: none"> <i>HHS seeks comments as to whether States might consider expanding the special enrollment period to include gaining dependents through other life events.</i> Error in enrollment where the Exchange finds that enrollment or non-enrollment in a QHP is unintentional, inadvertent or erroneous and is the result of the error, misrepresentation, or inaction of an officer, employee, or agent of the Exchange or HHS, or its instrumentalities as evaluated and determined by the Exchange. QHP in which an individual was enrolled substantially violated a material provision of its contract in relation to such individual and their dependents. <i>One example would be misrepresentation of the plan while marketing.</i> Becoming newly eligible or newly ineligible for premium tax credits or a change in eligibility for cost-sharing reductions. This would allow an individual to newly enroll in 	

Section	Summary	Questions/Comments
	<p>coverage or to change from one QHP to another.</p> <p><i>HHS seeks comments as to whether the start of the 60 day special enrollment period should be based upon the date on which an individual experiences a change in eligibility or based upon the date of the eligibility determination.</i></p> <p><i>HHS also requests comments on the timing of the special enrollment period in the case of an individual whose employer-sponsored coverage no longer provides minimum essential benefits or is no longer affordable in the coming plan year. In such a case, the individual would be allowed to apply for QHP coverage while still covered so as to prevent a gap in coverage.</i></p> <ul style="list-style-type: none"> • New QHPs offered through the Exchange become available to an employee as a result of a permanent move. <i>HHS requests comments on whether the special enrollment period should begin on the date of the permanent move or on the date the individual provides notification of the move.</i> • Indians will be entitled to a monthly special enrollment period, pursuant to section 1311(c)(6)(D) of PPACA. <i>HHS solicits comments on the potential implications on the process for verifying Indian status.</i> • Exceptional circumstances, as determined by the Exchange or HHS. <i>This special enrollment period could be used for a variety of situations, including natural disasters such as hurricanes or floods. Exceptional circumstances include circumstances that would impede an individual's ability to enroll on a timely basis, through no fault of his or her own.</i> <p>Loss of coverage does not include failure to pay premiums on a timely basis, including COBRA premiums prior to the expiration of COBRA coverage, or situations allowing for a rescission.</p> <p>During a special enrollment period, an existing enrollee of a QHP may only switch to another plan within the same coverage level. There would be an exception to this rule in the case of an individual who is newly eligible for subsidies. <i>HHS is requesting comment on whether an exception should also be made in the case of an individual enrolled in a catastrophic plan who becomes pregnant.</i></p> <p><i>HHS clarifies that the Exchange will provide information, accept applications, perform eligibility determinations, and accept enrollments and send enrollment information to QHPs year round in order to accommodate special enrollment periods and coverage through Medicaid and CHIP.</i></p> <p><i>To the extent other law applies to require a special enrollment period, that law will continue to apply.</i></p>	
§155.430-Termination of coverage	<p>The Exchange must determine the form and manner in which QHP coverage may be terminated. The following events will cause an individual's coverage in a QHP to be terminated:</p> <ul style="list-style-type: none"> • Voluntary termination by enrolled with appropriate notice to the Exchange; 	

Section	Summary	Questions/Comments
	<ul style="list-style-type: none"> • Loss of eligibility to purchase through the Exchange; • Enrolled becomes covered in other minimum essential coverage; • Payment of premiums for QHP coverage ceases, provided that the grace period in §156.270(d) has elapsed; • Coverage is rescinded; • QHP terminates or is decertified by the Exchange; • Enrolled switches to another QHP during an annual open enrollment period or special enrollment period. <p>An Exchange must establish maintenance of records procedures for terminations of coverage, track the number of individuals for whom coverage has been terminated, and submit that information to HHS on a monthly basis, establish terms for reasonable accommodations, and retain records in order facilitate audit functions.</p> <p>Effective dates of terminations:</p> <ul style="list-style-type: none"> • In the case of an individual who requests termination, coverage will be terminated effective on the date specified by the enrollee if the Exchange and QHP have a reasonable amount of time. If not, coverage will be terminated effective the first day after a reasonable amount of time has passed. • In the case of an enrollee obtaining new minimum essential coverage, the day before the effective date of the new coverage. <i>HHS is soliciting comments regarding how Exchanges work with QHP issuers to implement this proposal, which is intended to prevent double coverage (which would make an individual ineligible for subsidies).</i> • In the case of termination by the Exchange or QHP as a result of the enrollee changing QHPs, the last day of coverage before the new coverage begins. • In the case of any other termination, the last day of coverage is the 14th day of the month if the notice is sent by the Exchange or termination initiated by the QHP by the 14th day of the previous month, or the last day of the month, if the notice sent or termination initiated by the last day of the previous month. 	
Subpart H—Exchange Functions: Small Business Health Options Program (SHOP)		
§155.700-Standards for the establishment of a SHOP	An Exchange must provide for the establishment of a SHOP that meets the requirements of this subpart, and is designed to assist qualified employers and facilitate the enrollment of qualified employees into qualified health plans.	
§155.705-Functions of a SHOP	<p>A SHOP must carry out all required functions of an Exchange outlined in subparts C (General Functions), E (Individual Enrollment), H (SHOP Functions), and K (Certification of QHPs), except:</p> <ul style="list-style-type: none"> • Individual eligibility determinations and appeals of such determinations; • Enrollment of qualified individuals into individual market QHPs; • Premium calculator; <p><i>HHS encourages a SHOP to consider options to calculate and display the net employee contribution to the premium for different plans and different family compositions, after any employer contribution has been subtracted from the</i></p>	

Section	Summary	Questions/Comments
	<p><i>full premium amount.</i></p> <ul style="list-style-type: none"> • Certification of exemptions from the individual coverage requirement; • Requirements relating to payment of premiums by individuals, Indian tribes, tribal organizations, and urban Indian organizations. <p>In addition, a SHOP must:</p> <ul style="list-style-type: none"> • Adhere to unique enrollment and eligibility requirements in <u>§155.710</u> through <u>730</u>. • Facilitate special enrollment periods under <u>§155.420</u>, except for those due to changes in immigration status and in eligibility for subsidies. • Allow a qualified employer to choose a level of coverage, under which a qualified employee may select an available QHP; <ul style="list-style-type: none"> ◦ Exchanges may also choose additional ways for employers to offer one or more plans to employees, including: <ul style="list-style-type: none"> ▪ Allowing employees to choose any QHP at any level of coverage; ▪ Allowing employers to select specific levels from which an employee may choose a QHP; ▪ Allowing employers to select specific QHPs from different levels of coverage from which an employee may choose; or ▪ Allowing employers to select a single QHP to offer employees. <p><i>HHS requests comments on its interpretation of §1312(a)(2)(A) and (j)(2)(B) of PPACA, which speaks to employer specification of a level of coverage and permit a single QHP selection by an employer, respectively, and on the proposed flexibility in this provision.</i></p> <p><i>HHS requests comments on whether QHPs offered in the SHOP should be required to waive minimum participation rules at the level of the QHP or issuer, whether a minimum participation rule applied at the SHOP level is desirable, and if so, how the rate should be calculated, what the rate should be, and whether the minimum participation rate should be established in Federal regulation.</i></p> <ul style="list-style-type: none"> • Allow qualified employers to receive a single monthly bill for all QHPs in which their employees are enrolled and to pay a single monthly amount to the SHOP. <ul style="list-style-type: none"> ◦ The SHOP must provide a monthly bill to qualified employers that identifies the total premiums owed. ◦ The SHOP must collect from employers offering multiple coverage options a single cumulative premium payment for all a qualified employer's qualified employees enrolled through the employer in the SHOP. • Ensure that QHPs meet certification requirements outlined in <u>§156.285</u>. • Require all QHPs to make any changes to rates at a uniform time that is either quarterly, monthly, or annually and require that the rate for a given employer not change during the plan year. <p><i>HHS requests comments on whether it should allow a more permissive or restrictive timeframe than monthly, quarterly, or annually and on what rates</i></p> 	

Section	Summary	Questions/Comments
	<p><i>should be used to determine premiums during the plan year.</i></p> <ul style="list-style-type: none"> • Offer qualified employers and employees only small group QHPs. It may make available only those QHPs that meet the SHOP requirements if the State elects to merge its individual and small group risk pools. • States may allow insurers in the large group market to offer health plans inside of the SHOP beginning in 2017. In states that elect to do so, large employers could make an employee eligible for the SHOP if it provides all full-time employees the opportunity to do so. 	
<p>§155.710-Eligibility standards for SHOP</p>	<p>The SHOP must permit qualified employers to purchase coverage for qualified employees in the SHOP.</p> <p>The SHOP must ensure that the employer employs no more than 100 employees, with the exception that a State may limit enrollment in the small group market to employers with no more than 50 employees until January 1, 2016.</p> <p><i>Section 1304 of PPACA defines the calculation of an employer's size based upon the average number of employees employed on business days during the preceding calendar year. The terms "employer," "small employer," and "large employer" are defined in §155.20 and are based on the definitions in the PHS Act. The PHS act determines employer size by counting all employees, including part-time and seasonal employees, to determine an employer's size. Part time workers would be counted in the same manner as full-time workers, while seasonal employees would be counted proportionately to the number of days they work in a year...Because the PHS Act definition of employer and ERISA definition of group health plan refer to at least 1 employee, they exclude sole proprietors, certain owners of S corporations, and certain relatives of each of the above. HHS solicits comments on this approach.</i></p> <p>The SHOP must ensure that a qualified employer provides an offer of coverage through a SHOP to all full-time employees. An employer may cover all employees through the SHOP covering its principal business address or may cover employees through the SHOPS covering each employee's primary worksite.</p> <p><i>If an employer opts for the latter coverage option, SHPs could establish a participation rule with respect to the number of employees employed by the employer within the service area of the SHOP.</i></p> <p>An employer participating in SHOP may continue to do so if the number of workers employed grows to exceed 100 (or 50 if the state chooses that level until 2016), provided the employer continues to meet all other eligibility requirements.</p> <p>A qualified employee is an employee who receives an offer of coverage through the SHOP from a qualified employer.</p>	
<p>§155.715-Eligibility determination process for SHOP</p>	<p>A SHOP must determine eligibility of an employer consistent with the standards in §155.710.</p> <p><i>SHOPS may allow employers to self-report the size of their workforce with an attestation of its accuracy, however, they may also require a more stringent determination of</i></p>	

Section	Summary	Questions/Comments
	<p><i>employer size. The SHOP must also verify that the employer offers coverage through the SHOP to all full-time employees and that at least one employee works in the SHOP's service area. HHS believes self-reporting with attestations should be sufficient to verify this information.</i></p> <p>The SHOP must use only 2 application forms, one for employers and one for employees.</p> <p>The SHOP may use information attested to by the employer or employee on the applicable application for determining eligibility. However, the SHOP must verify that each employee applying for coverage is listed on the employer's roster of employees. A SHOP may establish additional verification methods.</p> <p><i>Future rulemaking will address appeals related to this process.</i></p> <p>The SHOP must have processes to resolve doubts regarding information provided on employer and employee applications. The applicant must be notified by the SHOP and the SHOP must make a reasonable effort to identify and address the cause of the doubt, confirm the accuracy of relevant information and provide the applicant with 30 days to correct the possible error. The applicant must then be notified of the SHOP's determination. If an employer was enrolled in a plan before the completion of the verification process, the SHOP must then discontinue the employer's participation at the end of the month following the month in which the notice was sent.</p> <p>The SHOP must notify employers and employees of eligibility determinations and their rights to appeal.</p> <p>If a qualified employer ceases to provide coverage through the SHOP, the SHOP must ensure that:</p> <ul style="list-style-type: none"> • Each QHP terminates the coverage of the employers qualified employees; and • Each qualified employee enrolled in a QHP is notified of the employer's withdrawal and their termination of coverage in advance. <p><i>HHS is considering whether this notice must inform the employee about eligibility for special enrollment periods in the Exchange and about the eligibility process for subsidies, Medicaid, and CHIP. They solicit comments on this eligibility and notification process.</i></p>	
§155.720-Enrollment of employees into QHPs under SHOP	<p>A SHOP must process applications for enrollment from employees and facilitate enrollment of qualified employees into QHPs.</p> <p>The SHOP must establish a uniform enrollment timeline and process to be followed by all employers and QHPs in the SHOP, which includes the following activities that must occur before the effective date of coverage for qualified employees:</p> <ul style="list-style-type: none"> • Determination of employer eligibility • Qualified employer selection of QHPs offered to qualified employees • Provision of a specific timeframe for employer selection of level of coverage or QHP offering 	

Section	Summary	Questions/Comments
	<ul style="list-style-type: none"> • Provision of a specific timeframe for employees to complete the employee application process • Determination and verification of employee eligibility for enrollment through the SHOP • Enrollment processing of employees into selected QHPs • Establishment of effective dates of employee coverage. <p><i>These activities should be standardized relative to a plan year, rather than a calendar year, to reflect the rolling enrollment of the SHOP.</i></p> <p>The SHOP must process applications in accordance with the above timeline and adhere to the requirements in <u>§155.400(b)</u> regarding enrollment and timing of data exchange between the SHOP and QHPs.</p> <p>The SHOP must adhere to standards in <u>§155.705(b)</u> regarding payment administration.</p> <p>The SHOP must ensure that qualified employees are notified of their effective date of coverage.</p> <p>The SHOP must maintain records of qualified employer participation and qualified employee enrollment in the SHOP, which must also be reported to HHS, consistent with <u>§155.400(d)</u>. Enrollment reconciliation with QHPs must occur at least monthly, though SHOPs may conduct them more frequently.</p> <p><i>HHS welcomes comments about whether it should establish target dates or deadlines so that multi-State qualified employers are subject to consistent rules.</i></p> <p>If a qualified employee voluntarily terminates coverage from a QHP, the SHOP must notify the individual's employer.</p>	
<p>§155.725-Enrollment periods under SHOP</p>	<p>The SHOP must adhere to the start of the initial open enrollment period for the Exchange and ensure that enrollment transactions are sent to QHPs and that issuers adhere to coverage effective dates in accordance with <u>§155.260</u>. The initial open enrollment period for SHOP begins on October 1, 2013 for coverage effective January 1, 2014. Because of the rolling enrollment in SHOP, there is no end date for the open enrollment period.</p> <p>Employers may begin participating in SHOP at any time during the year, though qualified employees may only enroll or change plans once a year unless they qualify for a special enrollment period. Plan years inside SHOP must consist of a 12 month period beginning with the employer's effective date of coverage.</p> <p><i>HHS invites comments on these provisions.</i></p> <p>A SHOP must provide for an annual employer election period in advance of the annual open enrollment period, during which time a qualified employer may modify its contribution and plan offerings.</p> <p>A SHOP must notify participating employers that their annual election period is approaching.</p> <p><i>HHS is considering whether to require the employer to receive 30 days advance notice</i></p>	

Obtained via FOIA by Judicial Watch, Inc.

Section	Summary	Questions/Comments
	<p><i>that the election period is approaching. HHS solicits comments on this requirement.</i></p> <p>A SHOP must establish an annual employee open enrollment period for qualified employees. This period must occur prior to the end of the plan year and after the employer's election period.</p> <p><i>HHS solicits comments on this requirement.</i></p> <p>A SHOP must ensure that a qualified employee hired outside of the initial or annual open enrollment period would have a specified window set by SHOP to seek coverage in a QHP beginning with the first day of employment, which would continue through the end of the employer's plan year, at which point the employee could renew or change coverage.</p> <p><i>HHS solicits comments on the se proposed notices and their interaction with existing law and regulation.</i></p> <p>A SHOP must establish effective dates of coverage for qualified employees consistent with those described in <u>§155.720</u>.</p> <p>A qualified employee enrolled in a QHP through SHOP will remain enrolled in that plan in the next plan year unless:</p> <ul style="list-style-type: none"> • The employee terminates coverage in accordance with <u>§155.430</u>; • The employee enrolls in another QHP if that option exists; or • The QHP in which the employee was enrolled is no longer available. <p><i>HHS welcomes comments about its approach in differentiating individual and small group enrollment as well as specific comments concerning the proposed structure for initial, rolling, and annual open enrollment through SHOP.</i></p>	
<p>§155.730-Application standards for SHOP</p>	<p>SHOP applications must adhere to application standards in this section.</p> <p>The SHOP must use a single employer application to determine employer eligibility and to collect the information necessary for an employer to purchase coverage through the SHOP. This information must include the:</p> <ul style="list-style-type: none"> • Employer's name and address • Number of employees • Employer Identification Number • List of qualified employees and their SSNs. <p><i>The application may be submitted by other individuals or organizations on behalf of the employer. HHS welcomes comments regarding other employer information it should require a SHOP to collect.</i></p> <p>The SHOP must use a single employee application to collect eligibility and QHP selection and enrollment information from employees. <i>The single streamlined application used in the individual Exchange may be modified to meet the needs of an employee in the SHOP. The application may be submitted by other individuals or organizations on behalf of the employee.</i></p>	

Section	Summary	Questions/Comments
	<p>SHOPs may use a model single employer application and model single employee application created by HHS. <i>The model application will be proposed by HHS, after consultation with the NAIC.</i></p> <p>A SHOP may use an alternative employer application with approval from HHS. It should include the information specified above. It may also use an alternative employee application with approval from HHS.</p> <p>The SHOP must allow employers and employees to submit their eligibility and enrollment information consistent with §155.405(c).</p>	
Subpart K—Exchange Functions: Certification of Qualified Health Plans		
§155.1000-Certification standards for QHPs	<p>An Exchange may not make available any health plan that is not a QHP. A QHP must have a certification issued or recognized by the Exchange as QHPs. Any reference to QHPs includes multi-State plans, unless specifically provided for otherwise.</p> <p>The Exchange may certify a health plan as a QHP if it provides evidence that it complies with the minimum certification requirements in subpart C of part 156 and the Exchange determines that making it available is in the interests of qualified individuals and qualified employers in the state.</p> <p>An Exchange may not exclude a plan because:</p> <ul style="list-style-type: none"> • It is a fee-for-service plan; • Through the imposition of price controls; or • On the basis that it provides treatments necessary to prevent patients' deaths in circumstances that the Exchange determines are inappropriate or too costly. <p>The Exchange must establish procedures for the certification of QHPs.</p>	
§155.1010-Certification process for QHPs	<p>A multi-State plan offered through OPM must be deemed as certified by the Exchange. MSPs must meet all the requirements of a QHP, as determined by OPM.</p> <p><i>HHS believes the intent of the statute is that each Exchange must accept MSPs as QHPs without applying an additional certification process to such plans.</i></p> <p>The Exchange must complete the certification of QHPs prior to the open enrollment periods established in §155.410.</p> <p>The Exchange must monitor QHP issuers for demonstration of ongoing compliance with the certification requirements in §155.1000(c).</p>	
§155.1020-QHP issuer rate and benefit information	<p>An Exchange must receive a QHP issuer's justification for a rate increase prior to its implementation and ensure that the issuer posts it to its website. <i>The Exchange may satisfy this requirement by receiving it from the state Department of Insurance or HHS.</i></p> <p>The Exchange must consider the following factors related to rates before certifying a QHP:</p> <ul style="list-style-type: none"> • The justification of the increase prior to its implementation; • Recommendations provided to the Exchange by the State under PHSA 2794(b)(1)(B); • Any excess rate growth outside the Exchange compared to rate growth inside the 	

Section	Summary	Questions/Comments
	<p>Exchange.</p> <p>The state rate review process, when available, should be leveraged by the Exchange to avoid any duplication with State law.</p> <p>HHS is considering a standard for the final rule in which there would be a bifurcated process for the rate increase justification. Where PHSA section 2794 applies (rates are subject to review), the Exchange may rely on the justification submitted pursuant to that section. Where it does not apply, the Exchange would develop a less burdensome rate justification to satisfy this requirement. HHS would encourage the Exchange and Department of Insurance to collaborate in this process. HHS solicits comments on how best to align PHSA 2794 and PPACA 1311(e)(2).</p> <p>The Exchange must at least annually receive the following information for each QHP:</p> <ul style="list-style-type: none"> • Rate information • Covered benefits • Cost-sharing information <p>HHS will provide the form and the manner for the submission of this information.</p>	
<p>§155.1040- Transparency in coverage</p>	<p>Exchanges must require plans seeking certification as QHPs to submit transparency information to the Exchange. HHS and state insurance commissioner as described in §156.220(a).</p> <p><i>HHS is soliciting comments under this proposed rule as part of the process of planning for implementation of PPACA 1311(e)(3)(D)</i></p> <p>The Exchange must monitor the use of plain language, consistent with the definition in §155.20 and future guidance to be issued by HHS and Labor, by QHP issuers when making information under this section available.</p> <p>The Exchange must require QHP issuers to make cost sharing information available to enrollees. This is described in §156.220(c).</p>	
<p>§155.1045- Accreditation timeline</p>	<p>The Exchange must establish a consistent deadline for accreditation with respect to each issuer's initial participation in the Exchange.</p> <p><i>Although 1311(c)(1)(D)(i) requires QHPs to be accredited, HHS is interpreting the requirement to mean that the issuer must be accredited. §156.275 requires all issuers to be accredited. A grace period may be necessary for issuers that are not already accredited, since the process can take 12-18 months. HHS encourages Exchanges to set timelines that accommodate the length of the process, particularly for issuers seeking accreditation for the first time.</i></p>	
<p>§155.1050- Establishment of Exchange network adequacy standards</p>	<p>Each Exchange must ensure that enrollees of QHPs have a sufficient choice of providers.</p> <p><i>HHS solicits comments on additional minimum qualitative or quantitative standards for the Exchange to use in evaluating whether the QHP provider networks provide sufficient access to care. In particular, they seek comment on a potential additional requirement that the Exchange establish specific standards under which issuers would be required to maintain the following:</i></p> <ul style="list-style-type: none"> • <i>Sufficient numbers and types of providers to assure that services are accessible without unreasonable delay;</i> 	

Section	Summary	Questions/Comments
	<ul style="list-style-type: none"> • Arrangements to ensure a reasonable proximity of participating providers to the residence or workplace of enrollees, including a reasonable proximity and accessibility of providers accepting new patients. • An ongoing monitoring process to ensure sufficiency of the network for enrollees. • A process to ensure that an enrollee can obtain a covered benefit from an out-of-network provider at no additional cost if no network provider is accessible for that benefit in a timely manner. <p><i>HHS also seeks comments on an additional standard that the Exchange ensure that QHPs' provider networks provide sufficient access to care for all enrollees, including those in medically underserved areas.</i></p>	
\$155.1055-Service area of a QHP	<p>Exchanges must have a process to establish or evaluate the service areas of QHPs.</p> <p>The service area of a QHP must cover at least a county, or a group of counties if the Exchange designates such a group, unless the issuer demonstrates that serving a partial county is necessary, non-discriminatory, and in the interest of qualified individuals and employers.</p> <p>The Exchange must ensure that QHP service areas are established without regard to the racial, ethnic, language and health status factors outlined in PHSA 2705(a).</p>	
\$155.1065-Stand-alone dental plans	<p>The Exchange must allow limited scope stand-alone dental plans to be offered provided that the plan furnishes at least the pediatric essential dental benefit required by PPACA 1302(b)(1)(I). The plan must also comply with IRC 9832(c)(2)(A) and PHSA 2791(c)(2)(A), which define excepted limited scope dental and vision plans.</p> <p>The dental plan may be offered as a stand-alone plan or in conjunction with a QHP.</p> <p>A health plan may be certified as a QHP without offering the pediatric essential dental benefit as long as a stand-alone plan is offered through the Exchange.</p> <p><i>HHS is considering interpreting this provision such that an Exchange may require issuers of stand-alone dental plans to comply with any QHP certification requirements and consumer protections that it determines to be relevant and necessary. HHS requests comment on whether some of the requirements on QHP issuers should also apply to stand-alone dental plans as a Federal minimum and what limits Exchanges may face on placing requirement on dental plans, given that they are excepted benefits.</i></p> <p><i>HHS also requests comment on whether it should set specific operational minimum standards. Substantial operational issues exist with allocating subsidies and calculating actuarial value when stand-alone dental plans segment coverage for the essential health benefits.</i></p> <p><i>HHS also requests comment on whether QHPs should be required to offer and price dental benefits separately from medical coverage in order to promote comparisons of dental coverage.</i></p>	

Section	Summary	Questions/Comments
<p>§155.1075- Recertification of QHPs</p>	<p>The Exchange must implement procedures for the recertification of health plans as QHPs that includes a review of the general certification criteria in §155.1000(c).</p> <p><i>An Exchange may use this process to make modifications to any agreements between the Exchange and its QHP issuers. The Exchange may determine the frequency for recertifying QHPs. HHS invites comment as to whether it should specify requirements regarding the term length for recertification.</i></p> <p>After reviewing all relevant information and determining whether to recertify a QHP, the Exchange must notify the issuer of its recertification status. If it determines that the QHP should be decertified, it should proceed with the process outlined in <u>§155.1080</u>.</p> <p>The Exchange must complete the recertification process on or before September 15 of each year.</p> <p><i>HHS requests comments on the appropriateness of this deadline.</i></p>	
<p>§155.1080- Decertification of QHPs</p>	<p>Decertification is the termination by the Exchange of the certification status and offering of a QHP.</p> <p>An Exchange must implement procedures for the decertification of a QWP.</p> <p>The Exchange may decertify a QHP at any time if it determines that the issuer is no longer acting in accordance with the general certification requirements in §155.1000(c), including that the QHP participation is no longer in the interest of its enrollees.</p> <p><i>HHS recommends that Exchanges solicit input from a broad range of stakeholders, including issuers, when determining how to implement the decertification procedures.</i></p> <p><i>HHS requests comments on the creation of the process and what other authorities should be extended to the Exchange to make the process more efficient.</i></p> <p>The Exchange must establish and appeals process for health plans that have been decertified by the Exchange.</p> <p>If a QHP is decertified, the Exchange must provide notice of the decertification to parties who may be affected, including:</p> <ul style="list-style-type: none"> • The QHP Issuer; • Exchange enrollees in the QHP who must receive information about a special enrollment period, as described in <u>§155.420</u>; • HHS; and • The State Department of Insurance 	
<p>PART 156—Health Insurance Issuer Standards Under the Affordable Care Act, Including Standards Related to Exchanges</p>		
<p>§156.20-Definitions</p>	<p>"Benefit design standards" means coverage that provides for all of the following:</p> <ul style="list-style-type: none"> • The essential health benefits as described in section 1302(b) of PPACA • Cost-sharing limits as described in section 1302(c) of PPACA 	

Section	Summary	Questions/Comments
	<ul style="list-style-type: none"> A bronze, silver, gold, or platinum level of coverage as described in section 1302(d) of PPACA, or is a catastrophic plan as described in section 1302(e) of PPACA. 	
\$156.50-Financial support	<p>Issuers of QHPs, multi-state plans, stand-alone dental plans, and other issuers identified by the exchange that participates in a specific Exchange function that is funded by user fees must remit user fee payments assessed by an Exchange under <u>\$155.160</u>.</p>	
Subpart C—Qualified Health Plans Minimum Certification Criteria		
\$156.200-QHP issuer participation standards	<p>To participate in an Exchange, a health insurance issuer must have in effect a certification issued or recognized by the Exchange to demonstrate that each health plan it offers in the Exchange is a QHP and that the issuer meets all requirements on QHP issuers.</p> <p>A QHP issuer must comply with all requirements of this subpart on an ongoing basis. QHP issuers must comply with any Exchange processes, procedures, and standards set forth under subpart K of part <u>155</u> and <u>\$155.705</u> for the small group market.</p> <p>A QHP issuer must ensure that each QHP it offers complies with the benefit design standards defined in <u>\$156.20</u>. The levels of coverage that are a component of these benefit design standards will be the subject of future rulemaking.</p> <p>A QHP issuer must be licensed and in good standing in each State in which it offers health insurance coverage.</p> <p><i>HHS interprets the term "good standing" to mean that the issuer has no outstanding sanctions imposed by the Department of Insurance. HHS seeks comments on this interpretation.</i></p> <p>A QHP issuer must comply with quality standards established in and pursuant to sections 1311(c)(1), (c)(3), (c)(4), and (g) of PPACA. These requirements will be addressed in future rulemaking.</p> <p>A QHP issuer must adhere to additional proposed requirements, including user fees described in <u>\$156.50</u>, if applicable, and the risk adjustment participation requirements in 45 CFR 153.</p> <p>Each QHP issuer must offer at least one QHP in the silver coverage level and one QHP in the gold coverage level. Any QHP issuer offering a non-catastrophic health plan in the Exchange must offer the identical plan as a child-only health plan, available only to individuals under age 21.</p> <p>A QHP issuer must offer a QHP at the same premium rate consistent with the requirements of <u>\$156.255(b)</u>.</p> <p>QHP issuers must adhere to the requirements of this subpart and any additional participation standards that may be applied by the Exchange or the State.</p> <p>QHP issuers must not discriminate based on race, color, national origin, disability, age, sex, gender identity and sexual orientation.</p>	

Section	Summary	Questions/Comments
§156.210-QHP rate and benefit information	<p>A QHP's rates must be applicable for an entire benefit year or, for the SHOP, plan year as described in <u>§156.285</u>.</p> <p>A QHP issuer must submit rate and benefit information to the Exchange as described in <u>§155.1020(c)</u>.</p> <p>A QHP issuer must submit a justification for a rate increase prior to its implementation. <i>HHS is considering a standard in which issuers will submit a rate justification in the form and manner determined by the Exchange.</i></p> <p>QHP issuers must post the rate justifications on their websites. <i>HHS is considering whether it should develop standards for "prominently posting" rate increase justifications.</i></p>	
§156.220-Transparency in coverage	<p>In order to receive and maintain certification, issuers must make available to the public and submit to the Exchange, the Secretary of HHS, and the State insurance Commissioner information, including:</p> <ul style="list-style-type: none"> • Claims payment policies and practices; • Periodic financial disclosures; • Data on enrollment; • Data on disenrollment; • Data on the number of claims that are denied; • Data on rating practices; • Information on enrollee rights under title I of PPACA; <p><i>HHS clarifies that, while the statute refers to "enrollee and participant rights, it believes that its definition of "enrollee" is inclusive of those who may be considered "participants." HHS seeks comment on whether issuers should be required to submit this information to the Exchange and other entities, or to make such information available to the Exchange and other entities.</i></p> <p>Issuers must submit the above information in plain language. Use of plain language should be consistent with the definition in <u>§155.20</u> and future guidance.</p> <p>QHP issuers must make available, in a timely manner through a website or other means, to the enrollee information on cost-sharing responsibilities for a specific service by a participating provider under the enrollee's plan.</p>	
§156.225-Marketing of QHPs	<p>QHP issuers must comply with applicable State laws and regulations regarding marketing by health insurance issuers.</p> <p>QHP issuers may not employ marketing practices that have the effect of discouraging enrollment of individuals with significant health needs. <i>HHS seeks comment on the best means for an Exchange to monitor QHP issuers' marketing practices to determine whether they have discouraged enrollment of individuals with significant health needs.</i></p>	

Section	Summary	Questions/Comments
	<p><i>HHS seeks comment on also applying a broad prohibition against unfair or deceptive marketing practices by all QHP issuers and their officials, agents or representatives. Such a requirement would protect consumers from deceptive and misleading marketing practices and allow an Exchange to take action to address such practices if the State's Department of Insurance or applicable State agency did not have the authority or capacity to do so under applicable law. HHS is particularly concerned that QHPs may be marketed towards certain vulnerable populations, such as Medicare beneficiaries, for whom coverage from a QHP would not be necessary.</i></p> <p><i>They seek comment on a standard that QHP issuers do not misrepresent the benefits, advantages, conditions, exclusions, limitations or terms of a QHP.</i></p>	
§156.230-Network adequacy standards	<p>QHP issuers must maintain networks for QHPs that include essential community providers in accordance with <u>§156.235</u>.</p> <p>QHP issuers must maintain networks that comply with any network adequacy standards established by the Exchange consistent with <u>§155.1050</u>.</p> <p>QHP issuers must ensure that the provider network of its QHPs is consistent with 2702(c) of PHSA, as amended by PPACA, consistent with PPACA 1311(c)(1)(B). This provision provides an exception to guaranteed issue requirements if the individual lives outside the plan's service area, or if the issuer does not have the capacity to serve the individual because of its existing obligations to enrollees. This exception must be applied uniformly across all employees or enrollees without regard to claims experience or health status.</p> <p>A QHP issuer must make its health plan provider directory available to the Exchange electronically and to potential enrollees and current enrollees in hard copy upon request. Issuers must note providers in the directory that are not accepting new patients.</p> <p><i>Exchanges will have discretion to determine the best way to get potential enrollees access to provider directories, including through a link to the issuer R's website, or by establishing a consolidated provider directory through which a patient may search for providers across QHPs.</i></p> <p><i>HHS seeks comments on standards it might set to ensure that QHP issuers maintain up-to-date provider directories.</i></p>	
§156.235-Essential community providers	<p>QHP issuers must maintain networks that include a sufficient number of essential community providers, where available, that serve low-income, medically underserved individuals. Nothing in this requirement shall be construed to require any QHP to provide coverage for any specific medical procedures.</p> <p><i>HHS interprets this to mean that while a QHP issuer must contract with essential community providers, coverage of specific services or procedures performed by an essential community provider is not required.</i></p>	

Section	Summary	Questions/Comments
	<p><i>HHS seeks comments on how to define a sufficient number of essential community providers.</i></p> <p><i>HHS is considering whether to provide separate consideration for integrated delivery network health plans where services are provided solely "in-house". They seek comment on whether it should create an exemption for these plans, which could be contingent upon the organization meeting other criteria, such as evidence of services provided to low income populations, compliance with standards for culturally and linguistically appropriate services or implementation of a plan to address health disparities.</i></p> <p>Essential community providers are defined to include providers that are eligible for 340B drug pricing. These providers include:</p> <ul style="list-style-type: none"> • Consolidated Health Centers (FQHC) • AIDS clinics and drug purchasing programs • Black Lung Clinics • Hemophilia Treatment Centers • Urban Indian Clinics • Tribal Centers • Family Planning Clinics • Sexually Transmitted Disease Clinics • Tuberculosis Clinics • Native Hawaiian Health Center • Federally Qualified Health Center look-a-likes • Certain Disproportionate Share Hospitals <p><i>HHS solicits comments on the extent to which the definition should include other similar types of providers that serve predominantly low-income, medically underserved populations and furnish the same services as the providers referenced in PHSA section 340B(a)(4).</i></p> <p><i>HHS notes that there may be a conflict between two provisions of PPACA regarding the payment of essential community providers and FQHCs. 1311(c)(2) provides that nothing shall be construed to require a QHP to contract with an essential community provider that refuses to accept the generally applicable payment rates of the plan. 1302(g), however, requires that a QHP reimburse FQHCs at each facility's Medicaid prospective payment system rate, which are paid on a per-encounter basis and may be higher than the rates the QHP pays to other providers. HHS invites comment on the issue of FQHC payment.</i></p> <p><i>HHS seeks comment on establishing requirements regarding reimbursement of Indian health providers. The Indian Health Care Improvement Act allows these providers to recover from third-party payers up to the reasonable charges billed for providing</i></p>	

