The Office of the National Coordinator for Health Information Technology

Health IT Advisory Committee

Trusted Exchange Framework Task Force
Key Provisions within Part B, Sections 6, 9, & 10

Arien Malec, Co-Chair
Denise Webb, Co-Chair

March 5, 2018

Privacy Requirements: Individual Access

- **6.1.1 Individual Access:** Each Qualified HIN agrees and acknowledges that individuals have a right to access, share and receive their available ePHI in accordance with the HIPAA Rules, section 4006(b) of the 21st Century Cures Act, and the terms and conditions of the Common Agreement. Each Qualified HIN agrees and acknowledges that individuals have a right to direct a HIPAA Covered Entity to transmit a copy of ePHI in a designated record set to any third parties designated by the individual in accordance with Applicable Law. Similarly, each Qualified HIN agrees and acknowledges that individuals have a right to direct a Participant or End User to transmit a copy of EHI to any third parties designated by the individual in accordance with Applicable Law.

Privacy Requirements: Consent

- **6.1.6 Consent:** If and to the extent that Applicable Law requires that an individual's consent to the Use or Disclosure of his or her EHI, the Participant of a Qualified HIN (or the End User of such a Participant) that has a direct relationship with the individual shall be responsible for obtaining and maintaining the consent of the individual (each a "Qualified HIN's Consenting Individual") consistent with the applicable requirements. Each Qualified HIN shall specify such responsibility in its Participant Agreements. Each Qualified HIN shall require its Participants to provide the Qualified HIN with a copy of each consent of a Qualified HIN's consenting individual and the Qualified HIN shall maintain copies of such consents and make them available electronically to any other Qualified HIN upon request.
- **6.1.7 Revocation of Consent:** Consistent with Applicable Law, each Qualified HIN agrees to maintain policies and procedures to allow an individual to withdraw or revoke his or her permission for the Use and Disclosure of the individual's EHI as obtained under Section 6.1.6 on a prospective basis.

Privacy Requirements: Breach Notification

- **6.1.3 Breach Notification:** When acting as a Business Associate, the Qualified HIN shall comply with all applicable Breach notification requirements regarding ePHI pursuant to 45 CFR §164.410 of the HIPAA Rules. Following discovery of a Breach of ePHI or EHI, the Qualified HIN further shall notify, in writing, the RCE without unreasonable delay, but no later than fifteen (15) calendar days, after Discovery of the Breach in order to allow other affected parties to satisfy their reporting obligations. Upon receipt of such notice, the RCE shall be responsible for notifying, in writing, other Qualified HINs affected by the Breach within seven (7) calendar days.

- **6.1.5 Law Enforcement Exception to Breach Notification:** If a Qualified HIN is notified, in writing, by any law enforcement official, that a Breach notification would impede a criminal investigation or cause damage to national security, then the Qualified HIN shall delay the Breach notification for the time period specified by the law enforcement official in accordance with the requirements of 45 C.F.R. §164.412 and 45 C.F.R. §164.528(a)(2).

Minimum Security Requirements

- **6.2. Minimum Security Requirements:** To ensure the confidentiality, integrity, and availability of ePHI and consistent with the Security Rule, each Qualified HIN (a Business Associate under the HIPAA Rules) shall be required to implement the following minimum security requirements described below within twelve (12) months from the date the TEFCA is published in the Federal Register, unless otherwise specified below. As a Business Associate, each Qualified HIN acknowledges that it is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making Uses and Disclosures of ePHI that are not authorized by its contract or required by Applicable Law. Each Qualified HIN further acknowledges that a Business Associate is directly liable and subject to civil penalties for failing to safeguard ePHI in accordance with the HIPAA Security Rule.

Security Requirements: Identity Proofing

- **6.2.4 Identity Proofing: Each** Qualified HIN's security policy shall include the following elements to ensure appropriate identity proofing:
  - (i) End Users/Participants. Each Qualified HIN shall identity proof Participants and participating End Users at a minimum of IAL2 prior to issuance of credentials; and
  - (ii) Individuals. Each Qualified HIN shall identity proof individuals at a minimum of IAL2 prior to issuance of credentials; provided, however, that the Qualified HIN may supplement identity information by allowing Participant staff to act as trusted referees. Participant staff also may act as authoritative sources by using knowledge of the identity of the individuals (*e.g.*, physical comparison to legal photographic identification cards such as driver's licenses or passports, or employee or school identification badges) collected during an antecedent in-person registration event. All personally identifiable information collected by the Participant staff or Qualified HIN shall be limited to the minimum necessary to resolve a unique identity.

