Health IT Standards Committee

A Public Advisory Body on Health Information Technology to the National Coordinator for Health IT

March 26, 2013

Farzad Mostashari, MD, ScM
National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Dr. Mostashari,

The HIT Standards Committee's (HITSC) Privacy and Security Workgroup prepared recommendations on the privacy and security criteria for EHR Modules. The recommendations below were presented to the HITSC on December 19, 2012 and accepted for transmittal to the National Coordinator.

For 2016 Edition EHR certification, each EHR Module presented for certification should be required to meet each privacy and security criterion in the minimal set using one of the following three paths:

- Demonstrate, through system documentation and certification testing, that the EHR Module includes functionality that fully conforms to the privacy and security certification criterion.
- Demonstrate, through system documentation sufficiently detailed to enable integration, that the EHR Module has implemented service interfaces that enable it to access external services necessary to conform to the privacy and security certification criterion.
- Demonstrate through documentation that the privacy and security certification criterion is inapplicable or would be technically infeasible for the EHR Module to meet.

Based on the 2014 Edition of EHR Certification Criteria, we recommend the following as the "minimal set" of security functionality that every EHR Module should be required to address via one of the defined paths:

- Authentication, access control, and authorization
- Auditable events and tamper resistance
- Audit report(s)
- Amendments
- Automatic log-off
- Emergency access
- Encryption of data at rest
- Integrity

Note that as new privacy and security certification criteria are adopted, this minimal set will need to be revisited. For example, the "optional" Accounting of Disclosures criterion will need to be evaluated as a potential addition to this minimal set once the final rules are issued.

In certifying modules that opt for paths 2 or 3 to meet specific security criteria, certifiers will need to make yes/no decisions based on the quality of documentation presented with the module. To facilitate this decision making, we recommend the ONC undertake the following:

1. To support certification via path 2, develop a standard identifying the minimal content that must be included in the documentation. To be clear, path 2 does not require that the interface itself conform to a technical standard, but rather that the documentation contain sufficient detailed information to enable integration with the required security services. For example,
    - Detailed specification of the interface and its uses (e.g., parameters expected, data structures returned, service protocol)
    - Named products with which Module can be integrated
    - Named standards implemented in the interface
2. To support certification via path 3, while minimizing regulatory burden, develop guidance on the documentation required to justify inapplicability or infeasibility
3. Adapt the Certified HIT Products List (CHPL) for EHR Modules to account for the 3 potential paths for meeting privacy and security criteria.

Sincerely yours,

/s/
Jonathan Perlin
Chair, Health IT Standards Committee

/s/
John Halamka
Vice Chair, Health IT Standards Committee