Section	Summary	Questions/Comments
	<i>services, or the highest amount the insurer would pay to other providers, if higher. This requirement applies whether or not there is a contract between the provider and the insurer. HHS believes this requirement applies to QHPs and seeks comment on how it might be reconciled with the essential community provider provision. HHS also seeks comment on other special accommodations that must be made when contracting with Indian health providers, including a possible contract addendum similar to one used by Medicare Part D plans, which would minimize potential disputes and legal challenges when contracting with Indian health providers.</i>	
§156.245-Treatment of direct primary care medical homes	A QHP may provide coverage through a direct primary care medical home that meets requirements to be specified by HHS. <i>HHS interprets the term "direct primary care medical home plan" to mean an arrangement where a fee is paid by an individual, or on behalf of an individual, directly to a medical home for primary care services, consistent with the program established in Washington state. HHS requests comment on what standards it should establish under this section.</i>	
§156.250-Health plan applications and notices	QHP issuers must adhere to the standards established for notices in §155.230(b).	
§156.255-Rating variations	A QHP issuer may vary premiums by the rating areas established by the States under PHSA 2701(a)(1)(A). Each QHP issuer must offer a QHP at the same premium rate without regard to whether the plan is offered through an Exchange or whether it is offered directly from the issuer or through an agent. <i>HHS interprets this provision to mean that an issuer must charge a premium that uses underlying rating assumptions that account for all expected enrollees of a QHP, including individuals who enroll in the QHP outside of the Exchange.</i> Issuers may vary premiums among no more than 4 different types of family composition: <ul style="list-style-type: none"> • Individual • Two adults • Adult plus child • Family <p>Issuers must cover all of these categories, but in doing so may combine two or more of them.</p> <p><i>HHS seeks comment on how it might structure family rating categories while adhering with PHSA 2701(a)(4), which requires that age and tobacco rating factors may only be applied to the portion of the premium that is attributable to each family member.</i></p> <p><i>HHS seeks comment on how to structure family rating categories when performing risk adjustment.</i></p> <p><i>HHS seeks comment on alternatives to four categories for defining family composition.</i></p>	

Section	Summary	Questions/Comments
§156.260-Enrollment periods for qualified individuals	<p><i>HHS is considering whether to require QHP issuers to cover an enrollee's tax household, including for purposes of applying individual and family rates because of the potential challenge of administering the premium tax credit for families with non-spousal adult dependents. QHP issuers would not be required to cover dependents outside of the Exchange service area. They seek comment on the potential considerations of this approach.</i></p> <p>QHP issuers must accept and enroll qualified individuals during the initial open enrollment period described in §155.410(f) and during the annual open enrollment period described in §155.410(e). QHP issuers must accept and enroll qualified individuals if they are granted a special enrollment period described in §155.420.</p> <p>QHP issuers must adhere to the coverage effective dates established in §155.410(c), §155.410(f), and §155.420.</p> <p>QHP issuers must provide enrollees with notice of their effective date of coverage corresponding with the effective dates established above.</p>	
§156.265-Enrollment process for qualified individuals	<p>QHP issuers must adhere to the Exchange's process for enrollment in QHPs, which includes standards for the collection and transmission of enrollment information.</p> <p>QHP issuers must use the application adopted pursuant to §155.405 when accepting applications from individuals seeking to enroll in a QHP through the Exchange enrollment process.</p> <p>After collecting the uniform enrollment information from an applicant, the QHP issuer must send it to the Exchange, in accordance with the standards in §155.260 and, as applicable §155.270. The issuer may enroll an applicant in a QHP only after it has received a confirmation from the Exchange that the eligibility determination is complete and the applicant is a qualified individual. Issuers must receive enrollment information from the Exchange in a format and manner that is consistent with the standards established pursuant to §155.260 and §155.270.</p> <p><i>HHS seeks comment on the frequency with which plans should receive electronic enrollment information.</i></p> <p>QHP issuers must abide by the premium payment process established by the Exchange and described in §155.240.</p> <p>QHP issuers must provide enrollees with an enrollment packet.</p> <p><i>HHS plans to issue standards for the content of the enrollment information package, which may include an enrollment card, information on how to access care, the summary of benefit and coverage document, and information on how to access the provider</i></p>	

Section	Summary	Questions/Comments
	<p><i>directory and drug formulary. They request comment on the appropriateness of these documents or information that should be included in an enrollment information package.</i></p> <p>QHP issuers must provide the summary of benefits and coverage document to qualified individuals. QHP issuers must reconcile enrollment files with the Exchange no less than once a month, consistent with <u>§155.400(d)</u>.</p> <p>QHP issuers must acknowledge the receipt of enrollment information in accordance with Exchange standards established in <u>§155.400(b)(2)</u>.</p>	
<p>§156.270-Termination of coverage for qualified individuals</p>	<p>A QHP issuer may only terminate coverage as permitted by the Exchange in accordance with <u>§155.430(b)</u>.</p> <p>QHP issuers must provide a notice of termination of coverage to the enrollee and the Exchange that is consistent with the standards for effective dates in <u>§155.430(d)</u>.</p> <p><i>HHS plans to issue standards for the termination of coverage notice, which may include content such as reason for termination and termination effective date. They solicit comment on other information that should be included in the termination notice.</i></p> <p>QHP issuers must develop a uniform policy as permitted by the Exchange for the termination of coverage due to non-payment of premium in accordance with <u>§155.430(b)(2)(iii)</u>.</p> <p>QHP issuers must grant a three month grace period for enrollees who receive subsidies through the Exchange and who have paid at least one month's worth of premium. During this period, the issuer must continue to pay all appropriate claims submitted on behalf of the enrollee. If an enrollee is more than one month behind on payments, any payment paid to the QHP issuer will be applied to amounts associated with the first billing cycle in which the enrollee was delinquent. The grace period will reset only when the individual has fully paid all outstanding premiums. During the grace period, the issuer will continue to receive subsidy payments on the delinquent enrollee's behalf from the Treasury.</p> <p>QHP issuers must provide notice to all enrollees who are delinquent on premium payments.</p> <p><i>HHS plans to issue standards for content and timing of the notice. They seek comments on the potential required elements of the notice, such as the total amount of delinquent payment, possible date of coverage termination and payment options, and the timing and frequency with which such a notice should be provided to enrollees.</i></p> <p>If an enrollee receiving subsidies exhausts the grace period without submitting any premium payment, the issuer may terminate their coverage effective at the completion of the three month period. This termination must be preceded by the appropriate notice as referenced above.</p> <p>QHP issuers must maintain records of termination of coverage in accordance with Exchange standards established in <u>§155.430(c)</u>.</p>	

Section	Summary	Questions/Comments
	QHP issuers must abide by effective dates for termination of coverage as described in §155.430(d).	
§156.275-Accreditation of QHP issuers	<p>A QHP issuer must be accredited on the basis of local performance in each of the following categories:</p> <ul style="list-style-type: none"> • Clinical quality measures, such as HEDIS; • Patient experience ratings on a standardized Consumer Assessment of Healthcare Providers and Systems survey; • Consumer access; • Utilization management; • Quality assurance; • Provider credentialing; • Complaints and appeals; • Network adequacy; and • Patient information programs <p><i>HHS clarifies that they interpret "local performance" to mean the performance of the issuer in the State in which it is licensed.</i></p> <p><i>HHS will provide the standards by which it will recognize accrediting entities in future rulemaking. They seek comments on these standards.</i></p> <p>A QHP issuer must authorize the accrediting entity to release certain materials related to the accreditation to the Exchange and HHS.</p> <p>A QHP issuer must obtain its accreditation within the time period established by the Exchange under §155.1045.</p> <p>A QHP must comply with any State law that prohibits abortion coverage in QHPs.</p> <p>Nothing in title I of PPACA shall be construed to require a QHP issuer to provide coverage of elective abortion services as part of the essential benefits.</p> <p>If a QHP provides coverage for elective abortion services, the QHP issuer must not use any subsidy funds to pay for those services. It must collect a separate payment from each enrollee equal to the actuarial value of coverage of these services. These payments must be deposited into a separate aggregation account. If QHP premiums are paid through a payroll deposit, the separate payment shall be paid by a separate deposit.</p> <p>A QHP issuer must comply with the efforts or direction of the state health insurance Commissioner to ensure compliance with this section.</p> <p>A QHP issuer who provides coverage for elective abortion services must provide notice of such to enrollees, only through the summary of benefits and coverage document at the time of enrollment.</p>	
§156.280-Segregation of funds for abortion services		

Section	Summary	Questions/Comments
	<p>The above notice, marketing materials, and any information provided by the Exchange and specified by HHS must provide information only with respect for the total combined premium for the QHP.</p> <p>No QHP may discriminate against any individual health care provider or facility because of its unwillingness to provide, pay for, or refer for abortions.</p>	
<p>\$156.285-Additional standards specific to SHOP</p>	<p>A QHP issuer must accept aggregated payment of premiums from the SHOP in accordance with <u>\$155.705(b)(4)</u> and must abide by the rate setting timeline established by the SHOP in <u>\$155.705(b)(5)</u>. QHP issuers must charge the same contract rate for a plan year.</p> <p>QHP issuers must accept and enroll applicants during the rolling initial enrollment period and special enrollment periods for a SHOP established in <u>\$155.725</u> and in <u>\$155.420</u> with the exception of the special enrollment periods for a change in immigration status or a change in subsidy eligibility.</p> <p>QHP issuers must abide by the effective dates of coverage established in <u>\$155.410(c)</u>. <i>HHS is considering whether to require QHPs in the SHOP to allow employers to offer dependent coverage. They solicit comment on this potential requirement.</i></p> <p>QHP issuers must abide by the SHOP enrollment process and timeline established pursuant to <u>\$155.720(b)</u> and accept electronic transmission of enrollment information from the SHOP in accordance with <u>\$155.260</u> and <u>\$155.270</u>. Issuers must provide all new enrollees with the enrollment information package as described in <u>\$156.265(e)</u> and must provide qualified employers and employees with the summary of cost and coverage document in accordance with <u>\$156.265(f)</u>.</p> <p>QHP issuers must reconcile enrollment files with the SHOP at least monthly. And abide by the SHOP standards for acknowledgement of the receipt of enrollment information. QHP issuers must issue qualified employees a policy that aligns with the employer's plan year.</p> <p>QHP issuers must abide by the general requirements regarding termination of coverage in <u>\$155.270(a)</u> and must provide qualified employers and employees with a notice of termination of coverage of enrollees and QHP non-renewal, as described in <u>\$156.270(a)</u> and <u>\$156.290(b)</u>. If the employer chooses to stop participating in SHOP, a QHP issuer must terminate all enrolled qualified employees.</p>	
<p>\$156.290-Non-renewal and decertification of QHPs</p>	<p>A QHP issuer must notify the Exchange of a decision to not seek recertification prior to the beginning of the recertification process adopted by the Exchange pursuant to <u>\$155.1075</u> and must continue covering benefits for each enrollee until the completion of the benefit year or plan year for the SHOP. A QHP issuer must continue providing the Exchange with reporting information for the benefit or plan year even after withdrawing its QHP from the Exchange. The issuer must provide written notice of the non-renewal to each enrollee of the QHP and terminate coverage for enrollees in accordance with the requirements in <u>\$156.270</u>.</p>	

Section	Summary	Questions/Comments
	<p><i>HHS will issue future guidance regarding the timing and content of the notice. They solicit comment on the potential content of the non-renewal notice and any other information they should consider including.</i></p> <p>If an Exchange decertifies a QHP, the issuer must terminate coverage for the QHP enrollees only after the Exchange has notified them as described in <u>§155.1080</u> and enrollees have had the opportunity to enroll in other coverage.</p> <p><i>HHS seeks comment on the extent to which enrollees should continue to receive coverage from a decertified plan, even if it is for only a short period of time.</i></p>	
<p>§156.295-Prescription drug distribution and cost reporting</p>	<p>A QHP issuer must report the following information to HHS in a form and manner to be determined by HHS:</p> <ul style="list-style-type: none"> • The percentage of all prescriptions that were provided under the contract through retail pharmacies compared to mail order pharmacies • The percentage of prescriptions for which a generic was available and dispensed, broken down by pharmacy type, that is paid by the QHP issuer or PBM under the contract; • The aggregate amount, and the type of rebates, discounts, or price concessions that the PBM negotiates that are attributable to patient utilization under the plan • The aggregate amount of the rebates, discounts, or price concessions that are passed through to the plan sponsor • The total number of prescriptions that were dispensed; and • The aggregate amount of the difference between the amount the QHP issuer pays the PBM and the amounts that the PBM pays retail pharmacies, and mail order pharmacies. <p><i>HHS anticipates issuing guidance on these requirements and seeks comment on how a QHP issuer whose contracted PBM operates its own mail-order pharmacy can meaningfully report on the aggregate difference between what the issuer pays the PBM and what the PBM pays the mail order pharmacy.</i></p> <p><i>HHS seeks comment on potential definitions for "rebates," "discounts" and "price concessions", they are considering using the term "direct and indirect remuneration" to encompass these various arrangements.</i></p> <p><i>HHS interprets statutory references to PBMs to include any entity that performs activities such as prescription drug claims processing, negotiation with prescription drug manufacturers, the development and maintenance of pharmacy networks and the distribution of prescription drugs on behalf of a QHP issuer. They seek comment on this interpretation and whether they should define PBMs as such in this section.</i></p> <p>The information reported above is confidential and shall not be disclosed by HHS or by a QHP receiving the information, except that HHS may disclose it in a de-identified format that does not disclose prices paid for prescription drugs in order to report it to GAO or CBO.</p>	

Section	Summary	Questions/Comments
	A QHP issuer that does not provide HHS with the above information or knowingly provides false information the issuer will be subject to a fine that would increase \$10,000 for each day the information is not provided or \$100,000 for each piece of false information provided.	

Privacy Standards for Non-Exchange Entities Under the Affordable Care Act

QHP Certification Webinar Series

May 23, 2013

Centers for Medicare & Medicaid Services (CMS)

Center for Consumer Information & Insurance Oversight (CCIIO)



Agenda

- ▶ Introduction
- ▶ Background
- ▶ Privacy Standards
- ▶ Compliance Guidance for Federally-facilitated Exchange (FFE)
Privacy Standards
- ▶ Additional Resources
- ▶ Closing Remarks



Session Guidelines

- ▶ This is a 90-minute webinar session
- ▶ As time allows, there will be three Q & A sessions throughout the session
- ▶ Documented Q & A responses will be posted in the coming weeks
- ▶ For questions regarding content or logistics, contact the REGTAP Registrar at (b)(6) @regtap.info or (b)(6)



Privacy Standards for Non-Exchange Entities Under the Affordable Care Act

INTRODUCTION



Introduction

- ▶ Centers for Medicare & Medicaid Services (CMS), Center for Consumer Information & Insurance Oversight (CCIIO) speakers:
 - Karen Mandelbaum, JD, MHA
 - Julia Cassidy, JD



Objectives

- ▶ Define Personally Identifiable Information (PII)
- ▶ Describe privacy standards that govern PII in the Federally-facilitated Exchange* (FFE)
- ▶ Share strategies for achieving and maintaining compliance with FFE privacy standards
- ▶ Identify resources

*The terms "Exchange" and "Marketplace" may be used interchangeably during this session to describe the new health insurance markets created through the Affordable Care Act.



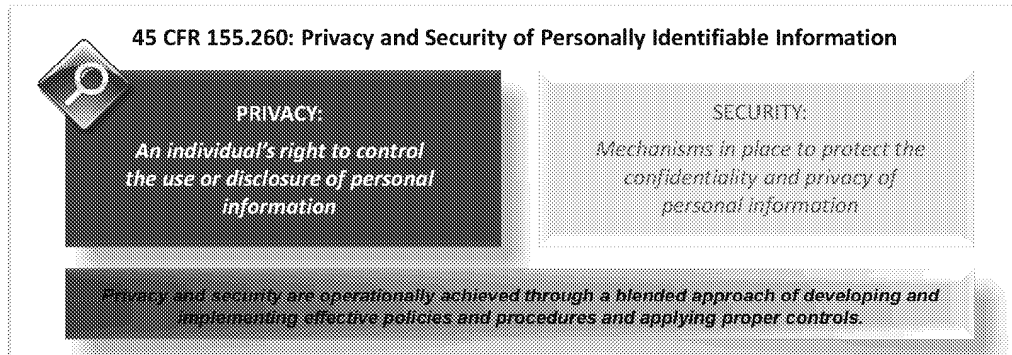
Privacy Standards for Non-Exchange Entities Under the Affordable Care Act

BACKGROUND



Privacy and Security in the Exchanges

- ▶ Qualified Health Plan (QHP) Issuers must comply with all applicable federal and state privacy laws and regulations
- ▶ Section 155.260 of the Exchange regulations governs privacy and security requirements within the Exchanges



This webinar will NOT address:
Topics related to security, such as building secure systems or implementing safeguards and controls



Draft Alt Text:

Graphic highlighting the following text:

45 CFR 155.260: Privacy and Security of Personally Identifiable Information

Privacy: An individual's right to control the use or disclosure of personal information.

Security: Mechanisms in place to protect the confidentiality and privacy of personal information.

Privacy and security are operationally achieved through a blended approach of developing and implementing effective policies and procedures and applying proper controls.

Application of Section 155.260

- ▶ The privacy requirements in Section 155.260 apply to all Exchanges, including FFE and State-based Exchanges (SBE)
- ▶ Each Exchange must establish standards that are consistent with the principles outlined in Section 155.260(a)(3) of the regulation
- ▶ Section 155.260(b) obligates Exchanges to require the same or more stringent privacy and security standards as a condition of contract or agreement with 'non-Exchange entities' that:
 - Gain access to PII submitted to an Exchange
 - Collect, use, or disclose PII gathered directly from applicants, qualified individuals, or enrollees while operating under the terms of an agreement with the FFE
- ▶ Examples of non-Exchange entities: QHP Issuers, Navigators, Agents, and Brokers



Significance of FFE Privacy Requirements for Issuers

- ▶ Issuers and other stakeholders will gain access to new, non-traditional information (e.g., Federal Tax Information, information that determines eligibility)
 - This information must be protected according to the FFE privacy requirements
 - The QHP Issuer Agreement includes a provision that requires the issuer to comply with the FFE privacy standards in order for the issuer to offer health plans through the FFE



What is PII?

► Definition:

- Information which can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information which is *linked* or *linkable* to a specific individual*
- Examples: name, social security number, biometric records, date and place of birth, mother's maiden name, email address, health information

► Special categories under the ACA:

- Applicant PII
- Federal Tax Information

PII Lifecycle



*Office of Management Budget (OMB) Memorandum M-07-16



Draft Alt Text:

Graphic showing the PII lifecycle:

Creation

Collection

Use

Disclosure

Disposal

10

Privacy Laws That Govern PII

- ▶ PII is governed by federal and state privacy laws
- ▶ Issuers must understand and comply with all legal obligations to protect PII
- ▶ Examples of laws that govern PII include:
 - Privacy Act of 1974
 - Health Insurance Portability and Accountability Act (HIPAA)
 - Internal Revenue Code (IRC) 6103
 - Federal Medicaid/CHIP Privacy Rules
 - State Privacy Laws
- ▶ Existing knowledge and resources can be adapted and leveraged to comply with the Exchange privacy standards

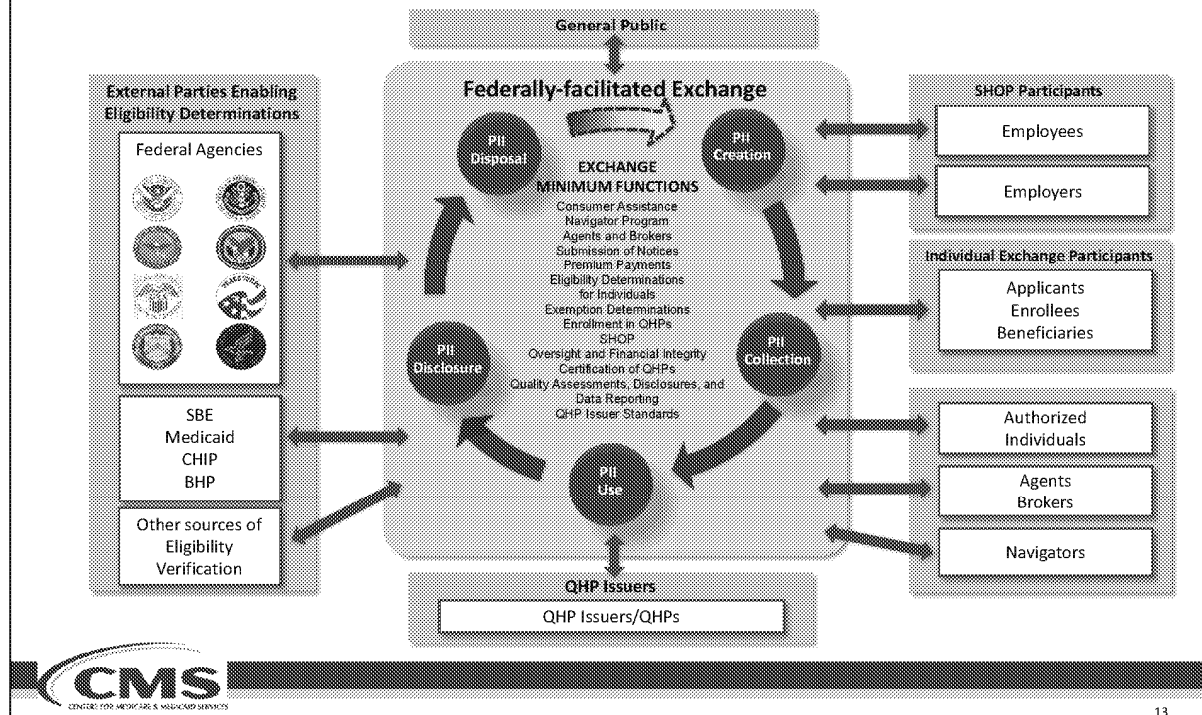


Exchange Minimum Functions That Involve PII

- | | |
|------------------------------------------------------|----------------------------------------------------------|
| 1. Consumer Assistance | 9. Small Business Health Options Program (SHOP) |
| 2. Navigator Program | |
| 3. Agents and Brokers | 10. Oversight and Financial Integrity |
| 4. Submission of Notices | 11. Certification of QHPs |
| 5. Premium Payments | 12. Quality Assessments, Disclosures, and Data Reporting |
| 6. Eligibility Determinations for Individuals | |
| 7. Exemption Determinations | 13. QHP Issuer Standards |
| 8. Enrollment in QHPs | |



Complexity of PII Flow in the Exchanges



13

Draft Alt Text:

Picture to provide a visual representation of PII flow in the Exchanges:

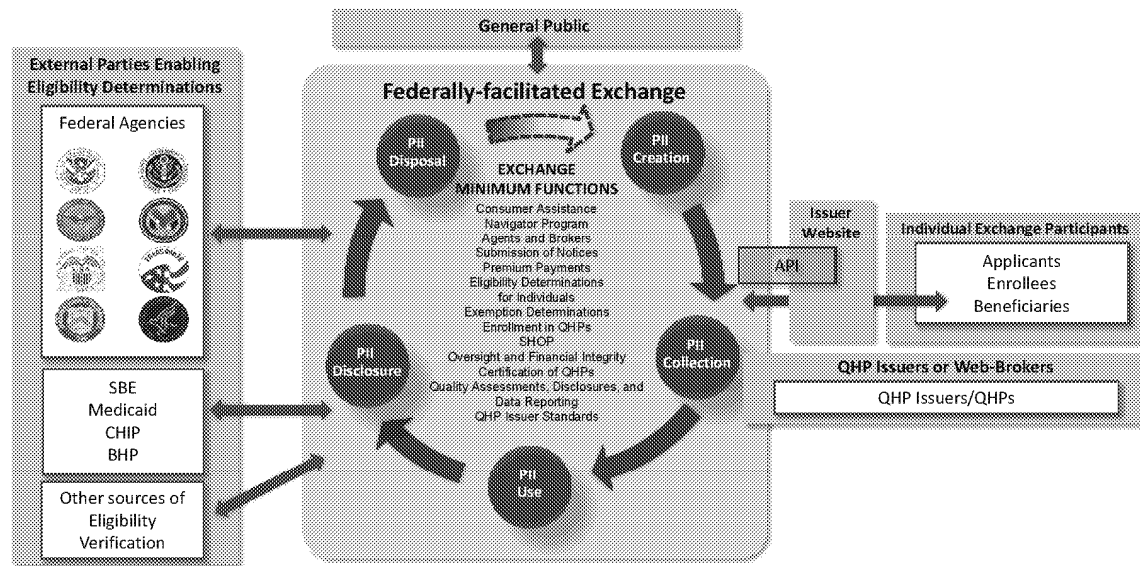
- General Public
- External Parties Enabling Eligibility Determinations
 - Federal Agencies
 - SBE
 - Medicaid
 - CHIP
 - BHP
 - Other sources of Eligibility Verification
- QHP Issuers
 - QHP Issuers/QHPs
- SHOP Participants
 - Employees
 - Employers
- Individual Exchange Participants
 - Applicants
 - Enrollees
 - Beneficiaries
- Authorized Individuals
- Agents/Brokers
- Navigators

All of the above link to the Federally-facilitated Exchange. Within the PII lifecycle (Creation, Collection, Use, Disclosure,

Disposal) there are Exchange Minimum Functions:

- Consumer Assistance
- Navigator Program
- Agents and Brokers
- Submission of Notices
- Premium Payments
- Eligibility Determinations for Individuals
- Exemption Determinations;
- Enrollment in QHPs
- SHOP
- Oversight and Financial Integrity
- Certification of QHPs
- Quality Assessments, Disclosures, and Data Reporting
- QHP Issuer Standards

Application Program Interface (API) Connection



Draft Alt Text:

Picture to provide a visual representation of the Application Program Interface (API) Connection:

- General Public
- External Parties Enabling Eligibility Determinations
 - Federal Agencies
 - SBE
 - Medicaid
 - CHIP
 - BHP
 - Other sources of Eligibility Verification
- QHP Issuers or Web-Brokers
 - QHP Issuers/QHPs
- Issuer Website
- API
- Individual Exchange Participants
 - Applicants
 - Enrollees
 - Beneficiaries

All of the above link to the Federally-facilitated Exchange. Within the PII lifecycle (Creation, Collection, Use, Disclosure, Disposal) there are Exchange Minimum Functions:

- Consumer Assistance
- Navigator Program
- Agents and Brokers

- Submission of Notices
- Premium Payments
- Eligibility Determinations for Individuals
- Exemption Determinations;
- Enrollment in QHPs
- SHOP
- Oversight and Financial Integrity
- Certification of QHPs
- Quality Assessments, Disclosures, and Data Reporting
- QHP Issuer Standards

QUESTIONS?



Privacy Standards for Non-Exchange Entities Under the Affordable Care Act

PRIVACY STANDARDS



Privacy Standards

- ▶ Privacy regulations protect PII in the Exchanges
- ▶ Privacy standards are based on principles from Section 155.260(a)(3)

Privacy Standards

- Creation, Collection, Use, and Disclosure
- Individual Access and Correction
- Openness and Transparency
- Individual Choice
- Data Quality and Integrity
- Accountability
- Safeguards



Creation, Collection, Use, and Disclosure

- ▶ PII cannot be used or disclosed for purposes other than those under the terms of the QHP Issuer Agreement
 - A record of disclosures must be maintained
- ▶ Applicant PII is limited to those elements included on the “streamlined application”
- ▶ Federal Tax Information can be used/disclosed only in accordance with 6103 of the IRS Code and IRS Publication 1075

Final Rule Citations: 155.260(a)(1), 155.260(a)(2), 155.260(a)(3)(v), 155.260(f), 155.260(g)



Individual Access and Correction

- ▶ Individuals whose PII has been collected as part of the eligibility and enrollment process have the right to access their PII in a timely manner and dispute and correct any erroneous information
- ▶ Requests for correction of information obtained by the FFE from a source other than the subject of the PII must be made to the source agency that originally provided the information to the FFE
- ▶ Documentation of denied correction requests must be maintained

Final Rule Citations: 155.260(a)(3)(i), 155.260(a)(3)(ii)



Openness and Transparency

- ▶ If an issuer wishes to obtain an individual's PII, the issuer must inform the individual about the policies, procedures, and technologies that would directly affect the individual and their PII
- ▶ The issuer must disclose the following information to an individual about the handling of their PII:
 - Why the information is needed
 - What it will be used for
 - To whom it will be disclosed
 - The authority under which the information is being collected
 - Whether the collection is mandatory or voluntary and what the effect is if the individual decides not to provide the information
 - How it will be secured
 - How long it will be retained

Final Rule Citation: 155.260(a)(3)(iii)



Individual Choice

- ▶ Individuals have the right to make informed decisions about the collection, use, and disclosure of their PII
 - A non-Exchange entity assisting an individual in obtaining an eligibility determination or enrolling individuals in a QHP must obtain authorization prior to obtaining PII
 - The non-Exchange entity providing assistance must keep a record of the authorization provided
 - Individuals must be able to revoke authorization at any time

Final Rule Citation: 155.260(a)(3)(iv)



Data Quality and Integrity

- ▶ Issuers must ensure all PII is accurate, complete, and up-to-date and has not been altered or destroyed in an unauthorized manner
- ▶ As non-Exchange entities, issuers must:
 - Verify the accuracy, completeness, and timeliness of PII at the time of collection
 - Process authorization of changes in a timely manner
 - Maintain an inventory of disclosures

Final Rule Citation: 155.260(a)(3)(vi)



Accountability

- ▶ Accountability means ensuring compliance with the Exchange privacy standards and legal agreements as well as establishing policies, procedures, and protocols for how the standards will be met
- ▶ QHP Issuers must develop policies and procedures based on the Exchange privacy standards
 - Training and awareness programs
 - Monitoring for non-adherence
 - Incident and breach reporting

Final Rule Citations: 155.260(a)(3)(viii), 155.260(c), 155.260(d)



Safeguards

- ▶ Appropriate operational, administrative, technical, and physical safeguards must be in place to ensure the confidentiality and integrity of PII
- ▶ Guidance for safeguards is provided through the Minimum Acceptable Risk Standards for Exchanges (MARS-E) suite of documents

Final Rule Citations: 155.260(a)(3)(vii), 155.260(a)(4), 155.260(a)(5), 155.260(a)(6)



QUESTIONS?

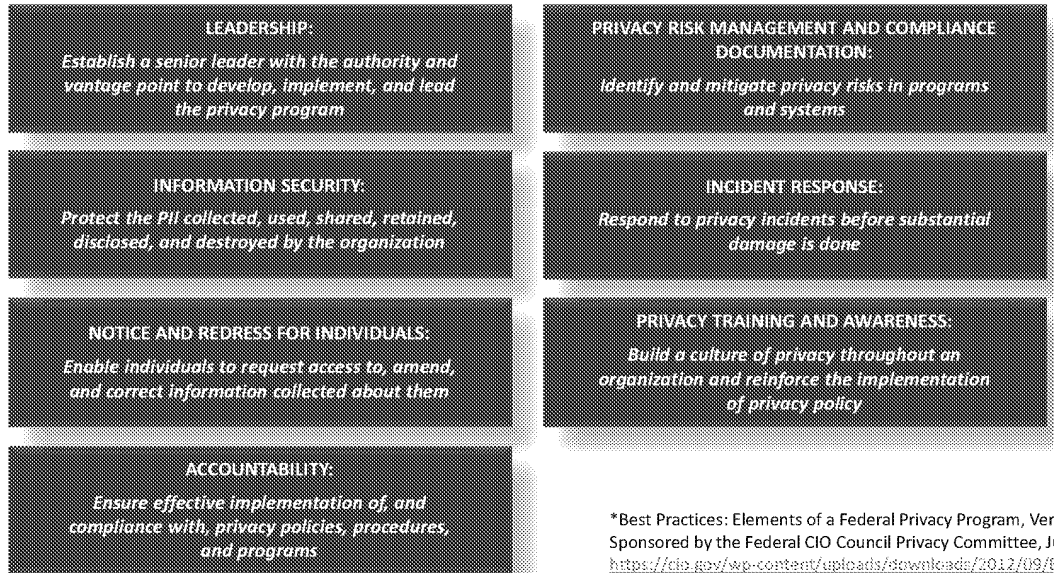


Privacy Standards for Non-Exchange Entities Under the Affordable Care Act

COMPLIANCE GUIDANCE FOR FFE PRIVACY STANDARDS



Best Practices* for Ensuring Compliance with Exchange Privacy Standards



*Best Practices: Elements of a Federal Privacy Program, Version 1.0, Sponsored by the Federal CIO Council Privacy Committee, June 2010, <https://cio.gov/wp-content/uploads/downloads/2012/09/Elements-Federal-Privacy-Program-v1.0-June-2010.pdf>



Draft Alt Text:

Graphic of text boxes to highlight best practices* for ensuring compliance with Exchange privacy standards:

LEADERSHIP: Establish a senior leader with the authority and vantage point to develop, implement, and lead the privacy program.

PRIVACY RISK MANAGEMENT AND COMPLIANCE DOCUMENTATION: Identify and mitigate privacy risks in programs and systems.

INFORMATION SECURITY: Protect the PII collected, used, shared, retained, disclosed, and destroyed by the organization.

INCIDENT RESPONSE: Respond to privacy incidents before substantial damage is done.

NOTICE AND REDRESS FOR INDIVIDUALS: Enable individuals to request access to, amend, and correct information collected about them.

PRIVACY TRAINING AND AWARENESS: Build a culture of privacy throughout an organization and reinforce the implementation of privacy policy.

ACCOUNTABILITY: Ensure effective implementation of, and compliance with, privacy policies, procedures, and programs.

Ongoing Compliance with Exchange Privacy Standards

- Privacy standards should be addressed as part of a comprehensive compliance program and documented in compliance plans required for QHP certification

Compliance Plan Element*	Corresponding Privacy-Related Question
Written Policies, Procedures, and Standards of Conduct	What are the privacy policies and procedures to be included in our organization's compliance plan?
Designation of a Compliance Officer and Compliance Committee	Who will be accountable for addressing privacy concerns in our organization?
Effective Training and Education	How will we train staff who handle PII?
Effective Lines of Communication	What are the processes for reporting privacy concerns or complaints? Is there a clear reporting structure in place?
Well-publicized Disciplinary Standards	What are staff/partner expectations for reporting noncompliance to privacy standards?
System for Monitoring and Identifying Compliance Risks	Is there a system for monitoring and identifying privacy risks, such as conducting self-assessments, to proactively address concerns?
Procedures and System for Prompt Response to Identified Issues	How will we respond to privacy complaints, security incidents, and/or breaches?

*For more information, reference 2/21/2013 webinar slides in the REGTAP Library, *Developing an Effective Compliance Plan*.