Security Requirements: Authentication

- **6.2.5 Authentication.**
  - (i) Individuals. Each Qualified HIN shall authenticate individuals at a minimum of AAL2, and provide support for at least FAL2 or, alternatively, FAL3.
  - (ii) End Users/Participants. Each Qualified HIN shall authenticate End Users and Participants at a minimum of AAL2, and provide support for at least FAL2 or, alternatively, FAL3.
  - (iii) For FHIR API-based transactions the SMART App Authorization Guide for the use of OAUTH 2.0.
  - (iv) For FHIR API-based transactions that require End User authentication, the identity data scopes of the SMART App Authorization Guide for the use of OpenID Connect 2.0.

Security Requirements: Credential Management

- **6.2.6 Credential Management:** Each Qualified HIN's security policy shall include the following elements to ensure appropriate credential management:
  - (i) Each Qualified HIN's issuer certificate authorities and registration authorities shall protect repository information not intended for public dissemination or modification. Each Qualified HIN issuer certificate authorities shall provide unrestricted read access to the Qualified HIN's repositories for legitimate uses and shall implement logical and physical access controls to prevent unauthorized write access to such repositories.

Security Requirements: Transport Security

- **6.2.7 Transport Security:** Each Qualified HIN's security policy shall include the following elements to ensure appropriate data transport security:
  - (i) Authentication Server Requirements.
    - (a) SOAP-based Security. Each Qualified HIN's SOAP-based servers shall conform to the connection authentication requirements as specified in the IHE ATNA Integration Profile for Transport Authentication Security. Each Qualified HIN using local authentication or federated authentication for SOAP-based requests shall convey the locally-authenticated user attributes and authorizations using SAML 2.0 assertions as detailed in the IHE XUA Profile.
    - (b) At a minimum, Qualified HINS shall employ the following ciphers to mitigate the risk of EHI being exposed during transport in order to eliminate all readable EHI that is not encrypted:
      - Null cipher where encryption is not necessary, but must be configured for the system to work;
      - Substitution cipher as a minimum cryptographic technique to render EHI unreadable; and
      - Transposition ciphers or other more advanced cipher techniques to render unsecured EHI information unusable, unreadable or indecipherable to unauthorized individuals.
    - (c) Each Qualified HIN shall ensure that message exchanges are secured using TLS/SSL 1.2 X.509 v3 certificates for authentication, and X.509 certificates are used for authentication of all transactions.
    - (d) FHIR APIs. Each Qualified HIN shall require Participants to conform to the recommendations described in both the Security Considerations sections of RFC 6749 and in the OAuth 2.0 Threat Model and Security Considerations sections of RFC 6819.

Security Requirements: Transport Security, cont'd

- (ii) Authentication Server Requirements for Third Party Application Access. Each Qualified HIN's security policy that supports third party application access shall implement the following requirements within three (3) months from the date that the Qualified HIN executes an agreement with the RCE; provided, that if the Qualified HIN has not currently implemented FHIR, then the Qualified HIN shall implement the following requirements within twelve (12) months from the date that the Qualified HIN executes an agreement with the RCE:
  - (a) Each Qualified HIN shall support the OAuth 2.0 Dynamic Client Registration Protocol for Individual registration as defined in RFC 7591; and
  - (b) Each Qualified HIN shall authenticate third party applications to the authorization server's endpoint using a JSON Web Token (JWT) assertion signed by the third party application's private key as defined in RFC 7519.

