Department of Health & Human Services
Office of the National Coordinator for
Health Information Technology

Privacy and Security Tiger Team

Summary of Recommendations on Provider and Patient Identity Management

May 21, 2013

Deven McGraw, Center for Democracy & Technology (Co-Chair, Tiger Team)
Walter Suarez, Kaiser Permanente, (Co-Chair, Privacy & Security Working Group, HITSC)
Peter Tippett, Chief Medical Officer, Verizon
Elizabeth Franchi, Director, Veterans Health Administration Data Quality Program
Paul Uhrig, Chief Administrative, Legal & Privacy Officer, Surescripts

Providers (September 26, 2012)

1. Providers should continue to ID proof professional & staff per HIPAA.
2. By Meaningful Use Stage 3, ONC should move toward requiring multi-factor authentication (meeting NIST Level of Assurance (LOA) 3) for remote access to protected health information; entities can identify other access environments necessitating higher authentication levels.
3. ONC's work to implement these recommendations should continue to be informed by NSTIC and technology developments, and appropriately account for provider workflow needs while establishing a secure environment.

Patients (May 3, 2013)

- ONC should develop and disseminate best practices on patient ID management; such best practices should be easy for patients to use, leverage solutions in other sectors (like banking), provide protections commensurate with risk.
- Patients should be able to ID proof both in person and remotely (ideally)
- Authentication should be more than user name and password but not set the bar too high (“Level 2.5”).
- Solutions should evolve with technology and be informed by NSTIC developments.

HIT Standards Committee

Patient Identity Management

- Need to uniquely identify patients for various purposes
  - Query of patient data, linking data from multiple sources, authorize patient access to data, other
- Lack of reliable means to identify patients continues to be seen broadly as a significant challenge to care delivery, continuity of care, and health care quality
- Multiple efforts currently underway to adopt/use ‘voluntary’ patient identifiers within secure systems
- No formal recommendations developed yet
  - Important that regulations allow progress and innovation to occur in this arena

HIT Standards Committee

Provider Identity Management

- Per policy direction, the overall expectation is to follow NIST criteria for LOA using SP-800-63-2.
- EHR technology should be configurable to enable an organization to require different levels of authentication and identity proofing, based on role within organization
- For example
  - Physicians and other providers with full access and write/edit capabilities should have IDP to at least NIST Level 3
  - Non-clinical staff without write/edit capabilities might more appropriately have IDP to NIST Level 2

HIT Standards Committee

Provider Identity Management (cont.)

- NSTIC offers benefits for authenticating both consumers and providers
- For MU Stage 3, EHR certification can require EHRs to support 2-factor authentication and permit one of the factors to be a third-party solution, in anticipation of NSTIC credentials becoming available
- We also may see consumers presenting NSTIC credentials before NSTIC has been broadly adopted by providers
- Not sure that a fully operational NSTIC approach will be ready in time for MU stage 3

Roundtable Discussion

Deven McGraw
Walter Suarez
Peter Tippett
Elizabeth Franchi
Paul Uhrig