Application to Downstream Entities/Business Partners

- ▶ Any individual or entity who handles or gains access to PII must meet or exceed the privacy standards established by the FFE
 - The requirement is passed to any downstream entities (e.g., sub-contractors) via legal agreements
- ▶ Approaches to ensuring consistency among partners with regards to meeting or exceeding privacy standards include:
 - Contractor training
 - Agreement conditions
- ▶ Creating a dependable network of partner entities through legal agreements ensures a uniform commitment to a consistent baseline of privacy protections for individuals

Final Rule Citations: 155.260(b), 155.260(e)



Privacy Standards for Non-Exchange Entities Under the Affordable Care Act

ADDITIONAL RESOURCES



Resources for Issuers

► **IRC 6103**

Law governing FTI. Available at: <http://www.gpo.gov/fdsys/pkg/USCODE-2011-title26/pdf/USCODE-2011-title26-subtitleF-chap61-subchapB-sec6103.pdf>

► **Minimum Acceptable Risk Standards for Exchanges (MARS-E) suite of documents**

Additional guidance on Exchange privacy and security standards. Available at: <http://ccilo.cms.gov/resources/regulations/index.html>

► **HIPAA Privacy and Security Resources**

Additional detail and guidance on HIPAA. Available at: <http://www.hhs.gov/ocr/privacy/>

► **OMB Memorandum (M-07-16)**

Provides federal definition of PII. Available at: <http://www.gsa.gov/portal/content/104256>

► **45 CFR 155.260**

ACA Exchange Privacy Rule. Available at: <http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=fcb6289611917706b98a028e99e8c258&ty=HTML&h=L&r=PART&n=45y1.0.1.2.71#45:1.0.1.2.71.3.27.7>

► **CClIO Resources**

CClIO presentations, guidance, and regulations. Available at: <http://ccilo.cms.gov/resources/other/index.html> and <http://ccilo.cms.gov/resources/regulations/index.html#hie>



Forthcoming Guidance from CCIIO

- ▶ Regulation on privacy requirements for non-Exchange entities
- ▶ Supplemental privacy guidance for SBE

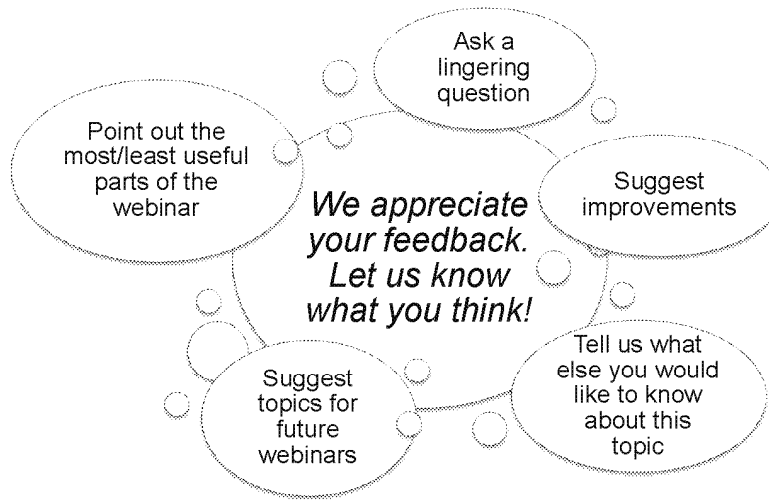


QUESTIONS?



Provide Feedback on Today's Webinar

- At the end of this call you will receive an email with a link where you can submit feedback on today's webinar



Draft Alt Text:

We appreciate your feedback. Let us know what you think!

Ask a lingering question

Suggest improvements

Tell us what else you would like to know about this topic

Suggest topics for future webinars

Point out the most/least useful parts of the webinar

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
Center for Consumer Information and Insurance Oversight
200 Independence Avenue SW
Washington, DC 20201



Date: [April 30, 2013]

Subject: Frequently Asked Questions on Health Insurance Marketplaces

Privacy and Security

Q1: Will CMS create additional security standards for SBMs and non-Marketplace entities such as Navigators, agents, and brokers?

A1: We intend to propose making compliance with the security standards that are defined in the Minimum Acceptable Risk Standards for Marketplaces (MARS-E) suite of documents a requirement for all SBMs and non-Marketplace entities associated with the FFM. The MARS-E suite of documents is posted on the CMS CALT website and is document 12248.

We also propose clarifying that the security standards apply to all information that is used for Marketplace functions, and not only to personally identifiable information.

Oversight of Premium Stabilization Programs, Advance Payments of the Premium Tax Credit, and Cost-sharing Reductions

Q2: What oversight measures does CMS intend to propose with respect to the premium stabilization programs, cost-sharing reductions, and advance payments of the premium tax credit?

A2: We intend to propose oversight measures related the premium stabilization programs. With respect to state-operated risk adjustment programs, we intend to propose a standard under which the state would maintain an accurate accounting for each benefit year of risk adjustment expenditures, receipts, and administrative expenses, and the state would provide to CMS and make public an annual summary of the program. We also intend to propose that each state-operated risk adjustment program provide for an annual external financial and programmatic audit, and maintain relevant records for ten years.

We intend to propose oversight standards applicable to states operating reinsurance that are substantially similar to those discussed above for state-operated risk adjustment. Finally, following further consultations with stakeholders, we intend to propose additional standards, including standards

INFORMATION NOT RELEASABLE TO THE PUBLIC UNLESS AUTHORIZED BY LAW:

This information has not been publicly disclosed and may be privileged and confidential. It is for internal government use only and must not be disseminated, distributed, or copied to persons not authorized to receive the information. Unauthorized disclosure may result in prosecution to the full extent of the law.

applicable to issuers, such as standards relating to risk adjustment data validation, to govern the oversight of the premium stabilization programs in future regulations and guidance.

With respect to advance payments of premium tax credit and cost-sharing reductions, we intend to propose standards for refunds to eligible enrollees when a QHP issuer incorrectly applies cost-sharing reductions or advance payments of the premium tax credits with respect to an enrollee. We also intend to propose ten year record retention and annual reporting standards.

Q3: How will CMS ensure that issuers of a risk-adjustment covered plan or reinsurance-eligible plan establish a distributed data environment?

A3: We intend to propose a framework for corrective actions and sanctions for noncompliance with distributed data standards by issuers of risk adjustment covered plans and reinsurance-eligible plans.

Issuer Oversight

Q4: How does the FFM intend to enforce issuers' ongoing compliance with Marketplace-specific standards?

A4: We note the traditional role of state departments of insurance in overseeing issuers in the health insurance market. As such, we intend to look to existing state compliance oversight and enforcement efforts for issues that fall under the states' regulatory and enforcement authority. We further note that coordination with state efforts will be important to avoid penalizing or investigating the same issuer more than once for the same issue. As mentioned in prior FAQs, (http://www.cciio.cms.gov/resources/factsheets/aca_implementation_faqs.html), we intend to continue assisting issuers to maintain compliance and to that end, we expect to release guidance related to our oversight approach in the near future.

Q5: Under what circumstances are issuers in the FFM subject to enforcement actions, including decertification of their QHPs?

A5: We envision a progressive approach and that any enforcement would take into consideration various factors, including any past or concurrent state determinations and indications of the issuer's good faith efforts in maintaining compliance with FFM-specific standards. We note the need to coordinate with states on issuer oversight to avoid duplicative enforcement or investigative actions for the same issue. We will generally look to the states to enforce standards applicable to issuers in the FFM. Where the state has elected not to enforce a standard or lacks the regulatory or enforcement authority to do so, we intend to propose enforcement of FFM-specific standards through civil money penalties (CMPs) and, in the most egregious cases, decertification. We believe that CMPs are an appropriate intermediary step prior to decertification, and we would reserve decertification for only the most egregious cases. Absent any extraordinary circumstances, we expect decertification to be

INFORMATION NOT RELEASABLE TO THE PUBLIC UNLESS AUTHORIZED BY LAW:

This information has not been publicly disclosed and may be privileged and confidential. It is for internal government use only and must not be disseminated, distributed, or copied to persons not authorized to receive the information. Unauthorized disclosure may result in prosecution to the full extent of the law.

uncommon, especially in 2014. We also intend for issuers to be able to appeal the issuance of CMPs or decertifications.

State-based Marketplace Reporting Requirements

Q6: Will SBMs be required to provide reports to CMS on Marketplace activities?

A6: Yes, we intend to propose requiring SBMs to report to CMS at least annually a financial statement, summary level statistical reports regarding eligibility determinations, enrollments, appeals, errors made in eligibility determinations, privacy and security safeguards, and fraud and abuse determinations. Additionally, we intend for SBMs to be required to submit performance monitoring data including financial sustainability, operational efficiency consumer satisfaction, and quality of care data.

Q7: Are there any recordkeeping requirements for SBEs?

A7: Yes, because CMS anticipates conducting a limited number of targeted audits each year, we intend to propose that SBMs will be required to maintain records from external audits, annual financial reports, error rate testing, consumer complaints and other data sources for a minimum of 10 years.

Q8: What types of audits will Marketplaces be required to conduct?

A8: We intend to propose that SBMs should expect to engage an independent qualified auditing entity to perform an independent audit of their annual financial statement and a review of the processes/internal controls associated with their eligibility determinations and enrollments. SBMs would provide the results of this financial and programmatic audit to CMS.

High Deductible Health Plans

Q9: How should plan variations for QHPs that are high-deductible health plans (HDHPs) designed to be paired with a health savings account (HSA) be structured?

A9: If an issuer seeks to offer an HDHP QHP designed to be eligible for pairing with an HSA in 2014, the issuer must comply with the cost-sharing reduction standards described in 45 CFR 156 subpart E. CMS recognizes that certain plan variations of an HDHP QHP may require a low or zero deductible, or that certain services be exempt from the deductible, which may result in the plan variation not being eligible to be offered in conjunction with an HSA. We recommend that issuers and Marketplaces educate consumers about this issue, both during open enrollment and when an individual has a change in eligibility for cost-sharing reductions. An individual who would not be eligible for the tax advantages of an HSA because the plan variation to which he or she would be assigned does not qualify as an HDHP may purchase the HDHP without cost-

INFORMATION NOT RELEASABLE TO THE PUBLIC UNLESS AUTHORIZED BY LAW:

This information has not been publicly disclosed and may be privileged and confidential. It is for internal government use only and must not be disseminated, distributed, or copied to persons not authorized to receive the information. Unauthorized disclosure may result in prosecution to the full extent of the law.

sharing reductions by not seeking income assistance on the Marketplace, or by purchasing the plan outside the Marketplace. If a QHP issuer chooses to offer an HDHP standard plan, with associated plan variations that are not eligible for pairing with an HSA, the QHP issuer should still select “yes” in the “HSA Eligible” field on the Plans & Benefits template.

Eligibility and Enrollment

Q10: What procedures will Marketplaces follow to determine eligibility when certain data are unavailable?

A10: In our January 22, 2013 proposed rule on eligibility, , published at 78 FR 4594, we specified that if electronic data were required for verification but it is not reasonably expected that such data sources would be available within two days of the initial attempt to reach the data source, the Marketplace would trigger an inconsistency period, during which the Marketplace would determine an applicant’s eligibility based on his or her attestation to the piece of information for which data could not be obtained, and provide the applicant with the opportunity to provide satisfactory documentation to the Marketplace or otherwise resolve the inconsistency.

Based on feedback and analysis, we intend to modify this provision in final rulemaking, such that if an application is submitted when data from the Internal Revenue Service (IRS), Social Security Administration (SSA), or Department of Homeland Security (DHS) is unavailable, and the data source is not reasonably expected to be available within one day of the initial request, the Marketplace would trigger an inconsistency period. This modification is based in part on our understanding that data from IRS, SSA, and DHS will be available seven days per week, with exceptions for unscheduled maintenance.

If other data sources are unavailable, such as data sources used in the verification of minimum essential coverage other than through an eligible employer-sponsored plan, we expect to clarify that the Marketplace will not delay the determination and instead, will accept the applicant’s attestation regarding the piece of information for which data is unavailable. We intend to closely monitor the availability of electronic data during the initial period of operations.

Q11: Is there additional flexibility available for Marketplaces to accept an attestation of projected annual household income without further verification?

A11: Yes. For October 1, 2013, when an attestation to projected annual household income is more than 10 percent below aggregated data from IRS and SSA, and current income data is unavailable, the Marketplace may choose to trigger the inconsistency process only for a statistically significant sample of the population that would otherwise be subject to such procedures, and accept the attestation of the remaining group. We expect that any Marketplace that takes this option will evaluate the results of the sample and adjust its size as needed to ensure that the verification process is effective.

INFORMATION NOT RELEASABLE TO THE PUBLIC UNLESS AUTHORIZED BY LAW:

This information has not been publicly disclosed and may be privileged and confidential. It is for internal government use only and must not be disseminated, distributed, or copied to persons not authorized to receive the information. Unauthorized disclosure may result in prosecution to the full extent of the law.

Q12: What services will CMS provide to help SBMs verify eligibility for individuals related to enrollment in an eligible employer-sponsored plan and eligibility for qualifying coverage in an eligible employer-sponsored plan for the first year of operations?

A12: In the Eligibility II proposed rule, we proposed that a SBM could rely on CMS for verification of enrollment in an eligible employer-sponsored plan and eligibility for qualifying coverage in an eligible employer-sponsored plan. Based on technology limitations, we expect to clarify that this service will not be available for October 1, 2013. Accordingly, for the first year of operations, CMS will not take any enforcement action against SBMs that are unable to independently implement the proposed provisions that involve contacting the employers of a statistically-significant sample of applicants, which we believe to be the challenging component of the proposed verification process. Further, we expect to modify the proposed rule to eliminate the requirement to utilize wage data as a component of this verification, since this data does not directly address employer-sponsored coverage. Consequently, for the first year of operations, SBMs will solely be responsible for checking Office of Personnel Management (OPM) data, which will be provided by CMS, and SHOP data. We intend to continue to work with SBMs to ensure that they can implement effective eligibility processes for October 1, 2013 and future years.

Q13: When can individuals and employees designate an individual or organization to act on that individual or employee's behalf for matters related to the Marketplace?

A13: Marketplaces will permit individuals and employees to designate an individual or organization to act on that individual or employee's behalf, or to have such a representative through operation of state law, subject to applicable privacy and security standards. The authorized representative would have the authority to act on behalf of this person for matters related to the Marketplace. Further, based on public comments, we expect to clarify in final regulations that subject to applicable state law, a QHP issuer will recognize an authorized representative who is designated through the process administered by the Marketplace. This is important to ensure that the vulnerable population that will utilize authorized representatives can complete the authorization process once. Further, we note that we expect that the process employed by the Marketplace will ensure that an authorized representative is properly designated, and the clarification regarding state law will ensure that additional requirements related to privacy and security are not superseded. Such authorized representatives will be identified to QHP issuers via the 834 enrollment transaction.

Q14: How should Marketplaces handle situations where individuals submit incomplete applications?

A14: While the online application will be structured to minimize the number of situations in which an individual will omit necessary information, individuals who use the paper application may errantly omit such information. In order to address this situation, we intend to clarify that if the Marketplace does not have enough information to determine an individual's eligibility for enrollment in a QHP

INFORMATION NOT RELEASABLE TO THE PUBLIC UNLESS AUTHORIZED BY LAW:

This information has not been publicly disclosed and may be privileged and confidential. It is for internal government use only and must not be disseminated, distributed, or copied to persons not authorized to receive the information. Unauthorized disclosure may result in prosecution to the full extent of the law.

through the Marketplace, APTC, or CSR, the Marketplace will request the missing information, and provide a period of 90 days before denying eligibility. During this period, an individual would not receive eligibility for enrollment in a QHP, APTC, or CSR, unless the individual has provided sufficient information to determine his or her eligibility for enrollment in a QHP through the Marketplace, in which case the Marketplace may make such a determination. After the necessary information has been received, the Marketplace would proceed with application processing.

Q15: What services will CMS provide to help SBMs make eligibility determinations for exemptions from the individual shared responsibility payment?

A15: In our February 1, 2013 proposed regulation regarding exemptions from the shared responsibility payment, published at 78 FR 7348 (“exemptions proposed rule”), we proposed that a Marketplace could be approved while relying on CMS to make eligibility determinations for exemptions from the shared responsibility payment, provided that the Marketplace accept applications, transmit the application information to CMS, receive the response from CMS, and issue the notice, including any certificate of exemption. Based in part on technology limitations, and also to reduce burden for SBMs, we intend to clarify that this “federally-managed service” will involve CMS taking applications, completing necessary verifications, determining eligibility, and issuing notices, including any certificate of exemption. In total, this means that a SBM may elect to have virtually no operational role in the exemption process, noting that SBMs will assist individuals seeking an affordability exemption based on projected annual household income by allowing such an individual to receive an eligibility determination for APTC and providing him or her with information regarding the cost of his or her lowest-cost bronze plan. We expect that this will not require any capability beyond what a SBM will otherwise maintain to support the general eligibility process.

Q16: Will Issuers be required to obtain a Health Plan Identifier (HPID) to conduct enrollment and payment transactions with the FFM?

A16: CMS intends to propose rulemaking and supplemental guidance on the use of HPIDs in enrollment and payment transactions between issuers and the FFM.

A standard for HPIDs was adopted by HHS in October 2011, and the system to enable insurance issuers to obtain an HPID has been available since March 28, 2013. All health plans are required to obtain HPIDs beginning November 7, 2014 (small plans have until November 2015). All covered entities health care clearinghouses, covered health care providers, and health plans are required to use HPIDs to identify health plans in standard transactions such as claims, referrals, and remittance advice by November 7, 2016.

Since it is permissible to obtain and use an HPID in advance of the mandatory compliance dates and to use the HPIDs outside the transaction (i.e., in the envelopes), beginning in October 2013,

INFORMATION NOT RELEASABLE TO THE PUBLIC UNLESS AUTHORIZED BY LAW:

This information has not been publicly disclosed and may be privileged and confidential. It is for internal government use only and must not be disseminated, distributed, or copied to persons not authorized to receive the information. Unauthorized disclosure may result in prosecution to the full extent of the law.

the FFM anticipates using the issuer's HPID for routing the electronic transactions correctly. The HPID will be used in the “envelope” of the enrollment and payment transactions to ensure that they successfully reach the right issuer or its designated trading partner. Issuers will be able to limit the number of HPIDs they obtain to only those needed for routing purposes to do business with the FFM. Each of the issuer's QHPs will be associated with an HPID, but the HPIDs need not be unique for each plan. An issuer could decide to obtain a single controlling HPID to be used for all transactions.

Third party entities, such as clearinghouses, are also able to obtain an Other Entity Identifier (OEID) at this time. If an issuer utilizes a third party, issuers would be able to use the OEID of the contracted party to identify where transactions would be routed.

For more information on HPID, visit <http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/Affordable-Care-Act/Health-Plan-Identifier.html>

Direct Enrollment

Q17: Will QHP issuers be permitted to enroll individuals directly in states where a Federally-facilitated Marketplace (FFM) is operating?

A17: Yes. 45 CFR 156.265(b)(2) establishes that a QHP issuer may directly enroll a qualified individual in a QHP, provided that the individual receives an eligibility determination through the Marketplace website. In states where FFMs are operating, CMS will support direct-to-issuer enrollment by making available an application programming interface, or API. The API will allow an applicant to approach a QHP issuer directly for enrollment through the Marketplace. To ensure compliance with 45 CFR 156.265(b)(2), the applicant will be securely redirected from the issuer's website to the Marketplace website to complete the eligibility application. The Marketplace will determine the individual's eligibility for enrollment in a QHP, and for any financial assistance. Once the applicant's eligibility determination is complete, the consumer will be securely redirected back to the issuer's website to shop for and select a QHP. The Marketplace will serve as the system of record for all enrollment transactions, including those that occur directly with the issuer.

CMS intends to propose in future rulemaking additional protections for qualified individuals who enroll directly with QHP issuers. Specifically, CMS intends to propose that QHP issuers offering direct enrollment inform the applicant that other coverage options are available via the Marketplace website; that issuers display QHPs separately from non-QHPs or ancillary products; and that QHP issuers display the same plan data as the Marketplace. In addition, CMS expects to require QHP issuers to mirror key aspects of the Marketplace consumer experience (e.g., a consumer's ability to change his/her APTC election or organize his/her family into multiple enrollment groups).

INFORMATION NOT RELEASABLE TO THE PUBLIC UNLESS AUTHORIZED BY LAW:

This information has not been publicly disclosed and may be privileged and confidential. It is for internal government use only and must not be disseminated, distributed, or copied to persons not authorized to receive the information. Unauthorized disclosure may result in prosecution to the full extent of the law.

INFORMATION NOT RELEASABLE TO THE PUBLIC UNLESS AUTHORIZED BY LAW:

This information has not been publicly disclosed and may be privileged and confidential. It is for internal government use only and must not be disseminated, distributed, or copied to persons not authorized to receive the information. Unauthorized disclosure may result in prosecution to the full extent of the law.

Preamble

c. Privacy and Security of Personally Identifiable Information (§155.260)

Section 1411(g) of the Affordable Care Act specifies that information provided by an applicant may be used to ensure the efficient operation of the Exchange. However, 45 CFR 155.260(a)(1) currently states that when an Exchange creates or collects personally identifiable information (PII) for determining eligibility for: enrollment in a QHP, an insurance affordability program, or an exemption from the individual responsibility requirement the Exchange may only use or disclose the PII to perform Exchange minimum functions as described in §155.200. We believe that current §155.260(a)(1) unduly limits the ability of an Exchange to evaluate its effectiveness and to ensure its efficient operation and narrows the scope of section 1411(g) of the Affordable Care Act. Therefore we propose amending §155.260(a)(1). We propose in (a)(1) that Exchanges would be allowed to use and disclose eligibility and enrollment PII to ensure the efficient operation of the Exchange, including the study of Exchange operations, or to conduct research that would inform Congress and the general public of the efficiency of the Exchange program, or when a state operates a reinsurance or risk adjustment program. We also propose in (a)(1) that Exchanges may share eligibility and enrollment PII with other Federal agencies for the purposes of ensuring the efficient operations of the Exchange consistent with other federal statutes. We welcome comment on this proposed expansion of the allowable uses and disclosures of eligibility and enrollment PII.

In (a)(1)(i) we recognize the additional limits on uses and disclosures that exist federal and state laws may impose. In addition, due to the sensitive nature of the PII involved, CMS would use a variety of controls to mitigate risk as part of their data sharing procedures, such as

de-identification and aggregation. In addition, we have considered that researchers would be required to submit a proposal outlining the type of research they intend to conduct and identify the institution which would sponsor the proposed study to ensure the proper use and/or disclosure of PII for research and study purpose. We welcome comment on the methods we have proposed for keeping personally identifiable information confidential.

In (a)(1)(ii) we propose that eligibility and enrollment PII collected or created by an Exchange that is subsequently de-identified is also subject to the requirements of this section. Section 1411 of the Affordable Care Act specifies that any information provided by applicants has a limitation on use. We welcome comment on both the use of de-identified data and preferred standards of de-identification of data.

We propose a re-designation of paragraph 155.260(b)(1) to define the term non-Exchange entity. Paragraph (1)(i) identifies individuals and entities that are certified by an Exchange or acting on behalf of the Exchange. Paragraph (1)(ii) identifies individuals or entities that are hired to perform an Exchange function that involves the use of PII. Paragraph (1)(iii) refers to individuals or entities that obtain access to PII directly from applicants, qualified individuals or enrollees.

Paragraph (2) obligates an Exchange to enter into a contact or other arrangement with a non-Exchange entity. There are a variety of arrangements that could define the relationship between an Exchange and a non-Exchange entity, including but not limited to certification by the Exchange, entering into a contract or agreement for a non-Exchange entity to act on its behalf, or an attestation from a non-Exchange entity.

Paragraph (3) outlines the terms the Exchange must establish in the contract or arrangement. We have added paragraphs (3)(i) and (3)(ii) to ensure that a non-Exchange entity complies with the Exchange privacy and security standards. Paragraph (3)(iii) ensures that the non-Exchange entity bind any employee, agent or subcontractor to the same or more stringent privacy and security standards established by the Exchange. Finally, paragraph (3)(iv) obligates the non-Exchange entity to only use or disclose PII according to the terms of the contract or arrangement. Even if an individual or entity does not have a direct relationship with an Exchange and is therefore not governed by a contract or arrangement with the Exchange, the misuse of applicant PII subjects any person to the civil money penalty described in 155.260(g). We welcome comment on this proposed re-designation of 155.260(b).

We propose to add paragraph (h), to clarify that the Exchange is not liable for any breaches in confidentiality made by a third party entity such as Navigators, agents, and authorized representatives that are beyond the control of the Exchange. We recognize that federal tax return information is not covered by this section as it is governed by section 6103 of the Code. We also note that a third party entity may be held liable for any breach in confidentiality pursuant to applicable State and Federal laws.

d. Implementation of privacy standards for the Federally-facilitated Exchange (§155.275)

Section 155.260(a)(3) requires Exchanges to establish and implement privacy standards that are consistent with the principles in (a)(3)(i) through (a)(3)(viii). These principles are consistent with the requirements found in the Privacy Act. Because the FFE is a federal entity and will collect, create, use and disclose personally identifiable information of individuals the FFE must comply with the Privacy Act. Therefore, we propose the establishment and

implementation of the privacy standards in 155.275(a) through (h) to ensure that the FFE is in compliance with the Privacy Act as well as with the Exchange final rule.

In §155.275(a) we propose the scope of the PII to which the standards described in this section would apply. The standards apply to any and all PII associated with FFE functions irrespective of the source, medium, or purpose for which the PII is received or stored.

In §155.275(b), we propose that the FFE may create, collect, use, and disclose eligibility and enrollment PII to accomplish the specific Exchange function for which it was obtained or to further the efficient operation of the Exchange as permitted under 155.260(a)(1).

In §155.275(b)(1), we propose that Federal income tax return information must be kept confidential and disclosed, used, and maintained only in accordance with section 6103(b)(2) of the Code.

In §155.275(b)(4) we propose that the FFEs would retain PII in accordance with the applicable National Archive and Records Administration (NARA) records retention schedule. The destruction of PII must be carried out according to the appropriate security standards established under the Minimum Acceptable Risk Standards for Exchanges (MARS-E).

In §155.275(c), we propose standards under which individuals could access their own PII stored by the FFE, correct erroneous information, and document a dispute if a correction request is denied.

In §155.275(c)(1), we propose a standard that would provide an individual the ability to access the record(s) and/or PII that the FFE has collected and created about them. In (c)(1)(i) we propose that individuals would be able to obtain access to their record(s) and/or PII collected or

created by the FFE in a simple and timely manner. In (c)(1)(ii) we propose that when an individual requests access to their record(s) they are provided in a format that is readable. In (c)(1)(iii) we propose that the FFE must provide an individual with a method to request the correction of PII that the individual believes is erroneous. If the FFE denies an individual's request to correct their PII, (c)(1)(ii)(A) requires that the FFE must document the dispute, and (c)(1)(ii)(B) requires the FFE to communicate such a dispute to other entities that need the PII to perform a function related to the information being disputed.

In §155.275(c)(2) we propose that if an individual seeks to correct PII about them obtained by the FFE, the individual must request such a correction from the source that originally provided the information to the FFE.

In §155.275(d), we propose standards for the FFE to meet the openness and transparency principle defined by §155.260(a)(3)(iii) to inform individuals about the policies, procedures, and technologies that impact individuals or their PII. In §155.275(d)(1) we propose that the FFE inform individuals as to how their PII will be used and handled at the time that it is collected; this would be accomplished via a standardized Privacy Act statement. The elements listed in paragraphs (f)(1)(i) through (f)(1)(v) are specified in the Privacy Act of 1974 (5 U.S.C. §552a (e)(3)) and are typically found in Privacy Act statements when a federal entity is collecting information from individuals. The elements in (vi) and (vii) regarding how information is secured and the retention periods exceed the Privacy Act requirements, and we invite comment on their inclusion.

In §155.275(d)(2), we propose that the FFE would provide explanations of the policies, procedures and technologies that directly affect individuals and their PII through consumer education materials.

In §155.275(d)(3) we propose that the FFE would post on the FFE web site Privacy Policies in accordance with section 208(c) of the E-Government Act of 2002 and OMB Memorandum M-03-22 and subsequent guidance.

In §155.275(e), we propose standards for the FFE to meet the individual choice principle defined in §155.260(a)(3)(iv). The proposed §155.275(e) would establish a requirement that individuals whose PII is created, collected, used or disclosed by the FFE must be provided a reasonable opportunity to make an informed decision about the collection, use, and disclosure of their PII. Individuals are informed of the uses and disclosures that might affect their personally identifiable information through the openness and transparency standards already defined in §155.275(d). CMS will develop a process for obtaining, maintaining and revoking authorizations from individuals that will be the subject of future guidance. We welcome comment on this standard.

In §155.275(f)(1) we propose to define the standard for maintaining the completeness, accuracy, and timeliness of PII created, collected, used, disclosed, retained, and destroyed by the FFE. We also propose that authorized requests for changes made to PII from individuals, authorized representatives or organizations involved in the operation of the FFE must be processed by the FFE in a timely manner to ensure that the insurance affordability program that an individual is eligible for remains appropriate to their circumstances.

In §155.275(f)(2), we propose that disclosures of PII by the FFE are accounted for pursuant to the requirements of the Privacy Act of 1974 (5 U.S.C. §552a (c)). The FFE would also be required to use this accounting of disclosures as the basis for communicating disputes of information as described under §155.275(c)(1)(iii)(B) as needed.

In §155.275(g), we propose that the FFE must develop policies and procedures, execute training and awareness programs, and conduct ongoing monitoring for non-adherence as required under §155.260(c) and §155.260(d). The FFE would develop policies and procedures that establish the rules of conduct and instructions for all workforce members of the FFE whose activities bring them in contact with PII in any form.

In §155.275(g)(1) and (g)(2) we propose the standards for monitoring non-adherence and breach reporting by the FFE. The processes defined within §155.280 are established as the standard the FFE is required to follow when reporting privacy or security incidents.

e. Implementation of Security Requirements (§155.276)

In §155.276, we propose that the Minimum Acceptable Risk Standards—Exchanges (MARS-E) suite of documents define the security standards required for compliance with §155.260(a)(3)(vii), §155.260(a)(4), §155.260(a)(5), §155.260(a)(6), and §155.270 for any Exchange or non-Exchange entity gaining access to information submitted to an Exchange or through an Exchange via a direct connection to the CMS Hub. The MARS-E suite of documents is guidance that defines a minimum set of security standards that Exchanges must address. It represents a combined effort of CMS and the Internal Revenue Service, Social Security Administration, Department of Veterans Affairs, Department of Homeland Security, Department of Defense, Peace Corps, Office of Personnel Management who will provide data to verify PII

provided through the eligibility and enrollment process. MARS-E is a harmonization of all of the various agencies' security standards that uniformly establishes the standards for all Exchanges and non-Exchange entities. MARS-E was published by CMS on August 1, 2012.

In §155.276, we propose that the applicable scope for security standards include any and all of the information associated with Exchange functions, not only PII. These standards are applicable to all Exchanges and non-Exchange entities.

f. Oversight and Monitoring of Privacy and Security Requirements (§155.280)

In §155.280, we propose standards for the oversight and monitoring of privacy and security requirements as established in §155.260. We propose the applicable scope for oversight and monitoring of security standards include any and all of the information associated with the efficient operation of the Exchange functions.

We propose in §155.280(a) that any individual or entity that gains access to information submitted to an Exchange or through an Exchange process would be subject to HHS oversight and/or monitoring activities to confirm that the individual or entity is in compliance with any of the security requirements or privacy provisions or any other conditions required by law, regulation or guidance, or the term of any contract or agreement.

In §155.280(b), we propose the scope of ongoing oversight activities that HHS may conduct in addition to the initial activities itemized above in order to ensure adherence to the privacy and security requirements. These may include audits and investigations. In addition, administration of APTCs and CSRs will implicate the use of Federal tax information, which would require any individual or entity that gains access to Federal tax information to comply

with 26 U.S.C. §6103 and the provisions that apply to the oversight, monitoring and enforcement authority of the IRS published in IRS Publication 1075.

In §155.280(c), we propose that Exchanges be required to comply with certain reporting requirements related to security and privacy incidents as defined by HHS incident reporting guidelines. In §155.280(c)(1), we propose that Exchanges and non-Exchange entities must develop appropriate policies, procedures and standards for incident handling and breach notification. In paragraph (c)(2), we propose that the policies, procedures and standards for incident handling and breach notification must comply with all applicable State and Federal laws, and all applicable HHS guidance. We welcome comments on the oversight and monitoring activities and how they will apply to the Exchange and non-Exchange entities alike.

PART 155 - EXCHANGE ESTABLISHMENT STANDARDS AND OTHER RELATED STANDARDS UNDER THE AFFORDABLE CARE ACT

§155.260 Privacy and security of personally identifiable information.

(a) Creation, collection, use and disclosure. (1) Where the Exchange creates or collects personally identifiable information for the purposes of determining eligibility for enrollment in a qualified health plan, determining eligibility for other insurance affordability programs, as defined in §155.20, or determining eligibility for exemptions from the individual responsibility provisions in section 5000A of the Code, the Exchange may only use or disclose such personally identifiable information to ensure the efficient operation of the Exchange, including carrying out the functions described in §155.200 of this subpart, to share with Federal executive branch agencies to ensure the efficient operation of the Exchange, to allow for Congressional oversight; and to share with non-Exchange entities in accordance with §155.260(b).

(i) In addition to the limitations on uses and disclosures in (a)(1) any disclosure of PII to entities for the specified purposes in (a)(1) is also subject to:

(A) Applicable State and Federal laws; and

(B) CMS data sharing procedures.

(ii) Secondary use or disclosure of de-identified data. Use or disclosure of personally identifiable information as defined in §155.260(a)(1) that is subsequently de-identified must be limited to that which is permitted under this section.

(b) Application to non-Exchange entities. (1) Definition. A non-Exchange entity means any individual or entity that:

(i) is certified by or acting on behalf of an Exchange or

(ii) is engaged to perform a function or operation for an Exchange where such individual or entity has access through the Exchange to any personally identifiable information or

(iii) collects, uses or discloses personally identifiable information gathered directly from applicants, qualified individuals or enrollees.

(2) Standard. An Exchange must enter into a contract or other arrangement that meets the requirement of (b)(3) with a non-Exchange entity.

(3) Contract or arrangement. Except for tax return information, which is governed by section 6103 of the Code, when collection, use or disclosure of personally identifiable information is not otherwise required by law, the contract or other arrangement described in paragraph (2) must provide that the non-Exchange entity will:

(i) comply with the privacy and security standards established and implemented by the Exchange under §155.260(a)(3),

(ii) comply with the requirements provided in §155.276,

(iii) ensure that any employee or agent, including subcontractors to whom the non-Exchange entity provides such information agrees to comply with the same or more stringent standards established by the Exchange, and

(iv) limit the use or disclose of any personally identifiable information obtained while performing the functions or operations to those specified in the terms of the contract or arrangement described in paragraph (2).

* * * * *

(h) Liability for breach of information. The Exchange is not liable for any breaches of confidentiality made by third party entities such as Navigators, agents, and authorized representatives, that are beyond the control of the Exchange adherent to paragraph (b) of this section.

155.275 Implementation of privacy standards for the Federally-facilitated Exchange.

(a) Scope. Except as otherwise provided, the privacy standards adopted under this section apply to all personally identifiable information created, collected, used or disclosed in the course of performing Exchange functions in the Federally-facilitated Exchange, regardless of

(1) The source of the personally identifiable information;

(2) The medium through and manner in which the personally identifiable information is received or stored; or

(3) The purpose for which the individual provided the personally identifiable information.

(b) Creation, collection, use and disclosure of personally identifiable information.

Collection, creation, use, or disclosure of personally identifiable information by the Federally-facilitated Exchange must be limited to that which is necessary to accomplish a specific purpose related to Federally-facilitated Exchange processes and operations as permitted under 155.260(a)(1).

(1) Non-disclosure of Federal tax information. Federal income tax return information, as defined by section 6103(b)(2) of the Code must be kept confidential and disclosed, used, and maintained only in accordance with section 6103 of the Code.