Security Requirements: Transport Security, cont'd

- (iii) Authorization Server Requirements. Each Qualified HIN's security policy shall implement the following authorization server requirements within twelve (12) months of the API Implementation Guide being published as specified in Section 2.4 above:
  - (a) Each Qualified HIN's authorization server shall compare a Participant's registered redirect universal record indicators with the redirect universal record indicators presented during an authorization request using an exact string match to avoid spoofing;
  - (b) Each Qualified HIN shall ensure that its authorization servers maintain access tokens to single use for a short lifetime of less than ten (10) minutes;
  - (c) Each Qualified HIN shall ensure that its authorization servers use refresh tokens for long term access to the user information endpoint or other similar protected resources; and
  - (d) Each Qualified HIN shall ensure that its authorization servers shall provide a mechanism for the End User to revoke access tokens and refresh tokens granted to a Participant or individual.

Security Requirements: Certificate Policies

- **6.2.8 Certificate Policies:** Each Qualified HIN's security policy shall include the following elements to ensure that all Participant SSL certificates meet or exceed the following criteria:
  - (i) Key Sizes:
    - The certificate authority shall utilize the SHA-256 algorithm for certificate signatures; and
    - All keys shall be at least 2048 bit.
  - (ii) Certificate Authority:
    - The certificate authority's certificate shall be issued by a mutually trusted certificate authority; and
    - The certificate authority's certification shall not be self-signed.

Participant Obligations

- **9.1.3 Privacy.** Each Participant agrees to comply with all applicable federal and state laws and regulations relating the privacy of health information.

- **9.1.4 Identity Proofing.** Each Participant shall identity proof participating End Users and individuals in accordance with the following requirements:
  - (i) End Users. Each Participant shall identity proof participating End Users at Identity Assurance Level 2 (IAL2) prior to issuance of access credentials; and
  - (ii) Individuals. Each Participant shall identity proof individuals at Identity Assurance Level 2 (IAL2) prior to issuance of access credentials; provided, however, that the Participant may supplement identity information by allowing its staff to act as trusted referees and authoritative sources by using personal knowledge of the identity of the individuals (e.g., physical comparison to legal photographic identification cards such as driver's licenses or passports, or employee or school identification badges) collected during an antecedent in-person registration event. All collected personally identifiable information collected by the Participant shall be limited to the minimum necessary to resolve a unique identity and the Participant shall not copy and retain such personally identifiable information.

- **9.1.5 Authentication**. Each Participant shall authenticate participating End Users and individuals in accordance with the following requirements:
  - (i) Individuals. Each Participant shall authenticate participating individuals at AAL2, and provide support for at least FAL2 or, alternatively, FAL3.
  - (ii) End Users. Each Participant shall authenticate End Users at AAL2, and provide support for at least FAL2 or, alternatively, FAL3.

- **9.1.6 Security Incident and Breach Notification Requirements**. Each Participant who is a Covered Entity or Business Associate shall comply with all applicable Breach notification requirements pursuant to 45 CFR §164.402 of the HIPAA Rules. Each Participant further shall notify, in writing, the Qualified HIN without unreasonable delay, but no later than fifteen (15) calendar days after Discovery of the Breach in order to allow other affected parties to satisfy their reporting obligations. Upon receipt of such notice, the Qualified HIN shall be responsible for notifying, in writing, other Participants affected by the Breach within seven (7) calendar days.

- **9.1.7 Security Technical Requirements.** Each Participant shall be responsible for complying with the technical security policy requirements relating to authentication, identity proofing and individual authorization described in Sections 6.2.3 to 6.2.5.

End User Obligations

- **10.1.3 Identity Proofing.** Prior to the issuance of access credentials by Participant, each End User shall be required to identify proof at Identity Assurance Level 2 (IAL2).
- **10.1.4 Authentication.** Prior to the issuance of access credentials by Participant, each End User shall be required to authenticate at AAL2, and provide support for at least FAL2 or, alternatively, FAL3.
- **10.1.5 Security Incident and Breach Notification Requirements.** Each End User who is a Covered Entity or Business Associate shall comply with all applicable Breach notification requirements pursuant to 45 CFR §164.402 of the HIPAA Rules. Each End User further shall notify, in writing, the Participant, if affected by the Breach, without unreasonable delay, but no later than fifteen (15) calendar days after discovery of the Breach in order to allow other affected parties to satisfy their reporting obligations.

The Office of the National Coordinator for Health Information Technology

Health IT Advisory Committee

Trusted Exchange Framework Task Force

@ONC_HealthIT @HHSONC HealthIT.gov