(2) Retention and destruction of personally identifiable information. Retention of personally identifiable information must be limited to the periods established by the applicable National Archive and Records Administration records retention schedule. Subsequent destruction of personally identifiable information must comply with the security standards set forth in §155.276.

(c) Individual access and correction. (1) Individuals whose information is stored by the Federally-facilitated Exchange must be provided with

(i) a simple and timely means to access the record or any information pertaining to the individual contained in the Federally-facilitated Exchange,

(ii) a copy of their record(s) in a readable form and format,

(iii) the ability to request the correction of erroneous personally identifiable information, and to:

(A) have their dispute documented, if their request is denied and

(B) communicated to other entities that need the personally identifiable information to perform a function related to the information being disputed.

(2) Request for correction. Individuals seeking to correct personally identifiable information used as part of Federally-facilitated Exchange processes and operations must request such a correction from the source that originally provided the information to the Federally-facilitated Exchange.

(d) Openness and transparency. Any individual who provides personally identifiable information to the Federally-facilitated Exchange must be informed by the Federally-facilitated

Exchange regarding policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information.

(1) Informing individuals when collecting personally identifiable information. When the Federally-facilitated Exchange collects or obtains access to personally identifiable information from an individual, the individual must be informed of the following:

- (i) Why the information is needed;
- (ii) What it will be used for;
- (iii) To whom it will be disclosed;
- (iv) The authority under which the information is being collected;
- (v) Whether the collection is mandatory or voluntary and what the effect is if the individual decides not to provide the information;
- (vi) How it will be secured; and
- (vii) How long it will be retained.

(2) Availability of policy explanations. The Federally-facilitated Exchange must make explanations of the policies and procedures related to the collection, use, disclosure, retention, and destruction of personally identifiable information available through consumer education materials.

(3) Web site Privacy Policies. The Federally-facilitate Exchange must post Privacy Policies that comply with the guidance established by the Office of Management and Budget.

(e) Individual choice. The Federally-facilitated Exchange must provide individuals whose personally identifiable information is created, collected, used, or disclosed as part of Federally-facilitated Exchange processes and operations with a reasonable opportunity to make an informed decision about the collection, use, and disclosure of personally identifiable information.

(f) Data quality and integrity. (1) Completeness, accuracy, and timeliness of PII. The Federally-facilitated Exchange must maintain personally identifiable information in a manner that ensures the completeness, accuracy, and timeliness of the information at the time of collection and through changes submitted by authorized sources and that it is not improperly altered or destroyed in an unauthorized manner.

(2) Accounting of disclosures. The Federally-facilitated Exchange must maintain an accounting of disclosures of personally identifiable information pursuant to the Privacy Act of 1974.

(g) Accountability. The Federally-facilitated Exchange must develop and implement policies, procedures, and training and awareness programs based on the above privacy standards to ensure workforce compliance under §155.260(c) and (d).

(1) The Federally-facilitated Exchange must participate in processes to oversee and monitor workforce compliance with the standards defined within §155.275.

(2) Reporting of privacy incidents and breaches by the Federally-facilitated Exchange must be based on the processes described within §155.280.

§155.276 Implementation of security requirements.

Security standards. Any individual or entity that gains access to information submitted to an Exchange or through an Exchange process and/or is required to comply with §155.260 must comply with the Minimum Acceptable Risk Standards for Exchanges documents, which establish security standards for operational, administrative, technical and physical safeguards; monitoring, assessing and updating security controls and risks; secure electronic interfaces; and use of standards and protocols for electronic transactions. The Minimum Acceptable Risk Standards for Exchanges documents can be found at: _____

§155.280 Oversight and Monitoring of privacy and security requirements.

(a) General. The oversight and monitoring activities in this section apply to any individual or entity that gains access to information submitted to an Exchange or through an Exchange process and/or is required to comply with §155.260.

(b) Audits and investigations. CMS will conduct and supervise oversight activities that include the following: audits; investigations; inspections; civil, criminal or administrative proceedings or actions; and any other activities necessary for appropriate oversight of Exchange-related activities and processes.

(c) Reporting. Security and privacy incidents related to Exchange activities must be reported according to CMS incident reporting guidelines as well as State reporting guidelines.

(1) The entity involved with the incident is responsible for managing the incident in accordance with entity's documented incident handling and breach notification procedures.

(2) Document incident handling and breach notification procedures must comply with:

(i) All applicable State and Federal laws; and

(ii) All applicable HHS guidance.

THIS QUALIFIED HEALTH PLAN ISSUER AGREEMENT (“Agreement”) is entered into on <<auto fill current date>> by and between THE CENTERS FOR MEDICARE & MEDICAID SERVICES (“CMS”) and <<auto fill Producer’s name>> (“QHP Issuer”), located at <<auto fill address>>.

Section A – General Provisions

Article I Term and Authority

This Agreement is entered into pursuant to Sections 1301–1334, §§ 1341–1343, and Sections 1401, 1402, 1411, and 1412 of the Affordable Care Act (ACA) and the regulations promulgated thereunder, as the same be codified from time to time in Title 45 of the Code of Federal Regulations (“CFR”), for the operation of an Affordable Insurance Exchange (“Exchange”). Except to the extent otherwise specifically noted herein, all citations to regulatory sections in this Agreement shall be interpreted as citations to sections of Title 45 of the CFR.

The term of this Agreement begins _____ [Need OGC input on what the date should be] and ends December 31, 2014, after which this Agreement may be renewed for each subsequent calendar year subject to Centers for Medicare & Medicaid Services’ (“CMS”) approval of QHP Issuer’s new rate and benefit package submission in accordance with § 155.1020(c) and § 155.1075, or as otherwise determined in writing by CMS

In accordance with § 156.200, this Agreement pertains to the obligations and responsibilities of the QHP Issuer and the respective rights and obligations of CMS and the QHP Issuer related to the offering of health plans or dental plans in the Exchange. This Agreement supersedes any prior agreements between the QHP Issuer and CMS with respect to the subject matter contained in this Agreement. This Agreement does not modify or supersede other agreements or contracts the QHP issuer has with CMS.

This Agreement incorporates any changes required by statute to be implemented during the term of the Agreement and any regulations, court orders or policies implementing or interpreting such statutory provisions.

The QHP Issuer must comply with all applicable requirements, including reporting and customer service requirements, and make accommodations for individuals with disabilities as described in CMS regulations and guidance implementing the ACA. This Agreement does not supersede or modify these requirements. Failure of this Agreement to reference a specific regulatory requirement does not affect the requirement’s applicability to the QHP Issuer and CMS. This Agreement incorporates any pertinent information collection requirements approved under the authority of the Paperwork

Reduction Act of 1995 and displaying a valid Office of Management and Budget (OMB) control number.

Article II Functions to Be Performed by QHP Issuers

A. GENERAL REQUIREMENTS

1. QHP Issuer agrees to abide by all applicable existing state and federal statutes and regulations, and all future state and federal statutes and regulations once they become effective.
2. QHP Issuer agrees that it is in compliance with all state laws and statutes related to its QHP plans in the state in which QHP plans are being offered, and agrees to notify CMS if in the future it is not compliant.
3. The QHP Issuer must comply with the privacy and security standards adopted by the Federally-facilitated Exchange (FFE) consistent with 45 CFR §155.260.

B. QUALIFIED HEALTH PLAN REQUIREMENTS

1. Establish and maintain an adequate network of providers—including those that specialize in mental health and substance abuse services as applicable—in order to ensure that all services under the approved QHPs will be accessible without unreasonable delay as required under §§ 156.230 and 156.235.
2. Have in effect at all times a certification issued or recognized by the Exchange to demonstrating that each plan it offers in the Exchange is a QHP as required under § 156.200(a).
3. Retain its license and remain in good standing to offer health insurance coverage in each state in which the issuer offers health insurance coverage as required under § 156.200(b)(4).
4. Have a sufficient number and geographic distribution of essential community providers (ECPs), where available, to ensure reasonable and timely access to a broad range of such providers for low-income, medically underserved individuals as required under § 156.235.
5. If providing coverage through a direct primary care medical home, ensure that the home meets criteria established by the Department of Health and Human Services (CMS), the QHP meets all requirements that are otherwise applicable, and that the services covered by the direct primary care medical home are coordinated with the QHP Issuer as required under § 156.245.

6. The QHP Issuer must ensure that each QHP it issues complies with benefit design standards in accordance with § 156.200(b)(3) and any future regulatory or administrative guidance.
7. The QHP Issuer must offer at least one QHP at the silver coverage level, at least one QHP at the gold coverage level [or at least one plan at a high or low coverage level for stand-alone dental plans], and a child-only option for each QHP in accordance with section 1302(d)(1) of the ACA and pursuant to § 156.200(c). [Pursuant to section 1302(f) of the ACA and § 156.200(c), this does not apply to catastrophic plans described in section 1302(e) of the ACA and § 156.155.]
8. A QHP Issuer in a Federally-facilitated individual market Exchange must also offer in the state's Federally-facilitated SHOP at least one QHP at the silver level of coverage and at least one QHP at the gold level of coverage [or at least one plan at a high or low coverage level for stand-alone dental plans], or document how it meets the provisions of § 156.200(c) and (g). [This does not apply to catastrophic plans described in section 1302(e) of the ACA and § 156.155.]
9. For each QHP offered, the QHP Issuer must also offer individual market plan variations for CSRs as described in section 1402 of the ACA and pursuant to § 156.420. [This does not apply to dental plans.]
10. The QHP Issuer must set rates for an entire benefit year—or for the Small Business Health Options Program (SHOP) plan year—in accordance with § 156.210(a). As required under § 156.210(b) and in a form and manner specified by HHS (§ 155.1020(c)), the QHP Issuer agrees to develop and submit an annual rate and benefit package, including any quarterly trend increases for small group plans, that includes all required information on rate tables, rating assumptions, covered benefits, cost-sharing requirements, and formularies.
11. For individual market plans, the QHP Issuer must ensure the cost sharing required of enrollees under any silver plan variation of a standard silver plan for an essential health benefit from a provider may not exceed the corresponding cost sharing required in the standard silver plan or any other silver plan variation thereof with a lower actuarial value in accordance with § 156.420(e).
12. The QHP Issuer agrees to provide detailed information on allocation of rates and the expected allowed claims costs, as applicable, for the plan to benefits included in the essential health benefits (EHBs) (other than services described in § 156.280(d)(1)) and additional benefits in excess of EHB, along with other QHP certification requirements in accordance with § 156.470.
13. The QHP Issuer must submit to the Exchange a justification for a rate increase prior to the implementation of the increase, and the QHP Issuer must prominently post the justification on its website in accordance with § 156.210(c). [This does not apply to stand-alone dental plans.]

14. The QHP Issuer must charge the same premium rate without regard to whether the plan is offered through an Exchange, or whether the plan is offered directly from the Issuer or through an agent in accordance with § 156.255(b).
15. The QHP Issuer agrees to meet all standards for providing essential health benefits (EHBs) as described in § 1302(b) of the ACA, §§ 156.100 – 156.150, and any guidance promulgated on such authority
16. The QHP Issuer agrees to abide by all cost-sharing limits as described in § 1302(c) of the ACA.
17. The QHP Issuer agrees to abide by all Actuarial Value (AV) requirements as described in § 1302(d) of the ACA, §§ 156.100 – 156.150, and any guidance promulgated on such authority, including the use of the AV calculator described in § 156.135.
18. The QHP Issuer must not charge any cost sharing for essential health benefits to Indians with expected household incomes that do not exceed 300 percent for the Federal Poverty Level as defined in 45 CFR 155.300, and enrolled in a metal level QHP in the individual market through an Exchange. In addition, the QHP Issuer will not charge cost sharing on essential health benefits to any Indian enrolled in a metal level QHP in the individual market through an Exchange, for an item or service furnished directly by the Indian Health Service, and Indian Tribe, Tribal Organization, or Urban Indian Organization, or through referral under contract health services. § § 156.410(b)(2) and (3), and 156.420(b).
19. The QHP Issuer agrees to issue a policy at the rate that is identified by the Exchange and transmitted to the issuer consistent with § 156.265.).
20. The QHP Issuer agrees to segregate funds for abortion services in accordance with the provisions of § 156.280.
21. Benefits for QHPs approved for a SHOP may be revised annually. Rates for QHPs approved for a SHOP will be filed annually. Issuers of SHOP QHPs can continue to file quarterly trend increases with their annual filings. Due to system limitations, until further notice, additional rate changes in the small group market (other than quarterly trending described above) can be processed only on an annual basis, as they are in the individual market. . The QHP issuer of SHOP QHPs agrees that the rates per individual for a given employer will remain constant for the employer's full plan year in accordance with §155.705(b)(6)(ii).
22. The QHP Issuer, to the extent it issues SHOP QHPs will adhere to all provisions contained in § 156.285 including rating and premium payment requirements, enrollment periods and processes, participation rules, and termination procedures.
23. The QHP Issuer will follow any guidance distributed by CMS pertaining to the QHP requirements associated with the risk adjustment, reinsurance, risk corridor, CSR, and APTC programs as described in Parts 153, 155, and 156.

C. ENROLLMENT REQUIREMENTS

1. The QHP Issuer must accept the enrollment of individuals found to be qualified in accordance with all applicable requirements pursuant to § 156.265(b). The first opportunity for enrollment will be during the initial open enrollment period that begins October 1, 2013, and extends through March 31, 2014. The annual open enrollment period for benefit years beginning on or after January 1, 2015 starts on October 15 and extends through December 7 pursuant to § 156.260(a).
2. The QHP Issuer will abide by the effective dates of coverage established by the Exchange in accordance with § 156.260(a)(1) and in accordance with the data in the enrollment transaction sent by the Exchange to the QHP Issuer as described in § 155.400(b)(1).
3. The QHP Issuer will enroll qualified individuals during special enrollment periods described in § 155.420(d) and abide by the effective dates of coverage for the special enrollment periods described in § 155.420(b) in accordance with § 156.260(a)(2) and in accordance with the data in the enrollment transaction sent by the Exchange to the QHP Issuer as described in § 155.400(b)(1).
4. The QHP Issuer will notify all qualified individuals who select one of its QHPs of their effective date of coverage in accordance with § 156.260(b).
5. The QHP Issuer will provide new enrollees with an enrollment information packet that complies with accessibility and readability standards established in § 155.230(b) in accordance with § 156.265(e).
6. In instances in which an individual initiates enrollment directly with the QHP, the QHP Issuer will comply with the terms of the application program interface (API) agreement in Section C, and will either
 - a. direct the individual to file an application with the Exchange in accordance with § 156.265(b)(2)(i), or
 - b. ensure the applicant receives an eligibility determination for coverage through the Exchange website as described in § 156.265(b)(2)(ii).
7. The QHP Issuer will accept and send enrollment information consistent with the privacy and security standards and requirements established by the Exchange, and in the appropriate electronic format in accordance with § 156.265(c), and in accordance with any future guidance regarding privacy and security standards or the acceptance or transmission of enrollment information.
8. The QHP Issuer will follow the premium payment process established by the Exchange in accordance with § 156.265(d) and any future guidance on the premium payment process.

9. The QHP Issuer will ensure that an individual assigned to a particular plan variation is only required to pay the applicable cost sharing for that plan variation in accordance with §156.410.
10. The QHP Issuer will assign the individual to the plan variation specified in the individual's enrollment information provided to the QHP Issuer by the Exchange in accordance with §156.410(b).
11. The QHP Issuer will accept the information described in § 155.340(a) that is necessary to enable the Exchange to implement, discontinue implementation of, or modify the level of the advance payment of the premium tax credit (APTC) or cost-sharing reduction (CSR) granted to an individual.
12. The QHP Issuer will change an individual's enrollment or plan variation assignment, pursuant to the enrollment information received from the Exchange, per § 156.425 and the final HHS Notice of Benefit and Payment Parameters published March 11, 2013. . In the case of a change in assignment to a different plan variation of the same QHP (or the QHP without CSRs under this subpart) in the course of a benefit year, the QHP issuer will ensure that any cost sharing paid by the individual under previous plan variations for that benefit year is accounted for in the new plan variation (or the QHP without CSRs) for purposes of calculating cost sharing on the basis of aggregate spending by the individual, such as for deductibles or for the annual limitations on cost sharing.
13. The QHP Issuer will enroll an individual eligible for an APTC pursuant to the enrollment information submitted by the Exchange pursuant to § 155.340(a)(2). The QHP Issuer will also reduce that individual's premium pursuant to the enrollment information submitted by the Exchange in accordance with § 156.460.
14. The QHP Issuer will accept the total premium breakdown as determined by the Exchange and as specified in the electronic enrollment transmission. This includes:
 - a.) the total premium amount which is based on rate attestations submitted by the applicant;
 - b.) the APTC amount;
 - c.) any other payment amounts as depicted on the enrollment transmission.
15. The QHP Issuer will participate in a financial reconciliation process to resolve discrepancies as described in 155.400(d) and 156.265(f).
16. The QHP Issuer will reconcile enrollment files with the Exchange at least monthly, in accordance with § 156.265(f) and in compliance with any future CMS guidance. The QHP Issuer will accept enrollment information as required by

§ 156.265(c) and acknowledge receipt of enrollment files from the Exchange as required by § 156.265(g). The QHP Issuer will accept enrollment files when sent by the Exchange, unless reported technical problems impair acceptance and the QHP Issuer provides appropriate notice to the Exchange as soon as is practicable.

17. The QHP Issuer will only terminate an enrollee individual's coverage in accordance with the process in § 156.270(a).
18. In cases of termination of coverage of a qualified individual, the QHP Issuer will provide the enrollee with termination of coverage notice, including the reason for termination, at least 30 days prior to the last day of coverage, consistent with the effective date established by the Exchange in accordance with § 156.270(b)(1).
19. In cases of termination of coverage of a qualified individual, the QHP Issuer will notify the Exchange of the enrollee's termination effective date and reason for termination in accordance with § 156.270(b)(2).
20. The QHP Issuer will establish a standard policy for the termination of coverage of enrolled individuals due to nonpayment of premium as required by § 156.270(c) that includes the grace period for enrolled individuals receiving APTC and is applied uniformly to enrollees in similar circumstances.
21. The QHP Issuer will adhere to all regulatory requirements for enrollees receiving APTCs during their grace period in accordance with § 156.270(d) and (e) and for enrollees receiving CSR during their grace period in accordance with § 156.430(f)(1).

These regulatory requirements include:

- i. Providing a grace period of 3 consecutive months if the enrollee receiving APTCs has previously paid at least one full month's premium during the benefit year;
- ii. Paying all appropriate claims for services rendered during the first month of the grace period;
- iii. The ability to pend claims for services rendered during months 2 and 3 of the grace period;
- iv. Notifying CMS of non-payment;
- v. Notifying providers of the possibility of denied claims when the enrollee is in the 2nd and 3rd month of the grace period
- vi. Continuing to collect APTCs on behalf of the enrollee;

- vii. Returning APTCs paid on behalf of the enrollee for month 2 or month 3 of the grace period if the enrollee exhausts the grace period without full payment.
22. The QHP Issuer will provide an enrolled individual who is delinquent in premium payment with notice of such delinquency in accordance with §156.270(f).
23. The QHP Issuer will terminate an enrolled individual for which the QHP Issuer receives or received APTCs for non-payment only after exhaustion of the grace period on the appropriate termination effective date in accordance with §156.270(g).
24. The QHP Issuer will maintain records in accordance with standards established by the Exchange in accordance with §155.430(c) and any relevant future guidance.
25. The QHP Issuer will make reasonable accommodations for all individuals with disabilities (as defined by the Americans with Disabilities Act) before terminating coverage for such individuals as required by the Exchange in accordance with § 155.430(c)(3).
26. The QHP Issuer will adhere to the guaranteed availability requirements of section 2702 of the Public Health Service Act as implemented by §147.104.

D. ENROLLEE PROTECTIONS

1. The QHP Issuer will have in place an internal claims and appeals process and external review process that, at a minimum, meet the requirements of 45 CFR Part 147 and all applicable sub-regulatory guidance. [This does not apply to stand-alone dental plans].
2. The QHP Issuer agrees to review and respond to consumer complaints as required as part of participation standards in § 156.200.
3. The QHP Issuer will comply with all termination of coverage and grace period requirements under § 156.270 and § 155.430.
4. The QHP issuer must provide for continuation of enrollee health benefits during instances of nonrenewal and decertification in accordance with § 156.290.
5. The QHP issuer must provide adequate coverage network and essential community providers (ECPs) pursuant to §§ 156.230 and 156.235.
6. The QHP issuer must provide for continuation of enrollee health benefits during instances of redetermination in accordance with § 155.330(f)(3).

E. QUALITY REQUIREMENTS

1. The QHP Issuer must comply with the minimum certification requirements pertaining to quality reporting and provide relevant information to the Exchange and CMS pursuant to § 156.200(b)(5) and as specified under any future applicable rules or regulations.
2. As required by § 156.275, the QHP Issuer agrees to meet and maintain the QHP accreditation standards in the time frame established by the Exchange pursuant to § 155.1045. [This does not apply to stand-alone dental plans.]
3. A QHP Issuer with existing accreditation agrees to authorize the release of its accreditation data from relevant accrediting entities) to the Exchange to facilitate the Exchange's certification decisions to be made in accordance with 45 CFR §155.1000 and to demonstrate its compliance with requirements under § 156.275. The QHP Issuer agrees to provide the necessary information about its existing health plan accreditation from the recognized accrediting entity(ies) so that the Exchange can use this information (if available) to certify a health plan as a QHP and determine if it is in the interest of the individuals in an Exchange.
4. The QHP Issuer understands and acknowledges that the Exchange website may display composite data gathered using the Consumer Assessment of Healthcare Providers and Systems (CAHPS®) measures, which correspond to existing product lines outside the Exchange. These data will be displayed if the following conditions are met: the QHP Issuer has authorized the release of its accreditation data as required for QHP certification, CAHPS® data were considered as part of the QHP Issuer's accreditation on Medicaid or commercial lines of business and were submitted to the Exchange by the accrediting entity, and the CAHPS® data submitted to the Exchange by the accrediting entity are available for the same product type as the QHP Issuer offered in the Exchange. § 155.1000.
5. The QHP Issuer understands and acknowledges that the Exchange website may display that a QHP Issuer is accredited if one of the recognized accrediting entities has accredited that issuer on any of its existing products being offered in its commercial, Medicaid, or Exchange product lines and verifies that accreditation. § 155.1000.

F. INFORMATION REPORTING REQUIREMENTS

The QHP Issuer will comply with all applicable information collection and reporting requirements approved through the Paperwork Reduction Act of 1995 and having a valid OMB control number. These include required information regarding

- reinsurance (45 CFR Part 153 subpart C, subpart E, and subpart H);
- risk corridors (45 CFR Part 153 subpart F);
- risk adjustment (45 CFR Part 153 subpart D, subpart F, and subpart H);

- CSRs, (45 CFR Part 155 and Part 156);
- APTC; (45 CFR Part 155 and Part 156); and
- Other information required for oversight purposes.

The QHP Issuer will submit all required information in a CMS-established manner and common data format. The QHP Issuer's chief executive officer (CEO), chief financial officer (CFO), or an individual delegated signature authority (who reports directly to one of these officers) must attest to the accuracy, completeness, and truthfulness of the data submitted to CMS, or its designee, for these programs.

G. MARKETING

The QHP Issuer agrees that all marketing materials will include the following statement:

“(Insert plan’s legal or marketing name) is a Qualified Health Plan in the (name of Exchange).”

H. RISK ADJUSTMENT, REINSURANCE AND RISK CORRIDORS

In accordance with 45 CFR Part 153 and the Annual CMS Notice of Benefit and Parameters, the QHP Issuer agrees to remit to CMS or a State operating risk adjustment the net balance of risk adjustment charges pursuant to § 153.610(e) and risk adjustment user fees pursuant to § 153.610(f)(2)—as assessed by CMS for covered plans inside and outside the Exchange, as applicable—and to do so in compliance with CMS-established processes and timelines. In accordance with 45 CFR Part 153 and the Annual CMS Notice of Benefit and Parameters, the QHP Issuer agrees to remit to CMS risk corridor charges pursuant to § 153.510(d) and reinsurance contributions pursuant to § 153.405(c)(2)—as assessed by CMS for covered plans inside and outside the Exchange, as applicable—and to do so in compliance with CMS-established processes and timelines. [This does not apply to stand-alone dental plans.]

Article III Payment

A. IDENTIFICATION

1. In accordance with §§ 156.430 and 156.460, the QHP Issuer agrees to provide CMS with its Tax Identification Number (TIN) and associated legal entity name as registered with the Internal Revenue Service in order to receive payments under the APTC, CSR, risk adjustment, reinsurance, and risk corridors programs

2. In accordance with §§ 156.430 and 156.460., the QHP Issuer agrees to promptly notify CMS regarding any changes in its TIN, associated legal entity, bank account information, address, or any other information needed by CMS to make payments to the QHP Issuer for the APTC, CSR, risk adjustment, reinsurance, and risk corridors programs.

B. METHOD

CMS agrees to pay the QHP Issuer under this Agreement in accordance with the provisions of the Annual Notice of Benefit and Payment Parameters and Parts 153, 155, and 156:

1. The QHP Issuer agrees to submit charges owed to CMS under the risk adjustment and risk corridors programs, and contributions owed to CMS under the reinsurance program under the time frames and specifications established in the annual CMS Notice of Benefit and Payment Parameters. The QHP Issuer agrees that it will remit applicable charges and contributions owed for non-QHP plans outside the Exchange pursuant to §§ 153.310, 153.410, 153.510 and §§ 156.430 and 156.460.
2. CMS agrees that payment for CSRs and APTC will be made on behalf of eligible and enrolled individuals to the QHP Issuer pursuant to § 156.430 and § 156.460.
3. The QHP Issuer agrees that it will accept APTC and advance CSR payments made by CMS to the QHP Issuer on behalf of eligible and enrolled individuals pursuant to § 156.430(b).
4. The QHP Issuer agrees to reduce premiums on behalf of eligible individuals if the Exchange notifies the QHP Issuer that it will receive an APTC on behalf of that individual pursuant to § 156.460.
5. The QHP Issuer agrees to submit to CMS the actual amount of CSRs provided to each enrollee pursuant to § 156.430(c).
6. The QHP Issuer agrees to accept payment information submitted by CMS. This includes payment amounts made to the QHP Issuer attributable to the risk adjustment, reinsurance, risk corridor, CSR, and APTC programs. The report also will include user fees. §§ 153.310, 153.410, 153.510 and §§ 156.430 and 156.460.
7. The QHP Issuer agrees that it is bound by 2 CFR 376 and that no individual or entity that is a part of the Issuer's organization is excluded by the Department of Health and Human Services Office of the Inspector General or by the General Services Administration. This includes any member of the board of directors, key management or executive staff or major stockholder of the Issuer and its affiliated companies, subsidiaries or subcontractors.

8. The QHP Issuer agrees that in accordance with sections 6401 and 6403 of the ACA, it will not enter into an agreement or sub-agreement with any entities or individuals that the CMS OIG has excluded from participation in Medicare, Medicaid, the Children's Health Insurance Program, or other federal healthcare programs (as defined in section 1128B(f) of the Social Security Act) on the basis of the authority contained in various sections of the Social Security Act, including sections 1128, 1128A, 1156, and 1892. When the OIG has excluded a provider, QHPs are prohibited from paying for any items or services furnished, ordered, or prescribed by the excluded individuals or entities until the provider has been reinstated by the OIG .

Article IV Records Rééquipements

A. REPORTING REQUIREMENTS

The QHP Issuer shall have effective procedures to develop, compile, evaluate, and report statistics and other information to CMS, its enrollees, and the general public, at the times and in the manner required by CMS, while safeguarding the confidentiality of the doctor-patient relationship as required by §§ 156.200(a)(1)–(7) and (b)(5).

The QHP Issuer shall develop, compile, evaluate, and report to CMS, the Exchange, its enrollees, and the general public—at the times and in the manner required by CMS or the Exchange, while safeguarding the confidentiality of the doctor-patient relationship—the following information and data:

- i. Information on the termination of enrollee coverage, initiated by either the enrollee or the QHP (§ 155.430(c));
- ii. Reporting and reconciliation of billing and payment information with SHOP premium aggregation services pursuant to § 156.285;
- iii. Data submission requirements for CSRs and APTC pursuant to § 156.450 and the Annual CMS Notice of Benefit and Payment Parameters;
- iv. Data submission requirements for the risk adjustment, reinsurance, and risk corridors pursuant to the Annual Notice of Benefit and Payment Parameters; and
- viii. Risk adjustment data (for QHP Issuers that offer risk adjustment covered plans) as requested by the state or CMS (on its own or on behalf of the state) to use for data validation (§ 153.620).

Article V Renewal of the QHP Issuer Agreement

A. RENEWAL OF AGREEMENT

QHP agrees to comply with renewal instructions and procedures identified by CMS.

B. NONRENEWAL OF AGREEMENT BY QHP ISSUER

1. Pursuant to § 156.290, if the QHP Issuer elects not to renew one or more QHPs for any calendar year, it agrees to:
 - a. notify the Exchange of its decision prior to the beginning of the recertification process and in accordance with procedures adopted by the Exchange in under § 155.1075;
 - b. fulfill its obligation to cover benefits for each enrollee through the end of the plan or benefit year;
 - c. fulfill data-reporting obligations from the last plan or benefit year of the certification;
 - d. provide notice to enrollees; and
 - e. terminate coverage for enrollees in the QHP in accordance with § 156.270.
2. Notice of QHP nonrenewal. If a QHP Issuer elects not to seek recertification with the Exchange for its QHP, the QHP Issuer must provide written notice to each enrollee.

C. DECERTIFICATION

If a QHP is decertified by the Exchange, the QHP Issuer must terminate coverage for enrollees only after -

1. The Exchange has made notification as described in § 155.1080, and
2. Enrollees have had an opportunity to enroll in other coverage.

Article VI Requirements of Other Laws and Regulations

A. The QHP Issuer agrees to comply with -

1. federal laws and regulations designed to prevent or ameliorate fraud, waste, and abuse, including applicable provisions of federal criminal law, the False Claims Act (31 USC section 3729 et seq.), and the anti-kickback statute (section 1128B(b) of the Social Security Act); and
2. Health Insurance Portability and Accountability Act administrative simplification rules at 45 CFR Parts 160 and 162. [§ 155.270(a)]

B. Pursuant to section 13112 of the American Recovery and Reinvestment Act of 2009 (ARRA), the QHP Issuer agrees that as it implements, acquires, or upgrades its health information technology systems, it shall utilize, where available, health information technology systems and products that meet the standards and implementation specifications adopted under § 3004 of the Public Health Service Act, as amended by section 13101 of the ARRA.

C. In the event that any provision of this Agreement conflicts with the provisions of any statute or regulation applicable to a QHP Issuer, the provisions of the statute or regulation take precedence.

Article VII Attestations

A. All attestations made and information provided as part of the certification application are hereby incorporated by reference into this Agreement.

B. The QHP Issuer agrees to notify CMS if any of the answers provided to the attestations in the certification application change.

Message

From: Linares, George E. (CMS/OIS) [NotResp]
[NotResp]
Sent: 11/7/2013 8:56:59 PM
To: Schankweiler, Thomas W. (CMS/OIS) [NotResp]
[NotResp] Fryer, Teresa M. (CMS/OIS) [NotResp]
[NotResp] Lyles, Darrin V. (CMS/OIS)
[NotResp]
Oh, Mark U. (CMS/OIS) [NotResp]
[NotResp]
CC: Fletcher, John A. (CMS/OIS) [NotResp]
[NotResp] Grothe, Kirk A. (CMS/OIS) [NotResp]
[NotResp] Outerbridge, Monique
[NotResp]
Subject: RE: TRB [NotResp]

A decision has to be made quickly as to which family of systems is this application going to be part of. If it is [NotResp] then it will need to be part of the [NotResp] CA test on Dec 9th. Additionally, we need to determine if additional funding is required since we are increasing the scope.

Thanks

George Linares

Acting Chief Technology Officer
Centers for Medicare & Medicaid Services (CMS)
410.786.2866 | george.linares@cms.hhs.gov
7500 Security Blvd., N3-15-25
Baltimore, MD 21244-1850

Need more information? Visit [the OIS website](#).

From: Schankweiler, Thomas W. (CMS/OIS)
Sent: Thursday, November 07, 2013 3:29 PM
To: Fryer, Teresa M. (CMS/OIS); Lyles, Darrin V. (CMS/OIS); Linares, George E. (CMS/OIS); Oh, Mark U. (CMS/OIS)
Subject: Re: TRB [NotResp]

I have a contractor that will be embedded tomorrow to look at a variety of topics, one being the ez application. I have no inf. Yet of what it is or where it is being developed or by when. I don't want this associated in any way at this point with the ffm. It is just to wild of a variable at this point. It needs to remain out of scope and checked some other way.

Tom

From: Fryer, Teresa M. (CMS/OIS)
Sent: Thursday, November 07, 2013 03:22 PM
To: Lyles, Darrin V. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)
Subject: FW: TRB [NotResp]

So this needs to be included in the scope of the [NotResp] testing on December 9.

Teresa

From: Linares, George E. (CMS/OIS)
Sent: Thursday, November 07, 2013 1:39 PM
To: Fryer, Teresa M. (CMS/OIS); Marantan, James (CMS/OIS)
Subject: FW: TRB [NotResp]

fyi

George Linares

Acting Chief Technology Officer

Centers for Medicare & Medicaid Services (CMS)

☎ 410.786.2866 ✉ george.linares@cms.hhs.gov

7500 Security Blvd., N3-15-25

Baltimore, MD 21244-1850

Need more information? Visit [the OIS website](#).

From: Booth, Jon G. (CMS/OC)
Sent: Thursday, November 07, 2013 1:04 PM
To: Linares, George E. (CMS/OIS)
Cc: Nelson, David J. (CMS/OEM); Chao, Henry (CMS/OIS); Patel, Ketan (CMS/OC); Oh, Mark U. (CMS/OIS); Wallace, Mary H. (CMS/OC)
Subject: Re: TRB - [NotResp]

Agreed. Ketan and I met on that topic last night and I will get you a response on that email thread today. Thanks.

From: <Linares>, George Linares BB <George.Linares@cms.hhs.gov>
Date: Thursday, November 7, 2013 at 1:02 PM
To: Jon Booth <jon.booth@cms.hhs.gov>
Cc: David Nelson BB <David.Nelson@cms.hhs.gov>, Henry Chao BB <henry.chao@cms.hhs.gov>, Ketan Patel BB <Ketan.Patel@cms.hhs.gov>, Mark Oh BB <mark.oh@cms.hhs.gov>, Mary Wallace BB <Mary.Wallace@cms.hhs.gov>
Subject: RE: TRB [NotResp]

Jon,

I appreciate incorporating the governance aspect on this effort. Actually, I had heard of [NotResp] but I didn't have any context on its role on the Marketplace. We can certainly proceed with a small review, and I would also include security, Teresa Fryer specifically. From a different email thread that I sent you and Ketan yesterday, Healthcare.gov is currently operating without an ATO, and if this application is going to be part of that family of systems, we need to have a plan to close the security gap as well.

Thanks

George Linares

Acting Chief Technology Officer

Centers for Medicare & Medicaid Services (CMS)

☎ 410.786.2866 ✉ george.linares@cms.hhs.gov

7500 Security Blvd., N3-15-25

Baltimore, MD 21244-1850

Need more information? Visit [the OIS website](#).

From: Booth, Jon G. (CMS/OC)

Sent: Thursday, November 07, 2013 12:52 PM

To: Linares, George E. (CMS/OIS)

Cc: Nelson, David J. (CMS/OEM); Chao, Henry (CMS/OIS); Patel, Ketan (CMS/OC); Oh, Mark U. (CMS/OIS); Wallace, Mary H. (CMS/OC)

Subject: TRB NotResp

George,

As you may be aware we are working on a contingency system to support increased NotResp enrollments. This project is on a very aggressive timeline with a launch date of 11/25.

As part of a discussion yesterday on provisioning NotResp for this project, the security directed us to schedule a TRB session.

We have been directed by OA to keep this project under the radar. I recognize the need to operate within the IT governance framework but we need to keep this project out of the spotlight, even from an internal perspective.

I spoke to Dave and Henry this morning and they suggested a small review with the tow of them them and you that we could consider a TRB briefing or review. Please let me know your thoughts on this and if there are any other key OIS resources we need to pull into this discussion.

Thanks,

Jon

Message

From: Fryer, Teresa M. (CMS/OIS) [NotResp]
[NotResp]
Sent: 11/7/2013 8:22:24 PM
To: Lyles, Darrin V. (CMS/OIS) [NotResp]
[NotResp] Schankweiler, Thomas W. (CMS/OIS) [NotResp]
[NotResp]
Subject: FW: TRB [NotResp]
Attachments: image001.jpg; image002.jpg

So this needs to be included in the scope of the FFM testing on December 9.

Teresa

From: Linares, George E. (CMS/OIS)
Sent: Thursday, November 07, 2013 1:39 PM
To: Fryer, Teresa M. (CMS/OIS); Marantan, James (CMS/OIS)
Subject: FW: TRB [NotResp]

fyi

George Linares

Acting Chief Technology Officer

Centers for Medicare & Medicaid Services (CMS)

410.786.2866 george.linares@cms.hhs.gov

7500 Security Blvd., N3-15-25

Baltimore, MD 21244-1850

Need more information? Visit [the OIS website](#).

From: Booth, Jon G. (CMS/OC)
Sent: Thursday, November 07, 2013 1:04 PM
To: Linares, George E. (CMS/OIS)
Cc: Nelson, David J. (CMS/OEM); Chao, Henry (CMS/OIS); Patel, Ketan (CMS/OC); Oh, Mark U. (CMS/OIS); Wallace, Mary H. (CMS/OC)
Subject: Re: TRB - [NotResp]

Agreed. Ketan and I met on that topic last night and I will get you a response on that email thread today. Thanks.

From: <Linares>, George Linares BB <George.Linares@cms.hhs.gov>
Date: Thursday, November 7, 2013 at 1:02 PM
To: Jon Booth <jon.booth@cms.hhs.gov>
Cc: David Nelson BB <David.Nelson@cms.hhs.gov>, Henry Chao BB <henry.chao@cms.hhs.gov>, Ketan Patel BB <Ketan.Patel@cms.hhs.gov>, Mark Oh BB <mark.oh@cms.hhs.gov>, Mary Wallace BB <Mary.Wallace@cms.hhs.gov>
Subject: RE: TRB - [NotResp]

Jon,

I appreciate incorporating the governance aspect on this effort. Actually, I had heard of [NotRes p] but I didn't have any context on its role on the Marketplace. We can certainly proceed with a small review, and I would also include security, Teresa Fryer specifically. From a different email thread that I sent you and Ketan yesterday, Healthcare.gov is currently operating without an ATO, and if this application is going to be part of that family of systems, we need to have a plan to close the security gap as well.

Thanks

George Linares

Acting Chief Technology Officer

Centers for Medicare & Medicaid Services (CMS)

410.786.2866 george.linares@cms.hhs.gov

7500 Security Blvd., N3-15-25

Baltimore, MD 21244-1850

Need more information? Visit [the OIS website](#).

From: Booth, Jon G. (CMS/OC)

Sent: Thursday, November 07, 2013 12:52 PM

To: Linares, George E. (CMS/OIS)

Cc: Nelson, David J. (CMS/OEM); Chao, Henry (CMS/OIS); Patel, Ketan (CMS/OC); Oh, Mark U. (CMS/OIS); Wallace, Mary H. (CMS/OC)

Subject: TRB [NotRes p]

George,

As you may be aware we are working on a contingency system to support increased FFM enrollments. This project is on a very aggressive timeline with a launch date of 11/25.

As part of a discussion yesterday on provisioning development-zone [NotRes p] for this project, the security directed us to schedule a TRB session.

We have been directed by OA to keep this project under the radar. I recognize the need to operate within the IT governance framework but we need to keep this project out of the spotlight, even from an internal perspective.

I spoke to Dave and Henry this morning and they suggested a small review with the tow of them them and you that we could consider a TRB briefing or review. Please let me know your thoughts on this and if there are any other key OIS resources we need to pull into this discussion.

Thanks,

Jon

Message

From: Gray, Edward M. (CMS/OIS) [NotResp]
[NotResp]
Sent: 9/11/2013 5:00:55 PM
To: Chao, Henry (CMS/OIS) [NotResp]; Linares,
George E. (CMS/OIS) [NotResp]
Stevenson, Corey B. (CMS/OIS) [NotResp]
[NotResp] Outerbridge, Monique (CMS/OIS) [NotResp]
[NotResp] Grothe, Kirk A. (CMS/OIS) [NotResp]
[NotResp] Walsh,
Timothy P. (CMS/OIS) [NotResp]
Plaucher, Mark J. (CMS/OIS) [NotResp]
[NotResp]
CC: Trenkle, Tony (CMS/OIS) [NotResp]
[NotResp] King, Terris (CMS/OIS) [NotResp]
[NotResp]; Mellor, Michael (CMS/OIS) [NotResp]
[NotResp] Byczkowski, Roxanne (CMS/OIS) [NotResp]
[NotResp] Fryer, Teresa M. (CMS/OIS) [NotResp]
[NotResp]
Subject: RE: Trusted Internet Connection (TIC) Update

Henry,

Attached is a list of concerns/issues that we have never been able to get HHS to respond to despite repeated communications and discussions at various levels. We reviewed these concerns with Tony and Terris on Monday and Tony was planning on raising these concerns with Frank Baitman at his next meeting. Currently, the team has not engaged in the development of any transition plan pending resolution of the expressed CMS concerns.

Ed

Ed Gray

Centers for Medicare & Medicaid Services (CMS)

Office of Information Services (OIS)

Enterprise Data Center Group (EDCG)

410.786.2616 edward.gray@cms.hhs.gov

7500 Security Blvd., N1-19-27

Baltimore, MD 21244-1850

Need more information? Please visit [the OIS website](#).

INFORMATION NOT RELEASABLE TO THE PUBLIC UNLESS AUTHORIZED BY LAW: This information has not been publicly disclosed and may be privileged and confidential. It is for internal government use only and must not be disseminated, distributed, or copied to persons not authorized to receive the information. Unauthorized disclosure may result in prosecution to the full extent of the law.

From: Chao, Henry (CMS/OIS)

Sent: Wednesday, September 11, 2013 12:24 PM

To: Linares, George E. (CMS/OIS); Stevenson, Corey B. (CMS/OIS); Margush, Doug C. (CMS/OIS); Outerbridge, Monique

(CMS/OIS); Grothe, Kirk A. (CMS/OIS); Gray, Edward M. (CMS/OIS); Walsh, Timothy P. (CMS/OIS); Plaugher, Mark J. (CMS/OIS)

Cc: Trenkle, Tony (CMS/OIS); King, Terris (CMS/OIS); Mellor, Michael (CMS/OIS); Byczkowski, Roxanne (CMS/OIS); Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Coutts, Todd (CMS/OIS); Berkley, Katrina (CMS/OIS); Rhones, Rhonda D. (CMS/OIS)

Subject: Fw: Trusted Internet Connection (TIC) Update

Do we already have a prioritized cutover plan that accounts for the Marketplace schedule?

Does that include factoring in Verizon-TMRK and HP outbound and inbound Internet connections on and off CMSNet?

Thanks.

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244
301-492-4100 (Pri)
410-786-1800 (Alt)
(b)(6) BB)

From: Charest, Kevin (OS/ASA/OCIO/OIS)

Sent: Wednesday, September 11, 2013 11:47 AM

To: OS - CIOLIST; OS - CIOALT; OS - HHS CISO Council

Subject: Trusted Internet Connection (TIC) Update

Colleagues:

We are moving forward with HHS's plans to transition OPDIVs to the Trusted Internet Connection (TIC). I appreciate the time your staff has taken to participate in the TIC working group meetings and support you have provided in preparations leading up to this transition. We are near completion of the Authorization to Operate (ATO), and will begin to send out preliminary documentation to your Team including the OPDIV Cutover questionnaire, the Service Level Agreement, and the Interconnection Security Agreement (ISA). Please work with your staff to ensure the timely provision of the information we need to accommodate a smooth transition. Through these preliminary efforts, we'll be working with your staff to schedule your OPDIV's transition and ensure you have the information to support your internal change management processes. I will be providing a more thorough review of the TIC at the September 25th CIO Council meeting.

Thanks in advance for your assistance with these efforts.

Kevin

Kevin Charest Ph.D., CISSP, PMP
Chief Information Security Officer
U.S. Department of Health and Human Services

Email: Kevin.Charest@hhs.gov

NotResp

Ofc. 202-690-5548; Mobile

(b)(6)



Message

From: Ashbaugh, Jason L. (CMS/OIS); [NotResp]
[NotResp]
Sent: 9/26/2013 9:55:30 PM
To: Linares, George E. (CMS/OIS); [NotResp]
[NotResp]; Every, Steven (CMS/OIS); [NotResp]
[NotResp]; Margush, Doug C. (CMS/OIS); [NotResp]
[NotResp]
Subject: RE: PII Process for Help Desk (Urgent)

In re-reading this I see the other side of the issue as well being discussed (not how we handle this internally, but an external secure webmail type solution).

If it's webmail, and it uses TLS, we're fine. That's the equivalent to [NotResp] we already use for exchange to outlook / mobile devices, and should be sufficient to protect transport.

The third option is something like PKI to leverage PIV certs, etc... or other types of PKI infrastructure.

[NotResp] or services like it seem like the simplest to use from what I've seen to be honest.

Thanks,

Jason L. Ashbaugh
CMS Computer Security Incident Response (CSIRT) - Lead
Enterprise Information Security Group (EISG)
Centers for Medicare & Medicaid Services
(w) 410.786.3017
(bb) [NotResp]

From: Ashbaugh, Jason L. (CMS/OIS)
Sent: Thursday, September 26, 2013 5:28 PM
To: Linares, George E. (CMS/OIS); Every, Steven (CMS/OIS); Margush, Doug C. (CMS/OIS)
Subject: RE: PII Process for Help Desk (Urgent)
So, it's two problems.

On the one hand, Tom is correct -- it provides marginal security to send the [NotResp]

On the other, that's because the [NotResp]

[NotResp]

Alternatives exist that are way better, like secured webmail sites like OIG [NotResp] (EDCG looked into this for adhoc stuff that doesn't make sense to EFT).

Thanks,

Jason L. Ashbaugh
CMS Computer Security Incident Response (CSIRT) - Lead
Enterprise Information Security Group (EISG)

Centers for Medicare & Medicaid Services

(w) 410.786.3017

(bb) (b)(6)

From: Linares, George E. (CMS/OIS)

Sent: Thursday, September 26, 2013 5:21 PM

To: Ashbaugh, Jason L. (CMS/OIS); Every, Steven (CMS/OIS); Margush, Doug C. (CMS/OIS)

Subject: FW: PII Process for Help Desk (Urgent)

Thoughts – I am on Tom's side. Should encrypted (secured) be good enough?

George Linares

Acting Chief Technology Officer

Centers for Medicare & Medicaid Services (CMS)

☎ 410.786.2866 ✉ george.linares@cms.hhs.gov

7500 Security Blvd., N3-15-25

Baltimore, MD 21244-1850

Need more information? Visit [the OIS website](#).

From: Schankweiler, Thomas W. (CMS/OIS)

Sent: Thursday, September 26, 2013 5:05 AM

To: Linares, George E. (CMS/OIS)

Subject: FW: PII Process for Help Desk (Urgent)

George,

See below, we should talk about getting some time about getting secure e-mail functions within CMS as a CIO directive. This whole thing [NotResp] is a bit antiquated and only marginally acceptable from a security perspective.

Tom

From: Schankweiler, Thomas W. (CMS/OIS)

Sent: Thursday, September 26, 2013 5:02 AM

To: Burke, Sheila M. (CMS/OIS)

Cc: Grothe, Kirk A. (CMS/OIS); Bush-Warren, Theresa (CMS/OIS); Skinner, Dennis R. (CMS/OIS)

Subject: RE: PII Process for Help Desk (Urgent)

Sheila,

If the Issuer has a secure e-mail function which the help desk can use to retrieve the file then following that process would supersede the need to perform the less secure process which CMS is instituting. [NotResp]

[NotResp]

Tom

From: Burke, Sheila M. (CMS/OIS)

Sent: Monday, September 23, 2013 10:39 AM

To: Schankweiler, Thomas W. (CMS/OIS)

Cc: Grothe, Kirk A. (CMS/OIS); Bush-Warren, Theresa (CMS/OIS); Skinner, Dennis R. (CMS/OIS)

Subject: PII Process for Help Desk (Urgent)

Importance: High

Tom,

This is a follow-up to our earlier conversation about the PII process for the help desk. The slide below is currently being communicated as the process. In addition, the Issuer Communications Team specifically is inquiring about a situation where an Issuer uses a secure email function – causing the helpdesk receiver (or whomever) to create an account in order to access the content of an email. Does this also require PW protected files

NotResp

NotResp

PII Data: Scenarios & Instruction

When an Issuer places a phone call into the Help Desk:

While on a call the Help Desk will record a ticket number and ask the Issuer to send the supporting (password protected) documents with the ticket number in the subject line while

NotResp

When the Issuer contacts the Help Desk outside of business hours:

The Issuer will send an e-mail to the Help Desk. All supporting documents will be attached as an encrypted password protected document.

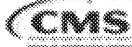
NotResp

NotResp

When the PII Data file is too large to send via email:

The Help Desk will open a ticket and send to the EFT team to help setup a onetime EFT transmission that will be attached to the ticket.

*In accordance with NIST/CMS, the CMS Information Security and Privacy Offices have implemented a process for protecting personally identifiable information (PII) and creating policy requirements for CMS staff and partners to notify the proper authorities in the event that an incident, breach, or potential breach, to PII has occurred.



NOTES: THIS INFORMATION IS FOR THE PURPOSE OF THE PII PROCESS ONLY. THIS INFORMATION HAS BEEN PUBLICLY DEVELOPED AND IS NOT PROTECTED AND NOT IDENTIFIED. IT IS AN INTERNAL GOVERNMENT DOCUMENT AND MUST NOT BE DISSEMINATED, DISTRIBUTED, OR RELEASED TO THE PUBLIC OR TO ANY OTHER ENTITY. UNAUTHORIZED DISCLOSURE MAY RESULT IN PROSECUTION TO THE FULL EXTENT OF THE LAW.

6

Sheila M. Burke,

Deputy Division Director

Division of Health Insurance Marketplace (DHIM)

Consumer Information and Insurance Systems Group

Office of Information Services

(410) 786-5951 - Office

(b)(6)

- BlackBerry

Sheila.Burke@cms.hhs.gov

Message

From: Gray, Edward M. (CMS/OIS) [NotResp]
[NotResp]
Sent: 8/16/2013 11:39:39 AM
To: Giles, April (CMS/OIS) [NotResp]
[NotResp]
CC: Linares, George E. (CMS/OIS) [NotResp]
[NotResp] Shields, Karen M. (CMS/OIS) [NotResp]
[NotResp]
Stevenson, Corey B. (CMS/OIS) [NotResp]
[NotResp]
Subject: RE: TRB Consult – Planning for Critical IT, Operations, and Security for ESD
Attachments: ATT20462; ATT20308

Ok. Thanks April. If I am reading your response correctly, it sounds like we can control and restrict access into CMS systems for those 100 users to ensure that their only access occurs through the VPN and utilizes PIV based authentication.

Ed

Ed Gray

Centers for Medicare & Medicaid Services (CMS)

Office of Information Services (OIS)

Enterprise Data Center Group (EDCG)

410.786.2616 edward.gray@cms.hhs.gov

7500 Security Blvd., N1-19-27

Baltimore, MD 21244-1850

Need more information? Please visit [the OIS website](#).

INFORMATION NOT RELEASABLE TO THE PUBLIC UNLESS AUTHORIZED BY LAW: This information has not been publicly disclosed and may be privileged and confidential. It is for internal government use only and must not be disseminated, distributed, or copied to persons not authorized to receive the information. Unauthorized disclosure may result in prosecution to the full extent of the law.

From: Giles, April (CMS/OIS)
Sent: Thursday, August 15, 2013 9:51 PM
To: Gray, Edward M. (CMS/OIS)
Cc: Linares, George E. (CMS/OIS); Shields, Karen M. (CMS/OIS); Stevenson, Corey B. (CMS/OIS)
Subject: RE: TRB Consult – Planning for Critical IT, Operations, and Security for ESD

Ed,

The ESD consult occurred on 7/10/13 and I was added to the TRB team on 7/24/13. So, you are correct, I was not engaged at the time of the consult.

As for your question:

“does the federation create a “backdoor” that impacts our ability to ensure that any access they have to CMS systems only occurs using their PIV card”.

Any Federation presumes that both organizations trust each other's identity vetting, credential management, device management, authentication, PKI, and AD management policies & processes. Not sure if CMS has reviewed and accepted the risk within SERCO's policies & processes, or if SERCO has done the same.

Additionally, depending on how the Active Directory Federation Service is implemented, there are mechanisms for insuring a certain level of assurance for the claimed identity (security tokens). There are also boundaries that can be placed on the resource accessed (i.e. employing claims-aware applications), as well as the account authenticated. These boundaries limit the risk for the resource domain (CMS).

Still, those that require PIV cards, will have to be sponsored by CMS, and therefore added to the CMS.local domain. But as I understand it, those that require PIV will amount to far less than 100 of the 1500 expected total subscribers.

Hope this helps.

Thanks

April

From: Gray, Edward M. (CMS/OIS)
Sent: Wednesday, August 14, 2013 4:56 PM
To: Giles, April (CMS/OIS)
Cc: Linares, George E. (CMS/OIS); Shields, Karen M. (CMS/OIS); Stevenson, Corey B. (CMS/OIS)
Subject: FW: TRB Consult – Planning for Critical IT, Operations, and Security for ESD

April,

Not sure if you are fully engaged in the TRB process yet so wanted to check to see if you were involved in or had seen this consult result below. They are suggesting an AD federation approach with this new contractor, SERCO who will be providing "call center" services for marketplace. Within their AD, they will have some number of people that will also receive CMS user id's and assumedly be included in CMS.Local and the PIV lockdown effort.

For those users that would be in CMS.Local and assumedly in SERCO's AD as well, does the federation create a "backdoor" that impacts our ability to ensure that any access they have to CMS systems only occurs using their PIV card.

I believe we are moving forward with this approach regardless but thought it would be good to level set on this just so we were all on the same page.

Appreciate any thoughts you would have - Ed

Ed Gray

Centers for Medicare & Medicaid Services (CMS)

Office of Information Services (OIS)

Enterprise Data Center Group (EDCG)

<< OLE Object: Picture (Device Independent Bitmap) >> 410.786.2616 << OLE Object: Picture (Device Independent Bitmap) >> edward.gray@cms.hhs.gov

7500 Security Blvd., N1-19-27

Baltimore, MD 21244-1850

Need more information? Please visit [the OIS website](#).

INFORMATION NOT RELEASABLE TO THE PUBLIC UNLESS AUTHORIZED BY LAW: This information has not been publicly disclosed and may be privileged

and confidential. It is for internal government use only and must not be disseminated, distributed, or copied to persons not authorized to receive the information. Unauthorized disclosure may result in prosecution to the full extent of the law.

From: Linares, George E. (CMS/OIS)

Sent: Thursday, August 08, 2013 3:07 PM

To: CMS Technical Review Board; 'chris.sullivan@serco-na.com'; 'Edward.Lee@serco-na.com'; 'marc.sosa@serco-na.com'; 'jim.schifalacqua@serco-na.com'; 'tony.clements@serco-na.com'; 'james.quinn@serco-na.com'; 'david.correll@serco-na.com'; 'jeremy.jennings@serco-na.com'; 'david.schopper@serco-na.com'; 'sonny.nasir@serco-na.com'; 'lakshmi.manambedu@cgifederal.com'; 'kkim@qssinc.com'; Margush, Doug C. (CMS/OIS); Dill, Walter (CMS/OIS); Trenkle, Tony (CMS/OIS); Byczkowski, Roxanne (CMS/OIS)

Cc: Pittman, Junious (CMS/CCIIO); Carabai, Jinean (CMS/CCIIO); Van, Hung B. (CMS/OIS); Henry, Galina (CMS/OIS); Oh, Mark U. (CMS/OIS); Kerr, James T. (CMS/CMHPO); Block, Lauren M. (CMS/CCIIO); Grothe, Kirk A. (CMS/OIS); Roche, Jacqueline R. (CMS/CCIIO); Schankweiler, Thomas W. (CMS/OIS); Gray, Edward M. (CMS/OIS); Stevenson, Corey B. (CMS/OIS); Berkley, Katrina (CMS/OIS); Wallace, Mary H. (CMS/OC); Booth, Jon G. (CMS/OC); Harmatuk, Frances R. (CMS/OC); Rhones, Rhonda D. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Thurston, Robert (CMS/CTR); Carter, Cathy T. (CMS/OIS); Gass, Carole F. (CMS/OIS)

Subject: RE: TRB Consult – Planning for Critical IT, Operations, and Security for ESD

All,

During the TRB consult 3 options were discussed:

Option-1: Federation

Assumptions/ Flow:

- ESD shall have its own identity management system that meets the CMS security requirements
- ESD is responsible for the SCA testing towards the ATO process
- ESD needs to have network connectivity to establish the federation with EIDM
- ESD is responsible for maintaining the user profile/access/authentications log for the auditing purposes
- ESD needs to maintain **NotResp** The user profiles are to be stored in the **NotResp** to the **NotResp**
NotResp can communicate with **NotResp**
- ESD user profiles will not be created in EIDM, Hence EIDM will not be aware of the ESD user profile
- EIDM will capture the ESD user access logs at the System Account level but not at the ESD User level

Option-2: EIDM/ Portal

Assumptions/ Flow:

- ESD user will access the CMS Portal and registers in to EIDM using the EIDM registration process to get the LOA1 account
- EIDM will configure one of the WaaS frameworks to suite the ESD application access approval workflow requirements
- Sample WaaS workflow can be: EIDM administration approves ESD Business Owner; ESD Business Owner approves ESD HR Representative; ESD HR Representative approves rest of the ESD users; ESD user role information is stored in EIDM
- ESD will be accessible via FFM which is protected by EIDM WebGate, Hence ESD users will login to FFM to get access to ESD
- As part of the FFM/ESD authentication, EIDM will pass the user credential to ESD via HTTP header
- ESD will retrieve the user role information from EIDM by consuming the WaaS consumption services (web services or stored procedure) using the user credential

Option-3: Replication of ESD **NotResp** at TM and use **NotResp** to authenticate

Assumptions/ Flow:

- ESD shall have its own identity management system that meets the CMS security requirements
- ESD is responsible for the SCA testing towards the ATO process
- ESD needs to maintain the user profiles are to be stored in the
- ESD will be replicated to TM and configure the same with the EIDM
- ESD will be accessible via FFM which is protected by EIDM. Hence ESD users will login to FFM to get access to ESD
- As part of the FFM/ESD authentication, EIDM will pass the user credential to ESD via HTTP header
- ESD will retrieve the ESD user role information from ESD using the user credential

In consultation with all the teams, the TRB, EIDM, CIISG, CCIIO and other teams supporting ESD, pursuing Option 1 is the more practical and expedient approach to implement and meet the aggressive timelines. The direction to all the teams is to pursue and implement Option 1, federation approach with SERCO's AD platform.

Regards,

George Linares

Acting Chief Technology Officer

Centers for Medicare & Medicaid Services (CMS)

<< OLE Object: Picture (Device Independent Bitmap) >> 410.786.2866 << OLE Object: Picture (Device Independent Bitmap) >> george.linares@cms.hhs.gov
7500 Security Blvd., N3-15-25
Baltimore, MD 21244-1850

Need more information? Visit [the OIS website](#).

-----Original Appointment-----

From: CMS Technical Review Board

Sent: Tuesday, July 09, 2013 9:35 AM

To: CMS Technical Review Board; Linares, George E. (CMS/OIS); Chao, Henry (CMS/OIS); 'chris.sullivan@serco-na.com'; 'Edward.Lee@serco-na.com'; 'marc.sosa@serco-na.com'; 'jim.schifalacqua@serco-na.com'; 'tony.clements@serco-na.com'; 'james.quinn@serco-na.com'; 'david.correll@serco-na.com'; 'jeremy.jennings@serco-na.com'; 'david.schopper@serco-na.com'; 'sonny.nasir@serco-na.com'; 'lakshmi.manambedu@cgifederal.com'; 'kkim@qssinc.com'; Margush, Doug C. (CMS/OIS); Dill, Walter (CMS/OIS); Trenkle, Tony (CMS/OIS); Byczkowski, Roxanne (CMS/OIS)

Cc: Pittman, Junious (CMS/CCIIO); Carabai, Jinean (CMS/CCIIO); Van, Hung B. (CMS/OIS); Henry, Galina (CMS/OIS); Oh, Mark U. (CMS/OIS); Kerr, James T. (CMS/CMHPO); Block, Lauren M. (CMS/CCIIO); Grothe, Kirk A. (CMS/OIS); Roche, Jacqueline R. (CMS/CCIIO); Schankweiler, Thomas W. (CMS/OIS); Gray, Edward M. (CMS/OIS); Stevenson, Corey B. (CMS/OIS); Berkley, Katrina (CMS/OIS); Wallace, Mary H. (CMS/OC); Booth, Jon G. (CMS/OC); Harmatuk, Frances R. (CMS/OC); Rhones, Rhonda D. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Thurston, Robert (CMS/CTR); Carter, Cathy T. (CMS/OIS); Gass, Carole F. (CMS/OIS)

Subject: TRB Consult – Planning for Critical IT, Operations, and Security for ESD

When: Wednesday, July 10, 2013 11:00 AM-1:00 PM (UTC-05:00) Eastern Time (US & Canada).

Where: C-112

**TRB Consult – Planning for Critical IT, Operations, and Security for ESD;
Requested by George Linares, OIS**

Dial-In information:

Central Office Participants: (b)(6)
All other Participants: (b)(6)
Meeting ID: (b)(6)

To join the meeting via webinar:

Please provide with an e-copy of any presentation materials by July 9th by noon (CMS Technical Review Board). Have hardcopy materials available on July 10th for distribution to all attendees. (There are 15 TRB members) You may distribute this appointment to others as needed.

Message

From: Trenkle, Tony (CMS/OIS) [NotResp]
[NotResp]
Sent: 8/26/2013 8:51:37 PM
To: Byczkowski, Roxanne (CMS/OIS) [NotResp]
[NotResp]
CC: King, Terris (CMS/OIS) [NotResp] Chao, Henry
(CMS/OIS) [NotResp] Linares, George E.
(CMS/OIS) [NotResp]
Outerbridge, Monique (CMS/OIS) [NotResp]
[NotResp] Trenkle, Tony (CMS/OIS) [NotResp]
[NotResp]
Subject: Agenda Items for the Frank Baitman meeting on Thursday

Rox,

Here are the agenda items for our meeting with Frank on Thursday:

1. Update on Marketplace SCA Testing-Teresa and Tom Schankweiller
2. MFA-Tom and Marc Richardson
3. HSPD-12-Marketplace Contractors-Corey and Karen
4. TIC and EaaS Status-Frank

I believe that everything will be a verbal except HSPD-12.

Henry,

We probably also should give him some kind of update on CGI so that he can understand how it is affecting the security testing.

Message

From: Linares, George E. (CMS/OIS) [NotResp]
Sent: 6/17/2013 9:37:00 PM [NotResp]
To: [NotResp]
 King, Terris (CMS/OIS) [NotResp]
CC: Chao, Henry (CMS/OIS) [NotResp]
Subject: CTO Update 6/17

Just a couple of points from 6/10-6/14. By the way, I did not send any updates last week, as I did not have anything of interest to report.

Physician Value & MicroStrategy

- In 2014 PV is expecting to have 300K users accessing the PQRS report. Currently [NotResp] is being used, but to scale the solution to support the 2014 volumes, there is a price tag of approx. \$12 million mainly attributed to licensing costs. I am working with EDG and ISDDG to find alternatives that are more cost efficient. We have also reached out to OEM to seek [NotResp] support for potential open source alternatives. [NotResp] is now supporting this effort.

Health Insurance Casework System (HICS)

- After working with ISSDG, CIISG, EDCG and Henry, we came to the conclusion to recommend the use of EUA to support HICS. There is a 75% overlap on the user population, and it has no impact on EIDM. Although EIDM could support the effort, it would require some development work, which given the aggressive timelines could be a risk to the project. On the other hand, EUA does not require any software development and it has a bulk-upload capability to update existing users' profiles.

Vendor week concluded successfully

- We believe to have uncovered a "nugget" of innovation with a tool already being used at CMS by EISG, but not well known across [NotResp]. A tool that collects system log information for security purposes, it has shown to have other capabilities that could help system maintainers in monitoring their applications and accessing their logs for troubleshooting. The best thing is that these capabilities are already included in the licensing agreement. We are planning to have an more in-depth review with Splunk.

Thanks

George Linares

Acting Chief Technology Officer

Centers for Medicare & Medicaid Services (CMS)

410.786.2866 | george.linares@cms.hhs.gov

7500 Security Blvd., N3-15-25

Baltimore, MD 21244-1850

Need more information? Visit [the OIS website](#).

Message

From: Richardson, Marc D. (CMS/OIS) [NotResp]
[NotResp]
Sent: 9/23/2013 1:36:12 PM
To: 'Minze Chien' [MChien@qssinc.com]; Linares, George E. (CMS/OIS) [NotResp]
[NotResp] CMS - EIDM CMS Team [NotResp]
[NotResp]; Carter, Cathy T.
(CMS/OIS) [NotResp] Didier
Simonazzi' [didier.simonazzi@oracle.com]; 'Pardha Reddy' [pardha.reddy@oracle.com]; 'Clayton Donley'
[clayton.donley@oracle.com]; 'Amit Jasuja' [amit.jasuja@oracle.com]
CC: 'Bikram Bakshi' [bbakshi@qssinc.com]; 'PK Malhotra' [pmalhotra@qssinc.com]; 'Michael Finkel'
[mfinkel@qssinc.com]; 'Yuri Radams' [yradams@qssinc.com]; 'Kovilvenni Ramaswamy' [kramaswamy@qssinc.com];
'Krishnamoorthi Ganesan' [kganesan@qssinc.com]; 'Nitin Matta' [nmatta@qssinc.com]; 'Girish Shetty'
[gshetty@qssinc.com]; 'Ivan Vinogradov' [ivinogradov@qssinc.com]; 'Vignesh Srinivasan' [vsrinivasan@qssinc.com];
'Bavani Murari' [bmurari@qssinc.com]; 'EIDM_Team_Leads' [EIDMTeamLeads@qssinc.com]
Subject: RE: EIDM Daily Updates - Tracking all [Not] Parallel Work Streams ... 9/22/2013

Are all of the [NotResp] recommendations #3 going to go into production at the same time?

Regards,



Marc Richardson, PMP, Director

Centers for Medicare & Medicaid Services (CMS)
Office of Information Services (OIS)
Innovative Healthcare Delivery Systems Group (IHDSG)
Division of Healthcare Information Systems (DHIS)
☎ 410.786.0016 ✉ marc.richardson@cms.hhs.gov

(b)(6)

7500 Security Blvd., N3-17-07
Baltimore, MD 21244-1850

Need more information? Please visit [the OIS website](#).



From: Minze Chien [mailto:MChien@qssinc.com]
Sent: Sunday, September 22, 2013 7:53 PM
To: Richardson, Marc D. (CMS/OIS); Linares, George E. (CMS/OIS); CMS - EIDM CMS Team; Carter, Cathy T. (CMS/OIS);
'Didier Simonazzi'; 'Pardha Reddy'; 'Clayton Donley'; 'Amit Jasuja'
Cc: Bikram Bakshi; PK Malhotra; Michael Finkel; Yuri Radams; Kovilvenni Ramaswamy; Krishnamoorthi Ganesan; Nitin

Matta; Girish Shetty; Ivan Vinogradov; Vignesh Srinivasan; Bavani Murari; EIDM_Team_Leads

Subject: EIDM Daily Updates - Tracking all EIDM Parallel Work Streams ... 9/22/2013

Marc,

As promised, here is the update for all work streams we are tracking.

High Level Summary – 9/22/2013

ID	Work Stream	Status	Issues/Risks	Target Completion Date
1	Production Login Issue	<ul style="list-style-type: none"> Intermittent login issue – All related logs have been closely monitored. QSSI is still working with [NotRes] on this issue. [NotRe] replication issue- [NotRe] data are not replicated to [NotResp] - Resolved. All three [NotRe] are running without issues and all in sync. 		TBD
2	Portal Provisioning/Registration Issues	<ul style="list-style-type: none"> Intermittent [NotRe] issue - registration errors as reported by the users [NotRe] has provided recommendations on the issue. QSSI will implement the changes in DEV and TEST tonight. [NotRe] issues – Worked with SAIC in identifying the list of users who passed phone ID proofing with Experian but failed the Manual ID proofing process with EIDM. 52 users were identified and stepped up to LOA2. Helpdesk team to send communication to the users 		September 23, 2013
3	Oracle Recommendations	<ul style="list-style-type: none"> Modify the [NotResp] response timeout setting to 4 seconds from 2 seconds. – Completed. Synchronize the configuration changes between [NotRe] to be exactly the same. Confirm that [NotResp] are receiving equivalent amount of traffic in terms of request volume. Inordinately large number of requests coming to [NotRe] for users who authenticate - from where and why Make sure all [NotRe] instances have the same data, object class configuration, [NotResp] are tuned properly. Evaluate the replication configuration from the [NotRe] in Terremark Data center to the BDC data center The recommendations made by the [NotRe] engineering team- QSSI will implement the changes in TEST tonight. 		TBD
4	IMPL1 Environment Setup	<ul style="list-style-type: none"> Rebuild [NotRe] from scratch - [NotRe] installation has been completed with integration with [NotResp] Manual custom code deployment for EIDM Release 1, 2, 3 – Working with [NotRe] in completing the pending items: [NotRe] connector, [NotResp] connector, [NotResp] Manager 		September 23, 2013

		<p>NotResp policies and WaaS Database provisioning.</p> <ul style="list-style-type: none"> • Pending regression testing • Completed: NotRe validation with NotRe is completed. Integration with NotRe completed. • Completed: Layer NotRe (VMs) were received from URS and verified. Firewall rules have been implemented by URS. We have confirmed all connectivity in place. Implementation of Layer NotRes completed. 		
5	Production user data setup	<ul style="list-style-type: none"> • Phase 1 – We submitted the request to Don Bartley (EIDM ISSO) from CMS for approval to copy production user data into Implementation 1 after de-identification of the data. Approval received from CMS <ul style="list-style-type: none"> ○ Completed: NotResp database data copy from PROD to IMPL Not data were sanitized on PROD servers before copying. All activities documented and signed off by EIDM Security. • Phase 2 – create/update automation script to generate user data into Implementation 1. <ul style="list-style-type: none"> ○ In progress 		September 23, 2013
6	Performance Testing	Once IMPL Not environment is ready we will run a full round of Performance testing including Identity and Access management services.		September 30, 2013
7	Performance Metrics Reporting (Tactical)	<p>Reporting for Registration, Access Management and Authentication Services.</p> <ul style="list-style-type: none"> • Completed more iteration of the revised scripts. • Continuing to analyze various data logs. 		September 23, 2013
8	eLDAP Logs for monitoring	<p>QSSI has initiated a discussion with BDC to come up with a process to automate the log dump from NotRes server to an EIDM server.</p> <ul style="list-style-type: none"> • Working with Nick Collingham, QSSI, and NotRes team to create a process for getting the access log regularly (hourly). • Firewall has been implemented for transferring NotResp access log files between NotResp and EIDM PROD. (Artifact artf155194 : EIDM PROD NotRes EIDM PROD NotResp) 		TBD
9	EIDM Elasticity	<p>Capacity Planning for stand by VMs to support scalability. Status: Per Terremark, we need CMS help to discuss with Doug Margush on providing available compute resource at Terremark that can be temporarily given to QSSI EIDM team to build and keep the servers on standby. We will need CMS assistance in putting a long term capacity expansion solution.</p>		TBD

10	Akamai Issue	<ul style="list-style-type: none"> We were asked by CGI & CMS to ensure that when user's login to <u>healthcare.gov</u> they are not redirected back to <u>cms.gov</u> and the cookies are generated for <u>healthcare.gov</u> and not <u>cms.gov</u>. Akamai solution for unsolicited logins may not work with the current FFM design and architecture. EIDM team is working with <u>NotRes p</u> product team, CMS and FFM team on options to resolve the issue. 		September 23, 2013
11	Federation for CSR and ESD	<ul style="list-style-type: none"> CSR in production has been completed ESD has been successfully federated in TEST. We are continuing to work with CGI, Serco and NGS. 		October 1, 2013
12	BDC Active-Active Build Out	<ul style="list-style-type: none"> Currently, BDC <u>NotResp</u> DEV is pending new firewall rules to complete the configuration. Global load balancer has now been finalized. BDC <u>NotResp</u> pending LM support to continue the configuration. The <u>NotResp</u> replication between BDC and TRMK has been broken due to unknown reasons. We have engaged the appropriate resources to investigate and fix this issue. We are holding a series of meetings with BDC and Portal team to plan out the active-active testing. Tentative Plan – BDC OAM DEV <ul style="list-style-type: none"> Configuration of <u>NotResp</u> application (Date: 9/27) Integration with portal (Date: 9/29) Functional Testing with Portal (Date: 10/4) BDC <u>NotResp</u> AL - <ul style="list-style-type: none"> Configuration of <u>NotResp</u> application (Date: 10/4) Integration with portal (Date: 10/7) Functional testing with Portal (Date: 10/11) Load testing with Portal (Date: 10/18) Load testing against <u>NotResp</u> system only, to find out break point for the <u>NotResp</u> system in BDC (Date: 10/25) BDC <u>NotResp</u> ROD - <ul style="list-style-type: none"> Configuration of <u>NotResp</u> application (Date: 10/27) Integration with portal (Date: 10/27) Functional testing with Portal (Date: 10/31) 	Due to the delay in getting the concurrence from all stakeholders of the GLB design and the pending firewall rules, the testing of BDC OAM DEV-EIDM TEST cannot occur until we complete IMPL1 buildup.	October 31, 2013
13	CMS Enterprise Portal Build up in CDS Data Center – EIDM Support	<p>CDS is standing up the failover site for CMS Enterprise Portal which connects to EIDM in TRMK</p> <ul style="list-style-type: none"> EDC Enterprise Portal PROD Environment – In Progress EDC Enterprise Portal IMP Environment – Completed (EIDM supported the <u>NotResp</u> configuration) 		TBD

Thanks.

Minze

Minze V. Chien, Ph.D., CISSP

Technical Director, IAM Strategic Solutions

QSSI | www.qssinc.com

10025 Governor Warfield Parkway, Suite 401

Columbia, MD 21044

(301) 977-7884 x305 and x223 (O)

mchien@qssinc.com

(b)(6)

CMMI ® Maturity Level 3 Rated

GSA Approved HSPD-12 System Integrator

Top 100 Diversity-Owned businesses in 2004 and 2005



This electronic mail (including any attachments) may contain information that is privileged, confidential, and/or otherwise protected from disclosure to anyone other than its intended recipient(s). Any dissemination or use of this electronic email or its contents (including any attachments) by persons other than the intended recipient(s) is strictly prohibited. If you have received this message in error, please notify the sender by reply email and delete the original message (including any attachments) in its entirety.

Message

From: Oh, Mark U. (CMS/OIS) [NotResp]
[NotResp]

Sent: 6/24/2013 3:58:28 PM

To: Linares, George E. (CMS/OIS) [NotResp]
[NotResp]; Robinson, Lori A. (CMS/CM) [NotResp]
[NotResp]; Miller, Daniel J. (CMS/OIS) [NotResp]
[NotResp]; Grothe, Kirk A. (CMS/OIS) [NotResp]
[NotResp]
Outerbridge, Monique (CMS/OIS) [NotResp]
[NotResp]

CC: Basavaraju, Venkat (CMS/OIS) [NotResp]

Subject: RE: Question re: issuer identifier assigned to an issuer employee's user ID

Hi Lori – let me know if below answers your question:

- In FFM/HIOS, user is restricted to particular modules (i.e. USP versus QHP)
- Within FFM/QHP, user has association to one or multiple Issuers (like MA/PD). Given that Issuer is defined at the state level, person from Aetna could have access to Issuer from multiple states. Meaning, just like MA/PD, Aetna user from CT will have access to Aetna data from multiple states (as long as they are associated and approved from HIOS roles perspective)
- Then, user will access to Issuer data and all associated QHP data.

Long story short, user is associated with highest level is single or multiple Issuer IDs (e.g., 40057 representing Aetna in ND).

Best,

Mark

From: Linares, George E. (CMS/OIS)
Sent: Monday, June 24, 2013 11:56 AM
To: Robinson, Lori A. (CMS/CM); Oh, Mark U. (CMS/OIS); Miller, Daniel J. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Outerbridge, Monique (CMS/OIS)
Cc: Basavaraju, Venkat (CMS/OIS)
Subject: RE: Question re: issuer identifier assigned to an issuer employee's user ID

Including Monique and Kirk

George Linares

Acting Chief Technology Officer

Centers for Medicare & Medicaid Services (CMS)

410.786.2866 george.linares@cms.hhs.gov

7500 Security Blvd., N3-15-25

Baltimore, MD 21244-1850

Need more information? Visit [the OIS website](#).

From: Robinson, Lori A. (CMS/CM)
Sent: Monday, June 24, 2013 10:09 AM
To: Oh, Mark U. (CMS/OIS); Miller, Daniel J. (CMS/OIS)
Cc: Linares, George E. (CMS/OIS); Basavaraju, Venkat (CMS/OIS); Robinson, Lori A. (CMS/CM)
Subject: Question re: issuer identifier assigned to an issuer employee's user ID
Importance: High

Hi guys –

As you may have heard, we've been instructed to use EUA to control user access for CCIIO's new casework system. In order to make this happen, we need to direct Lockheed Martin to make the necessary changes to the EUA system to support this new line of business.

I need to know ASAP how you are controlling access to issuer data for the FFM systems. **Specifically, what level of issuer identifier are you assigning to an individual issuer user ID to restrict their access to only their company's data?**

Example: In MA/PD, a plan employee's user ID must be assigned to one or more "contract numbers" that the application uses to determine who they work for and which company data they can edit/view.

What is the equivalent value in the FFM world? Are you using the highest level issuer ID (e.g., NotResp) Or are you using a lower level, like the standard component ID (e.g., NotResp) Or are you using something else?

I've asked several people and cannot get a definitive answer. I would greatly appreciate a response. Thanks.

Lori

Lori Robinson
Director | Division of Plan Data
Medicare Drug Benefit and C & D Data Group
Center for Medicare
Centers for Medicare & Medicaid Services
lori.robinson@cms.hhs.gov
410.786.1826 (phone)



WEEKLY PROJECT STATUS REPORT

CLIENT/PROJECT:	CMS/Enterprise Identity Management	YELLOW
PROJECT MANAGER:	Girish Shetty	
PROGRAM DIRECTOR:	Nitin Matta	
CLIENT CONTACT:	Deborah Seate, Venkat Basavaraju, Robert Burger, Todd Northwood, Sharlene Mansaray, Cathy Carter, Marc Richardson, Carla Jones, Tim Purcell, Mark Small	
STATUS PERIOD:	07/29/2013 to 08/04/2013	
STATUS SUMMARY		
TASKS COMPLETED /DELIVERIES FOR THIS PERIOD – 07/29/2013 to 08/04/2013		
Following are activities completed for this week:		
<div>1. EIDM TEST - Emergency fix for Validating the Regular Expression used for Phone Numbers was successfully deployed</div> <div>2. EIDM IMPL - Emergency fix for Validating the Regular Expression used for Phone Numbers was successfully deployed</div> <div>3. EIDM PROD - Emergency fix for Validating the Regular Expression used for Phone Numbers was successfully deployed</div> <div>4. EIDM TEST - Emergency fix for the EIDM Web services changes for handling the Spanish characters in FFM Lite Account creation was successfully deployed.</div> <div>5. EIDM IMPL - Emergency fix for the EIDM Web services changes for handling the Spanish characters in FFM Lite Account creation was successfully deployed.</div> <div>6. EIDM PROD - Emergency fix for the EIDM Web services changes for handling the Spanish characters in FFM Lite Account creation was successfully deployed.</div> <div>7. Provide round the clock 24 hour support to the CGI FFM team with the trouble shooting and Performance testing session for FFM Lite accounts.</div> <div>8. Release 3 build 11.2 was successfully deployed in the Test environment.</div> <div>9. Performance Testing on going in the Impl1 environment, also commenced web services testing of Lite Accounts in Impl0 environment.</div> <div>10. QSSI EIDM team continue to build the BDC environment for the [WORK] active solution [.asd]</div> <div>11. No Severity #1 or Severity #2 tickets currently opened in production. EIDM Helpdesk tickets status for this week:<div><div>a. # of New Tickets Opened between 07/29/2013 to 08/04/2013 → 14</div><div>b. # of Tickets Closed between 07/29/2013 to 08/04/2013 → 15 (Note: this number may include tickets opened from previous weeks).</div><div>c. # of Tickets unresolved from 03/25/2013 to 08/04/2013 → 1</div></div></div> <div>12. QSSI supported ongoing application integration meetings for SHOP, CSR, FFM and Zone and shared meeting minutes as applicable. QSSI also supported</div>		

Application integration meetings for the new applications in the pipeline like **NotResp** and shared meeting minutes.

TASKS PLANNED/DELIVERIES FOR THIS PERIOD - 08/05/2013 to 08/11/2013

1. Deploy EIDM Release 3 Build 11.3 in the Test and Impl environment
2. Tentatively Support the zOne webgate installation and configuration in the Production environment. Date not finalized yet.
3. Continue the performance testing effort in the Impl1 and Impl0 environment
4. Test the new sub codes for Augmented Analytics provided by SAIC.
5. Continue building the BDC OAM environment for the active active solution
6. Continue requirement gathering for new applications like **NotResp** integrating with EIDM
7. Continue Release 3 Build 11.3 testing and code fixes in the Test and Implementation Environment.
8. Analyze and Resolve outstanding issues in production, report delivery production status report on EIDM production and helpdesk operations.

Scheduled Deployments in the EIDM Environment:

Environment	Start Time	End Time	Activity
PROD	08/11/2013	08/11/2013	EIDM PROD - In support of Agent broker
IMPL 0	08/08/2013	08/08/2013	EIDM IMPL - In support of Agent broker
TEST	08/06/2013	08/06/2013	EIDM TEST weekly deployment - To support agent broker
IMPL 1	7/24/2013	8/6/2013	EIDM Performance testing

EIDM Application Integration Status

Applications	Current Status	Tentative Prod	CMS GTL
--------------	----------------	----------------	---------

		Date	
FFM	<ul style="list-style-type: none"> Deployed to Production. Integration testing in progress. EIDM team is working with CGI to resolve the uniqueness check issue found during testing. 	Already deployed	Susan Tudor/ Megan Reilly
Assister Integration (Agent Broker)	<ul style="list-style-type: none"> MLN data store – received info from Mark Oh on MLN datastore. It will be a single table in the App Zone of the FFM. We still need the date source details to set up firewall rules for connectivity. EIDM will query the table to validate information provided by user. 	August 11th 2013	Mark Oh?
SHOP	<ul style="list-style-type: none"> Testing in progress. SHOP team is working on the firewall issues. 	Sept 1st 2013	Hannah Yoo
CSR	<ul style="list-style-type: none"> Integration activities are in progress between EIDM, CSR and FFM teams. 	Sept 1st 2013	Frances Harmatuk/ Jeffrey Burdette
ASP	<ul style="list-style-type: none"> A CR for setting up [redacted] in Test environment has been created but the deployment to Test is on hold until Lite Accé [redacted]. NotResp NotResp 	Dec 15th 2013	Sarah Harding
ASET	<ul style="list-style-type: none"> ASET confirmed that it will use [redacted]. No need to pass ASET 2 user ID. The user will be asked for that info on the ASET website. ASET wants to modify the EIDM framework to satisfy the requirement of asking the user whether they have an existing ASET User ID. Mockups with descriptive help text for the ASET roles will be shared to hopefully avoid this modification. 	March 2nd 2014	Gladys Wheeler
EPPE	<ul style="list-style-type: none"> No update this week. Meeting needs to be scheduled. 	March 2nd 2014	
MACPro	<ul style="list-style-type: none"> CR to be submitted for setting up the application/roles in EIDM Test Environment. Recurring meeting has been set up starting August 13, 2013. 	Dec 8th 2013	Nancy Martin
	<ul style="list-style-type: none"> Testing in progress in EIDM test environment. NotRes attribute role routing development is in progress. All [redacted] sp roles have been set to Loa 1 to exclude identity proofing for testing purposes. Decision to have MFA has been finalized and currently requested by [redacted] sp to turn it off for testing purpose. Decision was made to have the RIDP and MFA turned on after the attribute approval routing has been completed. Helpdesk tier 1 functionalities walkthrough planned for Monday August 5, 2013. 	Jan 6th 2014	Kristine Maenner
OMAT	<ul style="list-style-type: none"> Application has been deployed to Production and successfully tested by the ZONE team. Bulk upload is pending from the ZONE team. Webgate installation and configuration is still pending. 	Already deployed	Damon Underwood
Zone			

Last Modified: April 20, 2011
Document # MONI-TEMP-027

Use or disclosures of data contained on this sheet is subject to restriction.



EIDM
Weekly Project Status Report

Open Payments	No update this week.	March 2014		
PROPOSED SCOPE FOR RELEASE 3				
Release 3:				
<ul style="list-style-type: none">EIDM Web Services to support Consumer Portal, CSR and SHOP Integration with EIDM.Implementation of Federation to integrate CSR users.Implement Waas for integration of Agents, Brokers and Agents.Modify EIDM Step up process from LOA #1 to LOA #2 and LOA #3.Implement Waas Database Connector.				
HIGH LEVEL SCHEDULE FOR RELEASE 3 – WORK IN PROGRESS				
Will be listed in next weeks Status Report.				
ISSUES	DATE OPENED	PRIORITY	STATUS	CORRECTIVE ACTION
1. EIDM Performance Testing issue. At present the Access Management and Identity lifecycle Management functions are not scaling beyond 250 CC users. EIDM Registration Services have been fine-tuned and is currently able to sustain 750 CC users with less than 1% error. On an average, EIDM can create around 9,000 users in an hour.	02/05/2013	High	Open	Update 0n 08/04/2013: We have completed one round of Performance testing on the NotResp component and were successful with 10K virtual users in the Impl1 environment. We are currently working on running the scripts for Lite account creation in Impl0 environment. Update on 07/28/2013: Performance Testing is on going in the Impl1 environment and we are sharing our finding on a daily basis. Update on 07/21/2013: QSSI EIDM is on schedule with the Performance Testing effort. The new IMPL1 environment is complete.



EIDM
Weekly Project Status Report

				<p>Scripts are complete as well and we will be running the scripts to get some baseline data on Sunday 07/21. There may be a scheduling conflict for the Performance center with the EDCG team. We have notified the EDCG team and are awaiting a response.</p> <p>Update on 07/14/2013: QSSI EIDM team is working on installing the ESP ^{Not} components in the EIDM Impl1 environment. QSSI EIDM team is also working with the EDCG team to get the scripts ready for the Performance testing effort. We are on schedule to complete the Testing effort by 07/31/2013.</p> <p>Update on 07/07/2013: Performance Test Plan will be shared with CMS by 07/09/2013. QSSI EIDM team continues to work on the Impl1 environment.</p> <p>Update on 06/30/2013: With multiple deliveries of inaccurate operating systems for the VMs by URS, QSSI estimates the completion of the Implementation1 environment to be delayed by 2 weeks. QSSI is currently working on the Performance Test Plan with work load model and will submit the plan early next week for all the stakeholders to review. QSSI continues to work on the development of the the Impl1 environment.</p> <p>Update on 06/23/2013: Implementation environments were delivered by URS with an operating system version for the Database VM that did not match the existing requirement for EIDM DB environments. Expected delivery is now 06/25/2013, which has delayed the performance testing timelines. QSSI has requested for a meeting with all stake holders to ensure participation from all stake holders and confirm that everyone is in consensus with the activities</p>
--	--	--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



EIDM Weekly Project Status Report

			scheduled for the Performance Testing effort. As an continued effort, QSSI is working with EDCG team in building the Impl1 environment.
			Update on 06/16/2013: QSSI has provided a high level schedule for all the tasks in Performance Testing and requested a meeting for early next week with all the parties involved in the effort. The meeting is to ensure everyone understands what is involved in the testing effort, clearly discuss the expectations from all stakeholders, and what metrics would be collected for the same.
			Update on 06/10/2012: No further updates. We are still waiting on Doug to provide the compute.
			Update on 5/24/2012: CMS decided on setting up a second instance of IMP environment to conduct the performance testing specifically to scale the "NOT Res" component. QSSI is working with Doug Wargush to provide the server details.
			Update on 05/17/2013: Awaiting CMS response on QSSI request for a dedicated implementation environment to execute performance testing. At this time performance testing scheduled for 5/20/2013 is put on hold. Received confirmation from CMS ETC team that performance testing can be executed up to 10,000 concurrent users at CMS ETC.
			Updated on 04/29/2013: Scheduling of performance testing is dependent on the scope and schedule for EIDM Release 2. QSSI is proposing to implement the open defects from Release 1 and upgrade of "NotRes". Currently QSSI is planning to schedule performance testing for the week of 05/20/2013.



EIDM
Weekly Project Status Report

				QSSI has requested CMS a dedicated window in implementation environment to execute the performance testing. Currently with applications integrated with EIDM in implementation environment, execution of the testing and implementing the recommendations from NotResp product team will be very difficult and could potentially impact other applications testing their applications with EIDM.	
2	NotResp 508 noncompliance issue. This week's 508 testing at CMS 508 team trained with only 25% score.	02/15/2013	High	Open	<p>Update on 08/04/2013: QSSI team is working on identifying the LOE to change all the screens with the option of screen reader mode per NotResp recommendation.</p> <p>Update on 07/28/2013: There are 2 tickets identified by the EIDM team to the NotResp Product team that we don't have a resolution on. NotResp team has provided a work around which is not feasible from a EIDM standpoint.</p> <p>Update on 07/21/2013: We are still testing the 508 issues in the test environment.</p> <p>Update on 07/14/2013: QSSI EIDM will be implementing the workarounds provided by NotResp for the 508 issues in the Test Environment as part of our scheduled deployment on tuesday 07/16/2013</p> <p>Update on 07/07/2013: No further updates.</p> <p>Update on 06/30/2013: We have escalated the NotResp issues to Sev 1 and are working with NotResp</p> <p>Update on 06/23/2012: QSSI still working with NotResp on the issue.</p> <p>Update on 06/16/2012: QSSI is working with the NotResp team this week to further troubleshoot the issue and identify possible fix</p>

				for the same. Update on 06/10/2012: No further updates. Update on 06/10/2012: No further updates. Update on 5/3/2013: Out of 4 defects fixed, only one defect has passed 508 testing. QSSI will setup a meeting with Oracle to perform further troubleshooting. Updated on 04/29/2013: 4 defects addressed and resolved in the Test Environment. Remaining 7 defects are still under analysis with QSSI EIDM and NotRes Product team. QSSI has submitted a remediation plan for resolving the 508 defects. There are in all 11 defects and all 11 defects have NotRes SR opened with product development team for analysis and resolution.
3. NotRes replication issue in the EIDM Test Environment and a one-off issue related new tcp connection. Analysis indicates that this is a known issue and a hot fix will be provided by NotRes to resolve this issue. This issue does not exist in Implementation environment, since production environment is similar to the implementation environment – the issue will not affect EIDM in production.	03/12/2013	Low	Open	This issue occurs only in test environment because there is only NotRes instance. Awaiting patch from NotRes to fix the issue in Test Environment.
4. Decision on Identity proofing users and determination of LOA 2, LOA 3 is awaited from CMS. As per Email sent to CMS OIS team by Henry Chao on 04/23/2013, there might be a change in the RIDP decisioning strategy to make the RIDP process simpler.	4/22/2013	High Tracking Purposes: Affects finalizing Release #3 scope and schedule	Open	Update On 08/04/2013: LOA2 functionality was deployed in the test environment on Sat 08/03/2013. We will be testing it in our test environment. Update on 07/28/2013: QSSI plans to implement the LOA2 functionality in the test environment this week. Update on 07/21/2013: The NotRes questions list was shared by CMS to SAIC. SAIC shared the sub codes to QSSI EIDM team on 07/19/2013. QSSI EIDM team will implement the new sub codes in the lower environment.



EIDM
Weekly Project Status Report

				<p>Update on 07/14/2013: The ^{NotR}esp questions list was shared by CMS to SAIC. SAIC plans to implement the sub codes by 07/28/2013, following which EIDM team will implement the same in the lower environment.</p> <p>Update on 07/07/2013: Meeting with SAIC was held on Tuesday 7/2. QSSI still awaiting the sub codes. CMS has made the decision to use Analytics Augmented approach for both LOA 2 and LOA 3. CMS will be sending the CMS approved ^{NotR}esp questions list to SAIC for them to implement the strategy and provide the sub codes.</p> <p>Update on 06/30/2013: QSSI is still awaiting the Sub Codes from SAIC. QSSI to set up a meeting with SAIC & CMS to get the latest updates on Id Proofing and plan for next steps.</p> <p>Update on 06/23/2013: QSSI is awaiting CMS to finalize the questions provided by SAIC.</p> <p>Update on 06/16/2013: No further updates.</p> <p>Update on 06/10/2013: It was decided with CMS on 06/07/2013 to proceed with Augmented Analytics approach for LOA2 ID Proofing. Pending decision on the use of Augmented Analytics for LOA3 Id proofing. Until further direction from CMS it was decided to follow the existing Id Proofing process for LOA3.</p> <p>Update on 06/02/2013: Still awaiting CMS decision on the approach</p> <p>Update on 05/03/2013: Awaiting CMS decision on Experian's Augment Analytics approach.</p> <p>QSSI is currently using the web services provided by SAIC/Experian to Id Proof and</p>
--	--	--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>user at LOA 2 and LOA 3. Any change to the decisioning strategy will require rework for the web services and the user interface developed so far in EIDM to identify Proof a user.</p>
<p>5. Installation of NotResp in CMS BDC to support EIDM Active-Active Solution.</p>	<p>05/03/2013</p> <p>Medium</p> <p>Open</p>	<p>Update On 08/04/2013. We are 60% done with installation of components across all environments. Still pending components are NotResp integration.</p> <p>Current Issues with BDC:</p> <ol style="list-style-type: none"> 1. NotResp are different NotResp at TMRK. NotResp BDC. Patch level not in sync. There are around 20,000 patches needed to bring BDC servers to be in sync. 2. Communications over port NotResp between NotResp <p>NotResp</p> <ol style="list-style-type: none"> 3. Global Load Balancer (GLB) status 4. Load Balancers with BDC for NotResp servers – LM team disputed that it was not part of the design. <p>Update on 07/28/2013: We have received the patch from NotResp. We still have the issues identified with installation of some Oracle components in BDC.</p> <p>Update on 07/21/2013: NotResp confirmed that they will provide the fix for the patch on the week of July 29th 2013. We are also working on fixing the NotResp functional issue on URL direct. It is being tracked as a NotResp. We have additional issues that were identified while installing the NotResp components in the NotResp.</p>



EIDM
Weekly Project Status Report

				<p>BDC environment:</p> <p>1. BDC environment was set up with non oracle system accounts, security constraints with the EDCG do not allow any NotResp components to be installed with NotRes stem account names. For the Not active solution to work NotRes esp will have to be installed with the p system accounts.</p> <p>2. The BDC environment is not in Sync with the Terremark environment with OS versions. Both the conditions listed above are required for the Not active solution to work.</p> <p>Update on 07/14/2013: It was decided to install all the sd components in BDC exactly similar to what we currently have in the Terremark Production environment. QSSI EIDM team has shared the installation CD with the BDC team for the initial scan. Two NotRes sources from QSSI EIDM team will be on site at the BDC location for the installation of Oracle components on Monday.</p> <p>Update on 07/07/2013: Installation of sd continues to be on hold since the issues identified with PS1 have not been resolved yet. Delivery of patch for Res active solution from NotRe is TBD, this was earlier scheduled to be 07/15/2013. QSSI has submitted a document listing the current issues and options impacting NotResp with NotResp p CMS.</p> <p>Update on 06/30/2013: QSSI has installed the NotRe database with the required schemas, followed by NotRes</p> <p>QSSI plans to install esp and installation of sd is on hold until the Res issue is resolved.</p> <p>Update on 06/23/2013: QSSI had multiple meetings with the CMS EDC team to review the design and more meetings are scheduled</p>
--	--	--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



EIDM
Weekly Project Status Report

				<p>for this week.</p> <p>Update on 06/16/2013: QSSI has provided the CMS EDC team with the updated EIDM diagrams. QSSI technical team also participated in a meeting with CMS EDC to further discuss the global load balancer requirements and how they can be configured. Additionally, the NotResp was successfully installed and tested in the Test environment.</p> <p>Update on 06/10/2013: URS and TM are in the process of implementing the firewall rules post CMS approval.</p> <p>Update on 06/02/2013: QSSI is awaiting the firewall rules to be implemented between TerrelMark and BDC. Additionally, NotResp support has added a requirement to install the NotResp before it is installed and configured in BDC. QSSI would require additional 5 weeks to apply the patch in the TM lower environments and perform regression testing.</p> <p>Update on 5/24/2013: QSSI has successfully installed and configured the NotRe DB and NotRe. The NotRe replication is on hold until a firewall between TerrelMark and BDC is opened. Once NotResp patch is configured, NotRes installation and configuration will commence followed by NotResp installations.</p> <p>Update on 05/17/2013: QSSI started supporting installation of NotRe at BDC from 5/16/2013. Only one work station is provided to QSSI for NotRe installation, which will delay the process of setting up NotRe in Test, Validation and Production Environment.</p> <p>Update on 05/03/2013: Awaiting decision from CMS on whether QSSI is required to install</p>
--	--	--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>6. Scope for Release 3 is not finalized. QSSI is working on completing the requirements and development of web services. Requirements for web services are expected to complete 5/10 and development of web services will be complete on 5/17/2013. QSSS will need CMS help for finalizing the following:</p> <ul style="list-style-type: none"> Additional details related to integration of Agents, Brokers and Navigators – QSSI has forwarded the proposed workflow (initial) to CMS on 04/29/2013 and will respond to Venkat's response by 5/6/2013. Decision on Experian Augmented Analytics to step up a user LOA to LOA #2 and LOA #3. Infrastructure and Network connectivity between CSR and FFM application is not finalized or at least QSSI is not aware when FFM and CSR applications will be integrated in Test Environment. QSSI needs the integrated environment to configure the federation of CSR users. Integration requirements from SHOP, PAS Applications. <p>Note: This issue is affecting finalizing the release schedule for integrating EIDM with CSR, Consumer Portal and SHOP.</p>	5/3/2013	High Tracking Purposes: Affects finalizing Release #3 scope and schedule.	Open	<p>Notes: to provide expertise to CMS BDC to install and configure at BDC.</p> <p>Update on 08/04/2013: We still need additional information on the new application to be integrated as part of Release 3. QSSI provided the LOE for one CR and had a meeting with CMS on the other CR on Friday. QSSI will send the LOE for the second CR early next week.</p> <p>Update on 07/28/2013: Additional application integration and implementation of new sub codes along with Updated Lifecycle configuration will be added to Release 3. QSSI to provide LOE by COB Monday. CMS to provide new CRs for these implementations.</p> <p>Update on 07/21/2013: QSSI EIDM has shared the updated integrated schedule with all application integration schedules included on 07/21/2013.</p> <p>Update on 07/14/2013: QSSI EIDM has shared the integrated schedule with CMS on 07/12/2013.</p> <p>Update on 07/07/2013: QSSI submitted the draft version of the schedule to CMS, QSSI will submit the completed version for CMS review by Friday 07/12/2013.</p> <p>Update on 06/30/2013: QSSI provided a draft version of the schedule and will continue to work on the schedule.</p> <p>Update on 06/23/2013: QSSI to provide an high level schedule to CMS this week.</p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------	-----------------------------------------------------------------------------------------------------	------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

				<p>Update on 06/16/2013: QSSI is still working on the new schedule and will provide an updated schedule on the basis of the recent developments.</p> <p>Update on 06/10/2013: QSSI had a meeting with CMS on 06/07/2013 and most of the items were finalized. QSSI will provide CMS with the updated schedule based on the decisions made in the meeting.</p> <p>Updates on 06/02/2013: High level plan with an integrated schedule was presented to CMS on 05/30/2013. QSSI is awaiting response from CMS.</p> <p>Update on 5/24/2013: QSSI is working with Deb to come up with the complete scope for Release 3. The QSSI team is working on required LOE to come up with a schedule that will be shared with CMS by end of this week.</p> <p>Update on 5/17/2013: QSSI has completed development of web service (to use for integration between EIDM, Consumer Portal and CSR) and deployed in Test environment on 5/17/2013. Final System Requirements for web services will be sent to CMS this week.</p> <p>QSSI PM to review with CMS EIDM on the next steps and will work with CMS to finalize the schedule for Release 3.</p>
<p>7. Resolution to NotRe SRS opened for asp NotRe Development Team. Currently there are 4 SRSs opened and is expected to be resolved as part of NotRes p.</p>	5/6/2013	Medium	Open	<p>Update on 08/04/2013: The list of NotRe SRSs with latest status is attached in the NotRe sp section.</p> <p>Update on 07/28/2013: The list of NotRe SRSs with latest status is attached in the NotRe sp section.</p> <p>Update on 07/21/2013: The list of NotRe sp SRSs with latest status is attached in the Risks section.</p>



EIDM
Weekly Project Status Report

				<p>Update on 07/14/2013: The list of NotResp SRs with latest status is attached in the Risks section.</p> <p>Update on 07/07/2013: QSSI to provide weekly status on open NotResp SRs to CMS. The first status report will be submitted to CMS on Monday 8th July 2013 in the format requested by CMS.</p> <p>Update on 06/30/2013: QSSI shared the entire list of NotResp SRs with current status to CMS. QSSI has also planned a weekly meeting with NotResp to review the status on each SR.</p> <p>Updates on 06/23/2013: No further updates.</p> <p>Updates on 06/16/2013: No further updates.</p> <p>Updates on 06/10/2013: No further updates.</p> <p>Updates on 5/24/2013: No further updates.</p> <p>Update on 5/17/2013: Hot fix from NotResp is awaited this week for resolving 4 errors per NotResp does not contain any NotResp that will be user of EIDM, expecting NotResp to be released in Mid-June and that is expected to provide resolution to some performance issues.</p> <p>QSSI is working with NotResp development team to find out when NotResp will be ready for EIDM. Response from NotResp is awaited.</p>	
8. Migration of EIDM Data Layer Physical machines.	NotResp and Database) from Virtual to sp	5/17/2013	High	Open	<p>Update on 08/04/2013: No further updates.</p> <p>Update on 07/28/2013: No further updates.</p> <p>Update on 07/21/2013: No further updates.</p> <p>Update on 07/14/2013: No further updates.</p> <p>Update on 07/07/2013: No further updates.</p> <p>Updates on 06/30/2013: No further updates.</p> <p>Updates on 06/23/2013: No further updates.</p>

			<p>Updates on 06/16/2013: No further updates.</p> <p>Updates on 06/10/2013: No further updates.</p> <p>Update on 5/24/2013: Meeting on 5/23/2013 was postponed due to unavailability of key contributors to this discussion. This meeting will be scheduled for some time this week.</p> <p>Update on 05/17/2013: QSSI/OCSS to provide the sizing of Not Res and Database layer to TerraMark on 5/21/2013. Meeting scheduled for 5/23/2013 to discuss the requirements and next steps on migration tasks related to migration of EIDM to Physical machines.</p>
<p>9 NotResp Asynchronous deployment. The Baltimore Data Center hosts the CMS Portal, but not FFM or other consumer facing applications which are only hosted at TerraMark. In Not Res terms, this is referred to an "asynchronous" deployment.</p>	5/17/2013	High	<p>Open</p> <p>Update on 08/04/2013: The patch will be tested once we have deployed all the components in the BDC environment and resolved the issues with the installation.</p> <p>Update on 07/28/2013: We have received the patch from Not Res and are deploying the same in our Development environment.</p> <p>Update on 07/21/2013: Not Res has confirmed that the patch will be ready on the week of July 29th 2013. QSSI is continuing with installation of all other components in the BDC environment.</p> <p>Update on 07/14/2013: No further updates.</p> <p>Update on 07/07/2013: No further updates.</p> <p>Updates on 06/30/2013: No further updates.</p> <p>Update on 06/23/2013: QSSI awaiting input from Not Res to submit the white paper.</p> <p>Updates on 06/16/2013: QSSI is reviewing the document with Not Res will provide the white paper this week.</p> <p>Updates on 06/10/2013: QSSI will read the white paper this week with Not Res recommendation and follow it up with a</p>

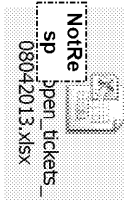
				meeting. QSSI will send a white paper on the current status and will schedule a meeting with CMS to discuss the next steps on the deployment of Active-Active solution at BDC.
10. Currently, EIDM is performing all the tasks of getting the approvals and doing all the paper work for environment change requests by external application owners, the work is labor intensive and would need better process considering the number of applications integrating with EIDM is increasing.	06/21/2013	Low	Open	Update on 08/04/2013: No further updates. Update on 07/28/2013: No further updates. Update on 07/21/2013: No further updates. Update on 07/14/2013: No further updates. Update on 07/07/2013: CMS EIDM team directed QSSI not to initiate any application integration meeting unless QSSI has approval from the CMS EIDM GTL. Updates on 06/30/2013: No further updates.
11. Lack of information on the MLN data source for Agent/Broker application could impact the Production deployment date of August 11 th 2013	07/20/2013	High	Open	Issue was discussed with CMS in the last status meeting and CMS would have an internal meeting to identify the right process. Future use of Remedy by application owners was suggested by QSSI. Update on 08/04/2013: The flow of MLN data was identified by CMS, still waiting on getting the data source information from CMS. Update on 07/28/2013: We still do not have server information on the data source for Agent Brokers. We are at a serious risk of making the Aug 11th Production date for Agents and Brokers. We need this information to open firewall rules and connect to the data store. Update on 07/21/2013: The issue has been escalated to the CMS EIDM team, QSSI EIDM team has configured the application in the test environment with a dummy table for testing purposes.

				Getting all the firewall rules implemented for the MLN data validation across all the environments could be a challenge. Update on 08/04/2013: Still awaiting CMS decision.
12. Augmented Analytics Decision pending with CMS. This was opened to track the augmented analytics decision from CMS which also impacts the implementation of NotResp in EIDM screen.	08/04/2013	Medium	Open	Update on 08/04/2013: It was decided to close this issue and open a new on decision pending with Augmented Analytics. Update on 07/28/2013: No further updates Update on 07/21/2013: No further updates. Update on 07/14/2013: No further updates. Update on 07/07/2013: No further updates. Update on 06/30/2013: No further updates. Update on 06/23/2013: No further updates. Update on 06/16/2013: No further updates. Update on 06/10/2013: This is pending on CMS decision of NotRe . This will be a non-issue if we proceed with SD NotRes implementation. Update on 5/17/2013: Awaiting CMS Response to the proposed options. Update on 05/13/2013: Alternative options for implementing NotResp sent to CMS on 05/13/2013. Additional time was taken to analyze the option of using NotRes as of the solution for implementing NotRes to prevent BOT attacks. Update on 05/03/2013: Discussed options for NotResp QSSI to send the write-up on the solution on 05/06/2013. CMS EIDM will analyze the solution and provide approval to proceed further. NotResp will be removed from Release 1
13. NotResp address change affects implementation of NotResp for EIDM User Registration process. At the time, we created the rules for NotResp the set of public IPs were different NotResp NotResp Currently NotResp URL is pointing to another pool NotResp NotResp This pool actually belongs to NotRe NotResp net is being set up as an alias (we believe this is a very recent change).	03/16/2013	Medium	Closed	

				Increment 2. Alternate suggestions for implementing a solution to prevent BOT attacks have been provided to CMS. Additional meeting will be scheduled this week and the timeline for alternate implementation for NotResp will be provided to CMS by this week.
14. Lack of information on testing schedule for applications integrated with EIDM. This affects QSSI ability to plan for testing activities like performance testing in EIDM Implementation Environment.	5/8/2013	High Tracking Purposes: Affects QSSI Testing tasks planned for Testing and Implementation Environment	Closed	<p>Update on 07/28/2013: No further updates</p> <p>Update on 07/21/2013: We do have a dedicated environment for Performance testing IMPL 1. The current environment built is just for NotResp. We will keep this issue open till the environment is complete with all NotResp and Res components.</p> <p>Update on 07/14/2013: No further updates.</p> <p>Update on 07/07/2013: No further updates.</p> <p>Update on 06/30/2013: No further updates.</p> <p>Update on 06/23/2013: No further updates.</p> <p>Update on 06/16/2013: No further updates.</p> <p>Updates on 06/10/2013: No further updates</p> <p>Updates on 5/24/2013: No further updates</p> <p>Update on 5/24/2013: No additional updates. Still waiting on schedule that specifies testing activities for other applications.</p> <p>Update on 5/17/2013: Awaiting details from CMS EIDM team on the testing activities for other applications integrated with EIDM in Test and Implementation Environment.</p> <p>To discuss with CMS and request for a weekly or bi-weekly meeting within applications integrated with EIDM (a meeting similar to CCB) and request for a schedule update from respective applications on their respective application testing activities including SCA in Test and Implementation Environment.</p>




EIDM
Weekly Project Status Report

Risks	DATE OPENED	PROBABILITY/ IMPACT	STATUS	CONTINGENCY PLAN
1. NotResp product defects are not addressed in the timely manner, then EIDM implementation schedule and quality of the solution will be negatively impacted.	08/23/2012	Low/High	Active	<div></div> <p>Update on 07/28/2013: The list of all open NotRe sp SRs is attached with the latest current status on each SR.</p> <p>Update on 07/21/2013: The list of all open NotRe sp SRs is attached with the latest current status on each SR.</p> <p>Update on 07/14/2013: The list of all open NotRes Rs is attached with the latest current status on each SR.</p> <p>Update on 07/07/2013: QSSI EIDM team to work with CMS to finalize plan of NotResp NotRes Rs to CMS.</p> <p>Updates on 06/30/2013: On further testing of NotResp QSSI testing team found some functionality with URL redirect not working as expected. NotR development team has advised QSSI EIDM team to install NotResp to fix the issue. The development is also working on fixing the issue with: sp to avoid the NotResp stall. Since P is a big installation and may impact other EIDM deployments, QSSI is working very closely with sp or alternate arrangements. A decision will have to be made early next week with the help of CMS for next steps.</p> <p>Update on 06/23/2013: QSSI team continues to work with the NotRe team to fix the issues.</p> <p>Updates on 06/16/2013: QSSI team is actively working with the NotRes Product and Engineering team to analyze and fix the issues. NotResp Upgrade Patch on: NotR as successfully installing in the lower environments.</p> <p>The Project Team has established a weekly touch point with the</p>



EIDM
Weekly Project Status Report

					NotResp Product Team to discuss open issues; NotResp prior Management for Product Development has been unable to providing immediate support on any issues identified by the EIDM Project Team.	
2.	NotResp	be configured in Terremark	10/18/2012	Low/Medium	Active	Update on 08/04/2013: No further updates. Update on 07/28/2013: No further updates. Update on 07/21/2013: No further updates. Update on 07/14/2013: No further updates. Update on 07/07/2013: No further updates. Update on 06/30/2013: No further updates. Update on 06/23/2013: QSSI system Engineers had visited the Culpeper facility and inventoried available hardware in May 2013. All relevant information were captured (CPU, RAM etc). Storage used to host NotResp DB VMs is still under discussion between QSSI work sd and TM. Various options were visited. QSSI is waiting on direction from CMS. Updates on 06/16/2013: No Further updates. Received Email from Peter Um that TM will support physical storage. QSSI has provided the requested EIDM Specifications for physical storage to Peter Um on 12/07/2012. As an alternative to ensuring High Availability, QSSI and NotResp recommend configuring sp DB with NotResp and for EIDM Release 1 – this will be the option that will be implemented. At this time the issue does not prevent proceeding forward for EIDM Release #1, but QSSI will further discuss and provide a plan for implementing NotResp post EIDM Release #1.
3.	Decision on Disaster Recovery Strategy and site for CMS Private Cloud is not determined.	10/22/2012	Medium/High	Active	Update on 08/04/2013: No further updates. Update on 07/28/2013: No further updates. Update on 07/21/2013: No further updates. Update on 07/14/2013: No further updates. Update on 07/07/2013: No further updates. Update on 06/30/2013: No further updates.	

				<p>Update on 06/23/2013: No further updates. Update on 06/16/2013: No further updates. Updates on 06/16/2013: No Further updates. As per Email from Doug Margush on 10/24/2012, the decision is still pending with CMS. As per Email received from Thomas Schankweiler on 11/12/2012, the suggestion is track this as an issue till this is solved.</p>  <p>Re CMS Private Cloud Security and EI</p>
--	--	--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

WEEKLY PROJECT STATUS REPORT

CLIENT/PRO JECT:	CMS/Enterprise Identity Management	
PROJECT MANAGER:	Girish Shetty	
PROGRAM DIRECTOR:	Nitin Malta	
CLIENT CONTACT:	Tim Purcell, Sharlene Mansaray, Venkat Basavaraju, Robert Burger, Todd Northwood, Cathy Carter, Marc Richardson, Carla Jones, Mark Small	
STATUS PERIOD:	09/23/2013 to 09/29/2013	
STATUS SUMMARY		
TASKS COMPLETED /DELIVERIES FOR THIS PERIOD – 09/23/2013 to 09/29/2013		
Following are activities completed for this week:		
1.	EIDM IMPL 1 – Completed the build up with <div>Not Res</div>	Started performance testing in IMPL 1.
2.	EIDM IMPL - Release 3 Build# 20.1, ESD Migration and the Roll back the EIDM Tier 1 Helpdesk capabilities for the SHOP Associate Role tasks, Password policy import on 09/23	
3.	EIDM PROD - To provision 1700 accounts into portal on 09/23	
4.	EIDM PROD - Release 3.20.1, ESD migration, T2P Copy on 09/24	
5.	EIDM TEST – Release 3.21 on 09/24	
6.	EIDM IMPL - Akamai support EIDM/FFM on 09/24	
7.	EIDM PROD - Implement <div>Not Res esp</div>	recommendation for performance tuning on 09/25
8.	EIDM PROD - Akamai support EIDM/FFM on 09/25	
9.	EIDM TEST – Release 3.21.1 and <div>Not Res p</div>	commmed changes on 09/27
10.	EIDM IMPL – Release 3.21.1 and <div>Not Res sp</div>	recommended changes on 09/27
11.	EIDM IMPL0 - <div>Not Res sp</div>	recommended changes on 09/28
12.	EIDM PROD – Release 3.21.1 and <div>Not Res p</div>	recommended changes on 09/29
13.	EIDM PROD – Update Waas DB with Agent Broker MLN information	
14.	EIDM Prod – OUD1 Reindexing of OUD1	

Last Modified: September 29, 2013
Document # MONI-TEMP-027

Use or disclosures of data contained on this sheet is subject to restriction.

15. EIDM Test and Impl – Update Waas DB with Agent Broker MLN information
16. EIDM Impl0 – Enabled Mock RIDP in the Impl0 environment to support End to End Performance testing
17. No Severity #1 and Severity #2 tickets currently opened in production. EIDM Helpdesk tickets status for this week:
 - a. # of New Tickets Opened between 09/23/2013 to 09/29/2013 → **341**
 - b. # Of Tickets Closed between 09/23/2013 to 09/29/2013 → **320** (Note: this number may include tickets opened from previous weeks).
 - c. # of Tickets unresolved from 03/25/2013 to 09/29/2013 → **148**
18. QSSI supported ongoing application integration meetings for QMAT, FFM, SHOP, ESD and Microstrategy and shared meeting minutes as applicable. QSSI also supported Application integration meetings for the new applications in the pipeline like QMAT, EPPE, Open Payments and shared meeting minutes.

TASKS PLANNED/DELIVERIES FOR THIS PERIOD - 09/30/2013 to 10/06/2013

1. Continue performance testing in IMPL1.
2. Tentatively Support the ZOne webgate installation and configuration in the Production environment. Date not finalized yet.
3. Continue building the BDC_{esp} environment for the active active solution. **NotResp**
4. Continue supporting CDS/BDC on CMS Portal Webgate configuration
5. Continue requirement gathering and application integration meetings for new applications like **NotResp** and Open Payments integrating with EIDM
6. Continue testing and deploy code for Bug fixes in the Test and Implementation Environment.
7. Analyze and Resolve outstanding issues in production, report delivery production status report on EIDM production and helpdesk operations.

Scheduled Deployments in the EIDM Environment:

Environment	Start Time	End Time	Activity
TEST	10/1/2013 06PM	10/1/2013 06PM	EIDM TEST weekly deployment – Bug Fixes
IMPL	10/3/2013 09PM	10/4/2013 12AM	EIDM IMPL Weekly deployment – Bug Fixes - Applications Integration: ASP

EIDM Application Integration Status:

Applications	Current Status	Tentative	Tentative	Tentative	Tentative	CMS GTL
--------------	----------------	-----------	-----------	-----------	-----------	---------

		Test Date	Impl Date	Prod Date	
FFM Consumers	<ul style="list-style-type: none"> ➤ Web services deployed to Production. ➤ EIDM team deployed the consumer lifecycle changes, and FARS redesign to Prod on 9/15 as planned. ➤ A bug fix to remove comma from the list of supported characters for Address field was deployed to Test on 9/17. This fix was deployed to Production on 9/22. ➤ The issue with the DOB field not consistently sent in the FARS response was resolved from Experian on 9/22. 	Already deployed	Already deployed	Already deployed	Susan Tudor/ Megan Reilly
	Assister Integration (FFM Agent Broker)	Already deployed	Already deployed	Already deployed	Mark Oh/ Joy Kraybill
SHOP	<ul style="list-style-type: none"> ➤ EIDM team continues to support the Agent Broker webinar held every week ➤ No Updates this week ➤ This application has been deployed in Production environment on 9/15 ➤ EIDM Tier 1 helpdesk functionality has been added to the SHOP Admin role. ➤ There have been some changes to the flow on the SHOP side to resolve the issue of passing the post-authentication parameters from SHOP to FFM. ➤ EIDM team has configured the required policies in the TEST environment and it needs to be tested by SHOP/FFM. 	Already deployed	Already deployed	Already deployed	Hannah Yoo
	CSR	Already deployed	Already deployed	Already deployed	Frances Hamalik/ Jeffrey Burdette
ASP	<ul style="list-style-type: none"> ➤ ASP team will continue testing in TEST with new data sent by EIDM. Only one user account from Experian was successful in Step Up process. ➤ Target date for IMPL is still 10/03. 	Already deployed	10/03/2013	EIDM - 1/27/2014 ASP - 3/1/2014	Sarah Harding

Last Modified: September 29, 2013
Document # MONI-TEMP-027

Use or disclosures of data contained on this sheet is subject to restriction.

	<p>➤ NotResp is development server has been switched from the BDC to TUSA, since the server has a Windows environment. Target date has not been set.</p> <p>➤ NotResp has agreed to moving IMPL date to 10/10, given the above other center issue.</p> <p>➤ NotResp is configuration in Test requires some updates based on the requirement change in role. EIDM still needs to add the authorizing code and database table to accommodate role requests.</p>	Already deployed	10/10/2013	EIDM - 2/16/2014	Gladys Wheeler
ASSET	<p>➤ EIDM Demo completed on 9/20.</p>			3/2/2014	
	<p>➤ An EIDM demo was performed on 9/12.</p> <p>➤ NotResp is targeting Test for Feb 2014.</p> <p>➤ NotResp is going to fill up the application onboarding documents and get back with EIDM.</p>	01/23/2014 (Application expected date is 02/16/2014)	02/18/2014	3/2/2014	Suman King
EPPE	<p>➤ No Updates this week</p> <p>➤ NotResp indicated that each role had its own functionalities and attributes.</p> <p>➤ NotResp indicated that there will be 3 levels of approvals for the State roles. In addition to the State attribute, there will be other attributes for state/CMS roles.</p> <p>➤ NotResp to send over an updated proposed approval hierarchy and attributes associated with each role and a updated setup form</p>	10/29/2013	11/15/2013	12/08/2013	Nancy Martin/Siani Kayani
MACPro	<p>➤ EIDM technical team is working with the Oracle team to come up with a resolution regarding the "My Action" link.</p> <p>➤ NotResp testing is in progress in Test environment and IMPL environment.</p> <p>➤ EIDM team had set up a webinar on Monday with Dickens to go over and troubleshoot the XML gateway web service issue.</p> <p>➤ The XML gateway web service issue is fixed as of Wednesday</p>	Already deployed (All NotResp are set up)	Already deployed	01/06/2014	Kristine Maenner
CMAT					

Last Modified: September 29, 2013
Document # MONI-TEMP-027

Use or disclosures of data contained on this sheet is subject to restriction.

	<ul style="list-style-type: none"> EIDM may need to provision the user to another group in Portal LDAP which will give them access to the MicroStrategy tab in the Portal. Mark Saks from EIDM team needs open a dialogue with the Portal and MicroStrategy group to get confirmation and if anything else needs to be done from the EIDM side. 				
	<ul style="list-style-type: none"> EIDM team performed a demo of an EIDM application functionality with the BCARE team BCARE team needs to understand why validating the BPID using an authoritative data source precludes them from using the BPID for routing BCARE team presented 3 option regarding how to access the BPID, no decision has been made 	10/01/2013	10/31/2013	12/15/2013	Elizabeth Truong
BCARE	<ul style="list-style-type: none"> EIDM team is working on analyzing the options and check feasibility 				
QIES	Follow-up meeting needs to be scheduled to discuss technical questions and other details.	Not sure	Not sure	2015	Jack Williams
Zone	No Update this week	Already deployed	Already deployed	Already deployed	Damon Underwood
ESD	Federation implemented with SERCO similar to CSR federation. LOA update functionality has been developed by EIDM to update a user's LOA once the helpdesk has verified the required documentation.	Already deployed	Already deployed	Already deployed	
	<ul style="list-style-type: none"> Open Payments was deployed in Test on 09/24/2013. 	Already deployed	11/19/2013	March 2014	Veronica/ Pennie
NPPT/ Open Payments	<ul style="list-style-type: none"> There will be another TEST deployment on 09/26/2013 to provision the users with Open Payments role to the proper Portal group. EIDM team will send RIDP test data with the Open Payments team. 				

EIDM Bugs Report

Please find attached the latest bugs report from EIDM. We will have tentative deployment dates for the bugs in next week's status report.

EIDM Defect List
09-26-2013.xlsx

EIDM Action Item Log:

Please find attached the action item log since last week:



Action Items
9-27-13.xlsx

PROPOSED SCOPE FOR RELEASE 3

Release 3:

- EIDM Web Services to support Consumer Portal, CSR and SHOP Integration with EIDM.
- Implementation of Federation to integrate CSR users.
- Implement Waas for integration of Agents, Brokers and Agents.
- Modify EIDM Step up process from LOA #1 to LOA #2 and LOA #3.
- Implement Waas Database Connector.

HIGH LEVEL SCHEDULE FOR RELEASE 3 – WORK IN PROGRESS

Will be listed in next week's Status Report.

ISSUES	DATE OPENED	PRIORITY	STATUS	CORRECTIVE ACTION
1. EIDM Performance Testing issue. At present the Access Management and Identity lifecycle Management functions are not scaling beyond 250 CC users. EIDM Registration Services have been fine-tuned and is currently able to sustain 750 CC users with less than 1% error. On an average, EIDM can create around 9,000 users in an hour.	02/05/2013	High	Open	Update On 09/29/2013: We completed the build up of the IMPL1 environment with [NotRe] using normal deployment process after failed attempt using the T2P scripts. We have used the Impl1 environment for running the Performance testing scripts for OIM.

2. NotResp 508 noncompliance issue. This week's 508 testing at CMS 508 lab failed with only 25% score.	02/15/2013	High	Open	Update On 09/29/2013: EIDM team is focusing on other high priority issues and will work on the 508 issues with Portal as soon as we resolve the issues.
3. Installation of NotResp in CMS BDC to support EIDM Active-Active Solution.	05/03/2013	Medium	Open	Update On 09/29/2013: QSSI EIDM team continues to provide regular status on the BDC build out. 1. Global Load Balancer for Active-Active. Risk Acceptance document was submitted to CMS for review. The design has now been finalized. 2. At Thursday weekly 9AM call, it was agreed on and decided that we can stop the work on BDC DEV environment and move to focus on standing up BDC VAL environment due to the fact that it does not have global load balancer and not internet facing. 3. The NotResp issue was resolved by the team work by QSSI, NotResp and LM. 4. A new SR was entered to create "keep-alive" connections for NotResp to prevent connectivity issues in BDC (Connections between NotResp are getting dropped and not reset.) Current projection for BDC PROD go live is 10/18/2013.
4. Scope for Release 3 is not finalized. QSSI is working on completing the requirements and development of web services. Requirements for web services are expected to complete 5/10 and development of web services will be complete on 5/17/2013. QSSI will need CMS help for finalizing the	5/3/2013	High Tracking Purposes: Affects	Open	Update On 09/29/2013: QSSI EIDM team provided dates with deployment schedule for Release 3 specific functionality.

Last Modified: September 29, 2013
Document # MONI-TEMP-027


Use or disclosures of data contained on this sheet is subject to restriction.

<p>following:</p> <ul style="list-style-type: none"> Additional details related to integration of Agents, Brokers and Navigators – QSSI has forwarded the proposed workflow (initial) to CMS on 04/29/2013 and will respond to Venkat's response by 5/6/2013. Decision on Experian Augmented Analytics to step up a user LOA to LOA #2 and LOA #3. Infrastructure and Network connectivity between CSR and FFM application is not finalized or at least QSSI is not aware when FFM and CSR applications will be integrated in Test Environment. QSSI needs the integrated environment to configure the federation of CSR users. Integration requirements from SHOP, PAS Applications. <p>Note: This issue is affecting finalizing the release schedule for integrating EIDM with CSR, Consumer Portal and SHOP.</p>		finalizing Release #3 scope and schedule.		
<p>5. Resolution of NotResp opened for Oracle Development Team. Currently there are 4 SRs opened and is expected to resolved as part of BP06.</p>	5/6/2013	Medium	Open	Update On 09/29/2013: The list of NotResp is with latest status is attached in the Risks section.
<p>6. Migration of EIDM Data Layer (NotR and Database) from Virtual to Physical machines.</p>	5/17/2013	High	Open	Update on 5/24/2013: Meeting on 5/23/2013 was postponed due to unavailability of key contributors to this discussion. This meeting will be scheduled for some time this week.
<p>7. NotResp Active-Active solution does not support Asynchronous deployment. The Baltimore Data Center hosts the CMS Portal, but not FFM or other consumer facing applications which are only hosted at Terremark. In NotR esp terms, this is referred to an "asynchronous" deployment.</p>	5/17/2013	High	Open	Update On 09/29/2013: NotR esp issues have been resolved. Global Load Balancer for Active-Active- Risk Acceptance document in submitted for CMS review. The design has now been finalized. We have proceeded to build up the Active-Active NotResp between BDC and Terremark.
<p>8. Currently, EIDM is performing all the tasks of getting the approvals and doing all the paper work for environment change requests by external application owners, the work is labor intensive and would need better</p>	06/21/2013	Low	Open	Update on 07/07/2013: CMS EIDM team directed QSSI not to initiate any application integration meeting unless QSSI has approval from the CMS EIDM GTL.

Last Modified: September 29, 2013
Document # MONI-TEMP-027

Use or disclosures of data contained on this sheet is subject to restriction.

process considering the number of applications integrating with EIDM is increasing.				
9. Augmented Analytics Decision pending with CMS. This was opened to track the augmented analytics decision from CMS which also impacts the implementation of reCaptcha on EIDM screen.	08/04/2013	Medium	Open	Update On 09/29/2013: Still awaiting CMS decision.
10. EIDM sub contractors from the technical and operations team have been charging very high number of hours for the last couple of weeks. This is to support the multiple activities EIDM team have been supporting with Release 3, Application Integration Support, Production Issues, Performance Tuning and FFM support.	09/15/2013	Medium	Open	Update On 09/29/2013: We are tracking these hours very closely and we will continue to report to CMS if there is a further increase in the number of hours being charged by the Subs.

Risks	DATE OPENED	PROBABILITY / IMPACT	STATUS	CONTINGENCY PLAN
1. If products defects are not addressed in the timely manner, then EIDM implementation schedule and quality of the solution will be negatively impacted.	08/23/2012	Low/High	Active	Update on 09/29/2013: The list of all open NotResp is attached with the latest current status on NotResp open tickets sp 7_2013.xlsx
2. Decision on Disaster Recovery Strategy and site for CMS Private Cloud is not determined.	10/22/2012	Medium/High	Active	Update on 06/09/2013: As per Email from Doug Margush on 10/24/2012, the decision is still pending with CMS. As per Email received from Thomas Schankweiler on 11/12/2012, the suggestion is track this as an issue till this is solved.  Re CMS Private Cloud Security and EI
3. If ZONE IMPL environment is connected to the EIDM production environment then this could lead to unauthorized access to the EIDM Production Environment.	08/23/2013	Medium/High	Active	Update On 09/29/2013: This risk was listed in the Security documentation and was opened in July; risk was also reported in the Status report for tracking purposes.
4. Portal at BDC has intermittent connection issues	2/21/2013	Medium/High	Active	Update On 09/29/2013: Currently the Risk limited to Enterprise

Last Modified: September 29, 2013
Document # MONI-TEMP-027

Use or disclosures of data contained on this sheet is subject to restriction.



EIDM
Weekly Project Status Report

with EIDM - If this connectivity issue prolongs then our SLA's will be impacted resulting in schedule, cost and quality of service level to CMS.				NotRe sp only. We are building a process to get NotRe logs from BDC on a regular basis. This helps us troubleshoot issues with NotRes in an efficient manner and also identify the root cause.
5. NotRe does not have the ability to encrypt data, and thus data stored in NotRe may be accessible to unauthorized individuals.	08/23/2013	Low/High	Active	Update 0n 09/29/2013: Mitigation for the risk is that Role based access controls restrict access on servers to individuals who have a business need. Access to privileged functions is logged and audited.
6. NotRe prod environment is in Tulsa, this is a new environment and technical issues will have to be worked through and could impact schedule.	7/26/2013	Low/Medium	Active	Update 0n 09/29/2013: This could potentially change to the Baltimore Data Center, QSSI EIDM team still awaiting confirmation from CMS and NotRe team.
7. If the environment for Performance Testing is not available, then we will be unable to execute Performance Testing as planned.	7/18/2013	Medium/High	Active	Update 0n 09/29/2013: The OIM buildup in IMPL 1 has been completed. This risk has been resolved.
8. Ongoing change requests from CMS EIDM team with very short turnaround time to deploy the code in Production could hamper the overall quality of the EIDM product.	08/23/2013	Medium/High	Active	Update 0n 09/29/2013: For CR's where scope is finalized, QSSI EIDM team is working on getting the change requests implemented in the lower environment as soon as possible to ensure extensive testing. We also plan to use automation testing to expedite regression testing.

Centers for Medicare & Medicaid Services

Restricted Distribution
Sensitive – For Official Use Only



Department of Health and Human Services



Centers for Medicare & Medicaid Services

Center for Consumer Information and Insurance Oversight

NotResp

Security Impact Analysis (SIA)

October 26, 2013

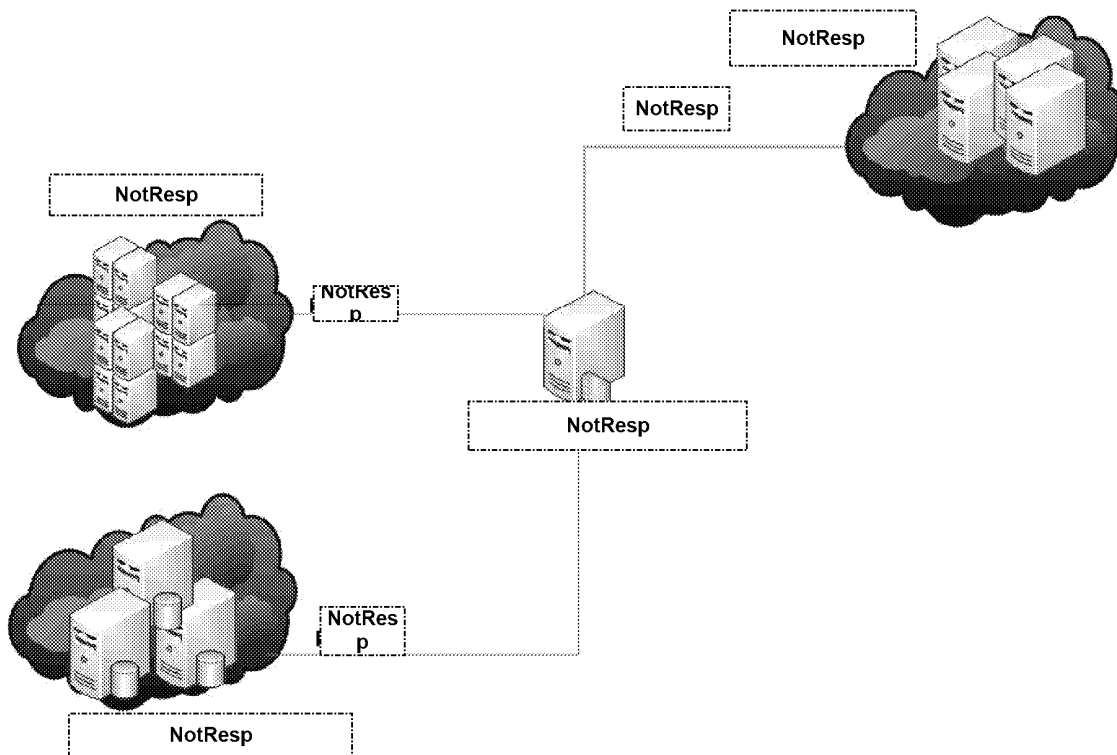
Template Draft v3 Oct 1, 2013

1. Executive Summary

1.1 Background

The CMS –eCloud network has a need for monitoring Federally Facilitated Marketplace application and data servers to give a higher visibility of the servers cpu utilization, memory, and throughput. The system monitoring tool, **NotResp** is a SaaS solution that monitors the overall performance and resource utilization of a system. This tool uses in-process **NotResp** **NotResp** to pages as they are built. This allows the agent to use timing information detail to identify specific web transactions processed on the backend as well as how much time was spent for each request. Monitoring this information also helps identify application server response time, web transactions, and throughput. Before the **NotResp** solution was implemented, there was no solution in place to identify these specific concerns. The **NotResp** addresses concerns of introducing new agents to the CMS eCloud private cloud environment can pose potential compatibility and security issues.

Figure 1:



1.2 Purpose

To have near real time visibility of the performance of FFM application and data servers, **NotResp** collects performance metrics from applications and systems, uploads those metrics to the **NotResp**

NotResp service, and presents application performance information through a secure website. This information can be used to assess the overall performance of the servers.

1.2.1 System Functions

Function	Description
Agents	Agents reside on servers within the CMS eCloud environment and communicate to New Relic service .
Application Errors	Collects exception class and stack trace from requests, along with 404 and 500 errors.
Transaction Traces	Snapshots of a single application transaction.
Inbound Data Transmission	NotResp uses an inbound data transmission method that sends collected application performance information over SSL-that is encrypted using HTTPS.

Table 1: System Functions

NotResp collects the following aggregate metric data for all applications:

- Application request activity, including view and controller breakdowns
- Database query activity, including create, update, and delete breakdowns
- View activity
- Requests that result in an error
- Process memory and CPU usage

The Security Impact Analysis is required per NIST 800-53, Certification and Accreditation (CA-2) and Change Management (CM-4) controls. CA-2 requires security analysis whenever updates are made to system security authorization artifacts, and CM-4 further defines the requirement for a System Impact Analysis. The System Security Plan will be updated with this change with 90 days, if it is determined that this service will remain in place.

2. System Identification

2.1 System Name/Title

System Identifier	Response Data
Official System Name:	Federally Facilitated Marketplace
System Acronym:	FFM

Classification:	Moderate
------------------------	----------

2.2 Designated Contacts

Business Owner	Response Data
Name:	James Kerr
Contact Information:	Deputy Director CCIO 7501 Wisconsin Ave. MS 38-3811 Bethesda, MD 20814 James.Kerr@cms.hhs.gov Phone: 212-616-2205

System Maintainer	Response Data
Name:	Mark Oh
Contact Information:	Division Director CIISG 7501 Wisconsin Ave. MS 38-3811 Bethesda, MD 20814 Mark.Oh@cms.hhs.gov Phone: 301-492-4378 Cell: (b)(6)

2.3 Assignment of Security Responsibility

Individual Responsible for Security (ISSO)	Response Data
Name:	Thomas Schankweiler
Contact Information:	Systems Security Officer (SSO) CIISG 7500 Security Blvd. MS N2-13-03 Baltimore, MD 21244 Thomas.Schankweiler@cms.hhs.gov Phone: 410-786-5956 Cell: (b)(6)

Individual Responsible for Security (ISSO)	Response Data
Name:	Darrin Lyles
Contact Information:	Information Systems Security Officer (SSO) CIISG 7500 Security Blvd. MS N2-13-03 Baltimore, MD 21244 Darrin.Lyles@cms.hhs.gov Phone: 410-786-4744 Cell: (b)(6)

3. System Analysis

NotResp

agents are installed on FFM application and data servers that are running

NotResp

NotResp

NotResp

agent connects to the NotResp web service, collects and disseminates pertinent information pertaining regarding FFM applications. The collections consist of the following:

- The OS type and version
- The version of NotResp
- All system properties
- The contents of the NotResp

Additionally, the collections will consist of the following types of data.

Aggregate metrics

These are counters that track the number of times a "normalized" url request is made and it's average response time. Aggregate metrics drive the time-series graphs on the website. We also create metrics for database tables. NotResp

Transaction traces

This is a complete snapshot of a single web request. They are collected only for slow requests. Only the slowest transaction trace per minute is sent to the NotResp website. Transaction traces include detailed information about the request, including (optionally) HTTP parameters and obfuscated NotResp

Error snapshots

These record uncaught exceptions that the application is propagating back to the web browser. They optionally contain the HTTP parameters of the request and also the exception that was unhandled. Part of the exception is a stack trace from the managed application

Enterprise Security Enabled

The NotResp has been configured to run in High Security Mode, also known as Enterprise Security Mode. This mode provides extra security in the ways

1. Requires agents to use SSL

Enterprise security mode requires an SSL connection. Non-SSL connection attempts will be rejected. The latest versions of all NotResp agents support SSL.

2. Prevents HTTP param capture

Agents configured to capture HTTP params, which may contain sensitive customer data, are not allowed to connect to **NotResp**. If the application is using server-side configuration, enterprise security mode will override the configuration to never capture HTTP params.

3. Prevents raw statement capture

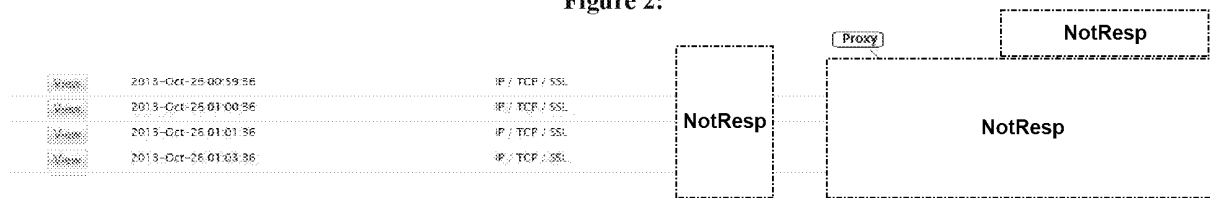
Agents configured to capture raw statements, which may contain sensitive customer data, are not allowed to connect to **NotResp**. If the application is using server-side settings, enterprise security mode will override the configuration to never capture raw **NotResp**.

New Relic Network Traffic Configuration

Current network configurations make use of the proxy **NotResp**. Internal traffic is routed to the proxy over **NotResp**. The proxy server then routes all encrypted traffic to **NotResp**.

Figure 2 is a sample of outbound CMS eCloud encrypted data being routed from the proxy to the newrelic.com service.

Figure 2:



NotResp

Agent Configuration

NotResp

NotResp

NotResp

NotResp

NotResp

3.1 Impact

There will be no negative security impact to the existing FFM environment and their applications. There will; however, be a “positive business impact” providing ability for real time application monitoring and the prevention of bottlenecks. Thus, providing a benefit for both performance and security.

The **NotResp** agents are located in the newrelic class package name and therefore should never collide with FFM’s application classes. The agent uses the **NotResp** engine to insert software probes, which **NotResp** has measured to impact the start time of the application by less than 10%. Application response times should see less than a 5% slowdown since instrumentation is only at request handling and remote system call methods. Memory impact yields approximately 5%.

With regards to security issues, **NotResp** agents are configured to send collected data through a proxy. This proxy is known as **NotResp** an additional proxy may be added in the future. All traffic going through this proxy is encrypted over SSL. Firewall settings have been set to **NotResp**

Data is posted via http or https once a minute from the agent to the **NotResp** website. The message format is **NotResp** The website returns a **NotResp** response to the agent notifying if the data was correctly received or if there was an error. For auditing purposes, the agent is able to dump to a log file communications.

3.2 Risk Analysis

NotResp provides an easy to use web interface to Common Vulnerabilities and Exposure (CVE) information. Data is derived from National Vulnerability Database (NVD) by

National Institute of Standards and Technology (NIST). The site has ~~only has one~~ reported CVE for **NotResp** which is a **NotRes** component **NotRes** is NOT an invoked **NotResp** element for the CMS implementation on the FFM **NotRe** servers.

NotResp

The following FFM risks are applicable to this SIA:

Table 1 Sample Risk Matrix

Title	Risk Description	Probability Occurrence	Risk Rating	Mitigation
NotResp SaaS application is not Fedramp Certified	CMS cannot validate if the vendor has implemented security controls that are compliant with NIST 800-53 Rev4 controls.	High	Moderate	CMS OIS/OC has been using the vendor site for five years without issue. However, the vendor site was never included in the SCA testing. No PII information is transmitted or stored at the vendor site.
NotResp	NotResp	High	Moderate	NotResp

Title	Risk Description	Probability Occurrence	Risk Rating	Mitigation
	NotResp			Action should be completed by 10/28/2013.
Exposure or loss of data hosted at NotResp.com	CMS system performance data could be exposed. Access would reveal the following types of system information [not all inclusive] for FFM NotResp system name, IP address, server performance statistics, and error codes. There is no chance of exposure of personal information.	Low	Moderate	NotResp
Update CFACTS, RA and SSP	Review of system in CFACTS would result in a finding that security documentation is not current	Low	Low	Update SSP and RA with reference to NotResp along with description and diagrams updates to CFACTS within the 90 days of signature, if deemed that this service will remain.

As the Business Owner/Manager and Certification Official, I have examined this Security Impact Analysis report for this system and consider them adequate to meet agency policy and the relevant business requirements. I also understand and accept the risk inherent in processing on a network or at the installation(s) that supports this system, particularly where the support system is operated outside of my management control. My acceptance is based solely upon the documentation provided within this SIA and the concurrence of the ISSO and System Maintainer.

(Thomas Schankweiler) _____ (signature) _____

Information System Security Officer

Date

(Mark Oh) _____ (signature) _____

System Developer / Maintainer

Date

(Monique Outerbridge) _____ (signature) _____

Business Owner

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N3-15-25
Baltimore, Maryland 21244-1850



OFFICE OF INFORMATION SERVICES

MEMORANDUM

DATE:

TO: Director,
Consortium for Medicare Health Plans Operations (OA/CMHPO) and Acting
Deputy Center Director for Operations, Center for Consumer Information and
Insurance Oversight (CCIIO)

FROM: Chief Information Officer and
Director, Office of Information Services (OIS)

SUBJECT: Authorization Decision for the Federally Facilitated Marketplace (FFM) System

ACTION REQUIRED 30 DAYS FROM THE DATE OF THIS MEMORANDUM

The Federally Facilitated Marketplace (FFM) is a *Moderate* level system to be located at the Terremark datacenter in Culpeper, Virginia. The system maintains records used to support all Health Insurance Exchange Programs established by the Centers for Medicare & Medicaid Services (CMS) under the health care reform provisions of the Affordable Care Act (Public Law 11-148). FFM will help qualified individuals and small business employers shop for, select, and pay for high-quality, affordable health coverage. FFM will have the capability to determine eligibility for coverage, for tax credits, and for cost-sharing reductions; as well as eligibility for Medicaid, Basic Health Plan (BHP), and Children's Health Insurance Program (CHIP) coverage. As part of the eligibility and enrollment process, financial, demographic, and health information will flow through the Marketplace.

I am issuing an Authorization to Operate (ATO) for the FFM information system to operate in its current environment and configuration until **March 20, 2014**. The current configuration of FFM only includes: Qualified Health Plan (QHP); QHP-Dental; Eligibility & Enrollment (E&E) (except: Identify Proofing for Agent/Broker and Call Center initiated applications; Second chance application completion; Advance Premium Tax Credits (APTC) eligibility determination; Cost Sharing Reduction (CSR) eligibility determination; Outbound account transfer for eligibility determination; Change in circumstances for plan compare; Eligibility Support Desktop (ESD); Direct Enrollment issuer redirects for eligibility determination; Direct Enrollment minor web interface; Initial/Change Enrollment cancel/terminate functionality; Enrollment validation of parsing of inbound 834 messages; Enrollment outbound business acknowledgement generation; Enrollment State-Based Marketplace (SBM) inbound 834 transactions; Enrollment Data Store (EDS); Enrollment double dip check; Small Business Health Options Program; Call Center user interface; and Call Center notices and mailing); Financial Management (FM) (except: Vendor and banking collection information, SBM data collection, and CSR calculation); and Plan Management (PM) (except: QHP Public Use File, Unified Rate Review (URR) Content Reviewer, Plan ratification and accreditation, Plan transfer, Deficiency Notices, and LMI Analyzer).

This system is not authorized to establish any new connections or interfaces with non-CMS FISMA or other non-CMS connections without prior approval during the period of this ATO. An impact analysis must be conducted for any system changes implemented after the issuance of this ATO. Any major modifications that affect the security posture of the system will require an appropriately scoped security controls assessment and issuance of a new ATO.

The security authorization of the information system will remain in effect until the indicated expiration date if the following conditions are maintained:

- (i) Required periodic security status reports for the system are submitted to this office in accordance with current CMS policy;
- (ii) New vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk that is deemed unacceptable; and
- (iii) The system has not exceeded the maximum allowable time between security authorizations in accordance with Federal or CMS policy.

The attachment provides information on requirements not met, as well as corrective actions needed to bring them into compliance. The actions set forth in the attachment must be entered into the approved CMS Plan of Action and Milestones (POA&M) tracking tool no later than 30 days from the date of this memorandum, and the action items addressed no later than the designated completion dates. This office will monitor all POA&M items submitted during the period of authorization.

If you have questions, please contact Teresa Fryer, Chief Information Security Officer (CISO), at 410-786-2614. The DISPC team is also available to support staff level questions at CISO@cms.hhs.gov.

Tony Trenkle

Attachment

cc:

Mark Oh, Director OIS/CIISG/DHIM
Darrin Lyles, ISSO, OIS/CIISG/DSMDS
Teresa Fryer, CISO, Director OIS/EISG
Michael Mellor, Dep. CISO, Dep. Director OIS/EISG
Desmond Young, OIS/EISG/DISPC
Jessica Hoffman, OIS/EISG/DISPC
James Mensah, OIS/EISG/DISPC

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Attachment

Federally Facilitated Marketplace (FFM) System

Authorization Decision

Authorization decision is required for the following reason(s):

	New System
X	Major system modification
	Serious security violation
	Changes in the threat environment
	Expired authorization to operate

I. Authorization Decision

X	Authorization to Operate The applicable system is authorized to operate until the designated date, subject to the authorization actions in Section II.
This authorization will expire: <u>March 20, 2014</u>. This authorization may be withdrawn at the discretion of the Authorizing Official for lack of progress on the authorization actions in Section II, or any security violations deemed to increase the risk to CMS beyond a tolerable level.	

	Denial of Authorization to Operate The applicable system <u>may not operate</u> until the authorization actions listed in Section II are completed, after which, verification of corrective actions and resubmission of the authorization package is required.
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

(Authorizing Official Signature and Date)

Tony Trenkle

CMS Chief Information Officer

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Federally Facilitated Marketplace (FFM) System**II. Authorization Actions**

Failure to meet the assigned due dates without prior approval invalidates this authorization to operate. The following specific actions are to be completed by the date(s) indicated:

Finding	Finding Description	Recommended Corrective Action	Risk	Due Date
NotResp				July 31, 2015
	NotResp		NotResp	
END OF ACTIONS				

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING
Federal Facilitated Marketplace (FFM) System

**DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES
OIS/EISG
RECORD OF SIGN OFFS**

Prepared by: Jerry Oar

Phone: 541-673-9085

Fax No. 703-361-0384

Typed By: Jerry Oar

Phone: 541-673-9085

Disc Identifier: FFM ATO ltr 9-26-2013

ACTION	NAME	OFF/DIV/BR	INITIALS/DATE
REVIEWED BY	Jacqueline Toomey	OIS/EISG/DISPC	
REVIEWED BY	Michael Mellor	OIS/EISG	
REVIEWED BY	Teresa Fryer	OIS/EISG	
REVIEWED BY	George Linares	OIS	
CLEARED BY	Tony Trenkle	OIS	

KEYWORD:

COMMENTS: Authorization To Operate form(s) attached for the CMS CIO's signature.

Please Return to Linda Velasco, EISG

Please include the name of someone who we can contact in your absence for questions/information.

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Federally Facilitated Marketplaces (FFM)

Executive Summary

There is an **Authorization to Operate (ATO) until March 20, 2014** to allow testing and closure of risk weaknesses in FFM and the supporting infrastructure. The current configuration includes: Qualified Health Plans (QHP), QHP-Dental modules, parts of Plan Management (PM), parts of Eligibility & Enrollment (E&E), and parts of Financial Management (FM).

Authorization Summary:

The following is a review summary of FFM:

- **The independent validation contractor was unable to adequately test the confidentiality and integrity of the FFM system in full.** The majority of the contractor's testing efforts were focused on testing the expected functionality of the application. Complete end-to-end security testing of the FFM application never occurred. Several factors contributed to the limited effectiveness of the SCA.

The contractor was not able to complete testing because:

- *Testing environments and module interconnections were not ready for the SCA.*
- *Valid test data was not provided prior to testing.*
- *Test environment availability was not consistent.*
- *Environments were not dedicated to SCA testing.*

Current Security Assessment Status Summary

Contractor	Assessment Status	POA&M (Y/N)
MITRE Blue Canopy	*2 high, 22 moderate and 13 low findings remain open (4/12/2013 MITRE) 3 moderate and 5 low findings remain open (9/19/2013 Blue Canopy) 11 moderate and 8 low findings remain open (9/19/2013 MITRE)	No for the Blue Canopy and the 2 nd MITRE tests

Points of Contact (POCs) were confirmed by CFACTS

System Level	Business Owner	Sys Developer/ Maintainer	ISSO
Moderate	James Kerr OA/CMHPO	Mark Oh OIS/CIISG/DHIM	Darrin Lyles OIS/CIISG/DSMDS

Documentation Artifacts

Authorization Request	SSP	RA	CP	CP Test	Security Assessment	PIA
	09/09/2013 Updates Included	09/09/2013 Updates Included	08/05/2013 Not Signed	08/16/2013	*04/12/2013 09/19/2013 MITRE 09/19/2013 Blue Canopy	08/05/2013

There was a FFM ATO memorandum signed and dated September 3, 2013. Although the action items from that ATO are not in CFACTS, they are applicable to this ATO. CIISG did not provide a Certification Form for this current authorization request.

*There are weaknesses listed in CFACTS from the FFM_FFE_SCA_05032013-FFM_FFE-QHP_SCA document. The weakness milestones were disapproved by EISG.

FFM could not be fully assessed during the August and September assessment attempts.

Note: Blue Canopy indicated –“Publically Accessible Data: Using NotResp data was accessed that should not be publically accessible. We recommend considering the potential security risks from divulging this data and implementing appropriate controls.” The incident response (IR) family assessment was not included in the scope of the independent tests. However, a review of the documentation included reviews of the IR family. The System Security Plan incorrectly indicates e-authentication level 2 which provides very little identity proofing to assist in protecting sensitive data and incident investigations.

Federally Facilitated Marketplaces (FFM)

Executive Summary

Recommended Decision:

- **Denial Authorization To Operate (DATO).** This allows testing and closure of risk weaknesses in FFM and the supporting infrastructure. The current configuration includes only the Federally Facilitated Marketplaces; Qualified Health Plans (QHP), and Dental modules, Plan Management (PM), Eligibility & Enrollment (E&E), My Account, Individual Application, Plan Compare, Eligibility Support Desktop (ESD), Call Center Integration, Direct Enrollment, Federal Functions (Double Dipping), Federal Functions (EDS to store FFM and SBM Transactions), Enrollment, Notices, Mailing Contractor Integration, and Financial Management (FM). Other FFM modules will be added in the future requiring their own Security Control Assessment (SCA).

Authorization Summary:

The following is a review summary of FFM:

- **MITRE was unable to adequately test the Confidentiality and Integrity of the HIX system in full.** The majority of the MITRE's testing efforts were focus on testing the expected functionality of the application. Complete end to end testing of the HIX application never occurred. Several factors contributed to the limited effectiveness of this SCA.

MITRE was not able to complete testing do to:

- *Testing environments and module interconnections were not ready for the SCA.*
- *Valid test data was not provided prior to testing.*
- *Test environment availability was not consistent.*
- *Environments were not dedicate to SCA testing.*

-

NotResp

The presence of high risk findings in a system represents an increased risk to the CMS enterprise. Lifecycle management of the system requires initial testing for FISMA authorization and continuous monitoring. Non-compliance with the *CMS Information Security (IS) Acceptable Risk Safeguards (ARS)*, *CMS Minimum Security Requirements (CMSR)* without continuous monitoring presents an unacceptable risk.

- NotResp

The presence of high risk findings in a system represents an increased risk to the CMS enterprise. Lifecycle management of the system requires initial testing for FISMA authorization and continuous monitoring. Non-compliance with the *CMS Information Security (IS) Acceptable Risk Safeguards (ARS)*, *CMS Minimum Security Requirements (CMSR)* without continuous monitoring presents an unacceptable risk.

- **All FFM weaknesses in CFACTS are in a delayed status.** Not mitigating the FFM weaknesses weakens the security posture of FFM and the CMS enterprise and as such requires immediate attention to provide the level of protection mandated by CMS.

FFM weaknesses have twice failed Component Validation, due to the lack of the required Corrective Action Plan (CAP) that should provide detailed milestones which describe planned actions necessary for FFM to correct the security deficiency and remediate the weaknesses.

- **All FFM controls are described in CFACTS as “Not Satisfied”.** Security controls are not documented as being fully implemented.

This introduces the possibility that the FFM controls are ineffective. Ineffective controls do not appropriately protect the confidentiality, integrity and availability of data and present a risk to the CMS enterprise.

- NotResp

- **Control inheritance is incorrectly documented in CFACTS.** FFM indicates many of its controls are “under the control of the

NotResp

 however, these controls are not marked as inherited from the

NotResp

 and do not accurately describe the security control implementation within CFACTS. For example, many controls describe other systems such as the Rate and Benefit Information System (RBIS) and the Health Insurance Oversight System (HIOS).

Unclear control responsibility can lead to controls not being appropriately implemented and a lack of accountability.

-

NotResp

Unclear role responsibility can affect the life cycle support of the FFM system.

Current Security Assessment Status Summary

Contractor	Assessment Status	POA&M (Y/N)
MITRE	*2 high, 22 moderate and 13 low findings remain open (4/12/2013) 11 moderate and 8 low findings remain open (9/19/2013)	N

Points of Contact (POCs) were confirmed by CFACTS

System Level	Business Owner	Sys Developer/ Maintainer	ISSO
Moderate	James Kerr OA/CMHPO	Mark Oh OIS/CIISG/DHIM	Darrin Lyles OIS/CIISG/DSMDS

Documentation Artifacts

Authorization Request	SSP	RA	CP	CP Test	Security Assessment	PIA
	07/29/2013 redline version	Draft		none	*04/12/2013 08/30/2013 09/19.2013	Draft 2012

*There are weaknesses listed in CFACTS from a referenced document FFM_FFE_SCA_05032013-FFM_FFE-QHP_SCA. The weakness milestones were disapproved by EISG. The weaknesses were entered into CFACTS in May of 2013. There were additional security control assessment attempts in August and September 2013. *The FFM could not be fully assessed.*

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N3-15-25
Baltimore, Maryland 21244-1850



OFFICE OF INFORMATION SERVICES

MEMORANDUM

DATE:

TO: Director
Consumer Information and Insurance Systems Group (OIS/CIISG)

FROM: Chief Information Officer and
Director, Office of Information Services (OIS)

SUBJECT: Authorization Decision for the Data Services Hub (DSH)

ACTION REQUIRED 30 DAYS FROM THE DATE OF THIS MEMORANDUM

The Data Services Hub (DSH) is a *Moderate* level system located at the Terremark Data Center in Culpeper, Virginia. DSH provides an electronic connection between the eligibility systems of the Marketplaces to already existing, secure Federal and state databases to verify the information a consumer provides in their Marketplace application. Data transmitted through the Hub will help State agencies determine applicants' eligibility to enroll in Medicaid or CHIP, and will help the Federally-facilitated and State-based Marketplace eligibility systems determine an applicant's eligibility to seek health insurance coverage through a Marketplace, their eligibility for advance premium tax credits, and cost-sharing reductions.

On August 30, 2013, you certified the controls for the system and submitted along with your certification the other required documentation necessary to obtain an Authorization to Operate (ATO) for DSH.

I have determined through a thorough review of the authorization package that the risk to CMS information and information systems resulting from the operation of the DSH information system is acceptable predicated on the completion of the actions described in the attachment. Accordingly, **I am issuing an Authorization to Operate (ATO)** for the DSH information system to operate in its current environment and configuration until **August 30, 2016**. This system is not authorized to establish any new connections or interfaces with non-CMS FISMA or other non-CMS connections without prior approval during the period of this ATO. An impact analysis must be conducted for any system changes implemented after the issuance of this ATO. Any major modifications that affect the security posture of the system will require an appropriately scoped security controls assessment and issuance of a new ATO.

The security authorization of the information system will remain in effect until the indicated expiration date if the following conditions are maintained:

- (i) Required periodic security status reports for the system are submitted to this office in accordance with current CMS policy;
- (ii) New vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk that is deemed unacceptable; and

- (iii) The system has not exceeded the maximum allowable time between security authorizations in accordance with Federal or CMS policy.

The attachment provides information on requirements not met, as well as corrective actions needed to bring them into compliance. The actions set forth in the attachment must be entered into the approved CMS Plan of Action and Milestones (POA&M) tracking tool no later than 30 days from the date of this memorandum, and the action items addressed no later than the designated completion dates. This office will monitor all POA&M items submitted during the period of authorization.

If you have questions, please contact Teresa Fryer, Chief Information Security Officer (CISO), at 410-786-2614. The DISPC team is also available to support staff level questions at CISO@cms.hhs.gov.

Tony Trenkle

Attachment

cc:

Mark Oh, Director OIS/CIISG/DHIM
John England-Gordon, ISSO, OIS/CIISG/DPMG
Teresa Fryer, CISO, Director OIS/EISG
Michael Mellor, Dep. CISO, Dep. Director OIS/EISG
Desmond Young, OIS/EISG/DISPC
Jessica Hoffman, OIS/EISG/DISPC
James Mensah, OIS/EISG/DISPC

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Attachment

Data Services Hub (DSH)

Authorization Decision

Authorization decision is required for the following reason(s):

X	New System
	Major system modification
	Serious security violation
	Changes in the threat environment
	Expired authorization to operate

I. Authorization Decision

I have reviewed the information concerning the request for an Authorization to Operate and with consideration of the recommendations provided by my staff, I concur with the assessment of the security risk. This risk has been weighed against the business operational requirements and security measures that have or will be implemented. I have determined the following authorization decision is appropriate.

X	Authorization to Operate The current risk is deemed acceptable. The applicable system is authorized to operate until the designated date, subject to the authorization actions in Section II.
This authorization will expire: August 30, 2016. This authorization may be withdrawn at the discretion of the Authorizing Official for lack of progress on the authorization actions in Section II, or any security violations deemed to increase the risk to CMS beyond a tolerable level.	

	Denial of Authorization to Operate The current risk is deemed unacceptable. The applicable system <u>may not operate</u> until the authorization actions listed in Section II are completed, after which, verification of corrective actions and resubmission of the authorization package is required.
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

(Authorizing Official Signature and Date)

Tony Trenkle

CMS Chief Information Officer

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING**Attachment****Data Services Hub (DSH)****II. Authorization Actions**

Failure to meet the assigned due dates without prior approval invalidates this authorization to operate. The following specific actions are to be completed by the date(s) indicated:

Finding	Finding Description	Recommended Corrective Action	Risk	Due Date
				November 15, 2013
		NotResp		October 15, 2013

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING**Attachment****Data Services Hub (DSH)**

Finding	Finding Description	Recommended Corrective Action	Risk	Due Date
				December 31, 2013
				December 31, 2013
				December 31, 2013
END OF ACTIONS				

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING
Data Services Hub (DSH)

**DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES
OIS/EISG
RECORD OF SIGN OFFS**

Prepared by: Anita Updike

Phone: 703-393-4249

Fax No. 703-361-0384

Typed By: Anita Updike

Phone: 703-393-4249

Disc Identifier: DSH_ATO_ltr_09-04-2013-1

ACTION	NAME	OFF/DIV/BR	INITIALS/DATE
CLEARED BY	Jacqueline Toomey	OIS/EISG/DISPC	
CLEARED BY	Michael Mellor	OIS/EISG	
CLEARED BY	Teresa Fryer	OIS/EISG	
CLEARED BY	George Linares	OIS	
CLEARED BY	Tony Trenkle	OIS	

KEYWORD:

COMMENTS: Authorization To Operate form(s) attached for the CMS CIO's signature.

Please Return to Linda Velasco, EISG

Please include the name of someone who we can contact in your absence for questions/information.

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N3-15-25
Baltimore, Maryland 21244-1850



OFFICE OF INFORMATION SERVICES

MEMORANDUM

DATE:

TO: Director
Consortium for Medicare Health Plans Operations (OA/CMHPO)

FROM: Chief Information Officer and
Director, Office of Information Services (OIS)

SUBJECT: Authorization Decision for the Federal Facilitated Marketplace (FFM) System

ACTION REQUIRED 30 DAYS FROM THE DATE OF THIS MEMORANDUM

The Federal Facilitated Marketplace (FFM) System is a *Moderate* level system located at the Terremark Datacenter in Culpepper, Virginia. The system maintains records used to support all Health Insurance Exchange Programs established by the Centers for Medicare & Medicaid Services (CMS) under the health care reform provisions of the Affordable Care Act (Public Law 11-148). FFM will help qualified individuals and small business employers shop for, select, and pay for high-quality, affordable health coverage. Exchanges will have the capability to determine eligibility for coverage through the Exchange, for tax credits and cost-sharing reductions, and for Medicaid, Basic Health Plan (BHP) and Children's Health Insurance Program (CHIP) coverage. As part of the eligibility and enrollment process, financial, demographic, and (potentially) health information will flow through the Exchange.

On August 8, 2013, you certified the controls for the system and submitted along with your certification the other required documentation necessary to obtain an Authorization to Operate (ATO) for FFM.

I have determined through a thorough review of the authorization package that the risk to CMS information and information systems resulting from the operation of the FFM information system is acceptable predicated on the completion of the actions described in the attachment. Accordingly, **I am issuing an Authorization to Operate (ATO)** for the FFM information system to operate in its current environment and configuration until **May 30, 2016**. The current configuration includes only the Federal Facilitated Marketplace; Qualified Health Plans (QHP) and Dental modules. This system is not authorized to establish any new connections or interfaces with non-CMS FISMA or other non-CMS connections without prior approval during the period of this ATO. Any major system modifications implemented after the issuance of this ATO that changes the security posture will require a full security controls assessment and a new ATO.

The security authorization of the information system will remain in effect until the indicated expiration date if the following conditions are maintained:

- (i) Required periodic security status reports for the system are submitted to this office in accordance with current CMS policy;

- (ii) New vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk that is deemed unacceptable; and
- (iii) The system has not exceeded the maximum allowable time between security authorizations in accordance with Federal or CMS policy.

The attachment provides information on requirements not met, as well as corrective actions needed to bring them into compliance. The actions set forth in the attachment must be entered into the approved CMS Plan of Action and Milestones (POA&M) tracking tool no later than 30 days from the date of this memorandum, and the action items addressed no later than the designated completion dates. This office will monitor all POA&M items submitted during the period of authorization.

If you have questions, please contact Teresa Fryer, Chief Information Security Officer (CISO), at 410-786-2614. The DISPC team is also available to support staff level questions at CISO@cms.hhs.gov.

Tony Trenkle

Attachment

cc:

Mark Oh, Director OIS/CIISG/DHIM
Darrin Lyles, ISSO, OIS/CIISG/DSMDS
Teresa Fryer, CISO, Director OIS/EISG
Michael Mellor, Dep. CISO, Dep. Director OIS/EISG
Desmond Young, OIS/EISG/DISPC
Jessica Hoffman, OIS/EISG/DISPC
James Mensah, OIS/EISG/DISPC

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Attachment

Federally Facilitated Marketplace (FFM) System

Authorization Decision

Authorization decision is required for the following reason(s):

X	New System
	Major system modification
	Serious security violation
	Changes in the threat environment
	Expired authorization to operate

I. Authorization Decision

I have reviewed the information concerning the request for an Authorization to Operate and with consideration of the recommendations provided by my staff; I concur with the assessment of the security risk. This risk has been weighed against the business operational requirements and security measures that have or will be implemented. I have determined the following authorization decision is appropriate.

X	Authorization to Operate The current risk is deemed acceptable. The applicable system is authorized to operate until the designated date, subject to the authorization actions in Section II.
This authorization will expire: May 30, 2016. This authorization may be withdrawn at the discretion of the Authorizing Official for lack of progress on the authorization actions in Section II, or any security violations deemed to increase the risk to CMS beyond a tolerable level.	

	Denial of Authorization to Operate The current risk is deemed unacceptable. The applicable system <u>may not operate</u> until the authorization actions listed in Section II are completed, after which, verification of corrective actions and resubmission of the authorization package is required.
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

(Authorizing Official Signature and Date)

Tony Trenkle

CMS Chief Information Officer

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Attachment

Federally Facilitated Marketplace (FFM) System**II. Authorization Actions**

Failure to meet the assigned due dates without prior approval invalidates this authorization to operate. The following specific actions are to be completed by the date(s) indicated:

Finding	Finding Description	Recommended Corrective Action	Risk	Due Date
		NotResp		July 31, 2015

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Attachment

Federally Facilitated Marketplace (FFM) System

Finding	Finding Description	Recommended Corrective Action	Risk	Due Date
				February 1, 2014
		NotResp		February 1, 2014

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Attachment

Federally Facilitated Marketplace (FFM) System

Finding	Finding Description	Recommended Corrective Action	Risk	Due Date
		NotResp		February 1, 2014
				February 1, 2014
END OF ACTIONS				

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING
Federal Facilitated Marketplace (FFM) System

**DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES
OIS/EISG
RECORD OF SIGN OFFS**

Prepared by: Jerry Oar

Phone: 541-673-9085

Fax No. 703-361-0384

Typed By: Jerry Oar

Phone: 541-673-9085

Disc Identifier: FFM_ATO_ltr_8-20-2013

ACTION	NAME	OFF/DIV/BR	INITIALS/DATE
CLEARED BY	Jacqueline Toomey	OIS/EISG/DISPC	
CLEARED BY	Michael Mellor	OIS/EISG	
CLEARED BY	Teresa Fryer	OIS/EISG	
CLEARED BY	George Linares	OIS	
CLEARED BY	Tony Trenkle	OIS	

KEYWORD:**COMMENTS:** Authorization To Operate form(s) attached for the CMS CIO's signature.

Please Return to Linda Velasco, EISG

Please include the name of someone who we can contact in your absence for questions/information.

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Federally Facilitated Marketplace (FFM)

Executive Summary

Recommended Decision:

- **Authorization To Operate (ATO) until May 30, 2016.** This ATO date allows testing and closure of high risk weaknesses in FFM and the supporting infrastructure. The current configuration includes only the Federally Facilitated Marketplace; Qualified Health Plans (QHP) and Dental modules. Other FFM modules will be added in the future requiring their own Security Control Assessment (SCA).

Authorization Summary:

The following is a review summary of FFM:

- **FFM has open high findings from a development test.** The most recent security assessment for FFM indicates there are open high findings which should require quarterly reviews and continued testing.

The presence of high risk findings in a system represents an increased risk to the CMS enterprise. Lifecycle management of the system requires initial testing for FISMA authorization and continuous monitoring. Non-compliance with the *CMS Information Security (IS) Acceptable Risk Safeguards (ARS)*, *CMS Minimum Security Requirements (CMSR)* without continuous monitoring presents an unacceptable risk.

- **All FFM controls are described in CFACTS as “Not Satisfied”.** Security controls are not documented as being fully implemented.

This introduces the possibility that the FFM controls are ineffective. Ineffective controls do not appropriately protect the confidentiality, integrity and availability of data and present a risk to the CMS enterprise.

- **FFM has selected an inappropriate E-Authentication level.** FFM information contains financial privacy data. *CMS System Security & E- Authentication Levels by Info Type* indicates that Privacy Data should be protected by E-Authentication Level 3 controls.

The E- Authentication level of a system determines the controls which should be in place when connecting to a system over an untrusted network. Use of inappropriate controls exposes the enterprise to additional risk.

- **Control inheritance is incorrectly documented in CFACTS.** FFM indicates many of its controls are “under the control of the Terremark PaaS”; however, these controls are not marked as inherited from the PaaS and do not accurately describe the security control implementation within CFACTS. For example, many controls describe other systems such as the Rate and Benefit Information System (RBIS) and the Health Insurance Oversight System (HIOS).

Unclear control responsibility can lead to controls not being appropriately implemented and a lack of accountability.

- **CMS Security Certification Form and updated POC list from CFACTS do not match.** The system developer/maintainer on the CMS Security Certification Form is different from the person listed on the POC list.

Unclear role responsibility can affect the life cycle support of the FFM system.

Current Security Assessment Status Summary

Contractor	Assessment Status	POA&M (Y/N)
MITRE	*2 high, 22 moderate and 13 low findings remain open.	Y

Points of Contact (POCs) were confirmed by CFACTS

System Level	Business Owner	Sys Developer/ Maintainer	ISSO
Moderate	James Kerr OA/CMHPO	Mark Oh OIS/CIISG/DHIM	Darrin Lyles OIS/CIISG/DSMDS

Documentation Artifacts

Authorization Request	SSP	RA	CP	CP Test	Security Assessment	PIA
08/08/2013	07/29/2013 redline version	Draft	Draft	none	*04/12/2013	Draft 2012

*There are weaknesses listed in CFACTS from a referenced document

NotResp The weakness milestones were disapproved by EISG. The weaknesses were entered into CFACTS in May of 2013. Two emails were sent to FFM to update the weaknesses in CFACTS, yet nothing was done.

Weakness Listed in CFACTS

8/8/2013

There were 37 findings found in April 2013 that have not been resolved. In total they increase and put the CMS enterprise at risk. High open findings precludes an accurate risk assessment to the system, the business function, and the enterprise. Without known risk in a system that has known multiple vulnerabilities, a long term ATO is not recommended.

Weakness	Risk Category
NotResp	High
Software is being deployed into implementation and production that contains functional errors. Untested software may produce functional errors that cause unintentional Denial of Service and information errors. "	High
NotResp	Moderate
Information was missing from the SSP. The SSP evaluation document provided by MITRE contains specific details. Without complete and updated information about the controls, it is not possible to test and verify whether the security controls are adequate to protect it at the necessary level. This poses a problem for the business owner who must make the decision to accept the residual risk when approving a system to operate using incomplete information."	Moderate
NotResp Contingency plan testing has not been performed. The risks of not testing the contingency plan are that 1. Key steps may have been omitted; 2. The plan, as written, may not work and that staff are not familiar with the plan and their role in the process. This increases the risk of not being able to successfully respond to an emergency situation in which a key business system is no longer available."	Moderate

NotResp	Moderate
	Moderate
	Moderate
	Moderate
	Moderate
	Moderate
	Moderate
	Moderate

<p>NotResp</p>	Moderate
	Moderate
	Moderate
	Moderate
	Moderate
	Moderate
Unauthorized application development can introduce a variety of vulnerabilities to the database."	Moderate
NotResp	Moderate

<div>NotResp</div> <p>Information was missing from the contingency plan. The evaluation provided by MITRE contains specific details. The risk of an incomplete CP is that when the plan is put into effect, missing information can increase the risk of the organization not achieving recovery time objectives for the application and system, thus not satisfying the business requirements for system availability."</p>	Moderate
<div>NotResp</div> <p>Information was missing from the RA. The RA evaluation document provided by MITRE contains specific details. Ensure all risks associated with QHP and any controls not implemented for the application are included in the RA. The risk of an incomplete RA or missing documentation is that the business owner and Chief Information Security Officer are making a decision about the acceptability of residual risk based on incomplete information and providing an authorization to operate for a system that otherwise might not be authorized if all the information were available."</p>	Moderate
<div>NotResp</div>	Moderate
<p>The ARS specifies the time period for reviewing system audit records and the records are not reviewed as required by the ARS. The risk of not having a well defined audit review process and regular audit reviews is that, even if malicious activity is captured in the audit data, it will not be detected. When audit records are not reviewed there is a risk of not detecting a compromise in security."</p>	Low
<div>NotResp</div>	Low

NotResp	Low
<p>There is currently no means to review accounts at the time this SCA is occurring. There is correspondence with the EISG over this matter, and the mechanism will not be fully implemented until September.</p> <p>The risk of not having a review mechanism in place for accounts is that user accountability is not fully exercised. This impacts account maintenance and monitoring."</p>	Low
NotResp	Low
	Low
	Low
	Low
	Low

<div>NotResp</div>	Low
	Low
	Low
	Low

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING



Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Health Insurance Exchange (HIX) Information Security (IS) Risk Assessment (RA)

IS RA Date: August 15, 2013
IS RA Version Number: 1.6

IS RA Template May 7, 2009 Version 3.1

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

TABLE OF CONTENTS

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

NotResp

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

NotResp

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING
Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

IS RA Template May 7, 2009– Version 3.1

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Page 10

NotResp

NotResp

NotResp

NotResp

NotResp

NotResp

NotResp

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

NotResp

NotResp

NotResp

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

NotResp

NotResp

NotResp

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

NotResp

NotResp

NotResp

NotResp

NotResp

NotResp

NotResp

NotResp

NotResp

NotResp

NotResp

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

NotResp

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

NotResp

NotResp

NotResp

NotResp

NotResp

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

NotResp

NotResp

NotResp

NotResp

NotResp

NotResp

NotResp

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

NotResp

NotResp

NotResp

NotResp

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING
Health Insurance Exchange (HIX) August 15, 2013 – Version 1.6

NotResp

NotResp

NotResp

NotResp

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Health Insurance Exchange (HIX)

August 15, 2013 – Version 1.6

NotResp

NotResp

NotResp

End of Document