Key Considerations: HIPAA Security, Health IT, and the App Ecosystem

Steve Posnack, ONC
About ONC

• The Office of the National Coordinator for Health Information Technology
  o Sits within US Department of Health and Human Services

  o Created in 2004 under an Executive Order by President Bush

  o Codified in law in 2009 as part of the American Recovery and Reinvestment Act (“Recovery Act”)

  o Substantial new authority as a result of the 21st Century Cures Act (2016)
Title IV of the 21st Century Cures Act

- Sec. 4001. Assisting doctors and hospitals in improving quality of care for patients.
- Sec. 4002. Transparent reporting on usability, security, and functionality.
- Sec. 4003. Interoperability.
- Sec. 4004. Information blocking.
- Sec. 4005. Leveraging electronic health records to improve patient care.
- Sec. 4006. Empowering patients and improving patient access to their electronic health information.
Two Statutory Sections Implemented Together
45 CFR Part 170.4xx and Part 171.2xx

Conditions of Certification
• 170.401 Information blocking
• 170.402 Assurances
• 170.403 Communications
• 170.404 APIs (without special effort)
• 170.405 Real world testing
• 170.406 Attestations
• 170.40x EHR Reporting Program

Information Blocking Exceptions
• 171.201 Preventing harm
• 171.202 Promoting the privacy of electronic health information
• 171.203 Promoting the security of electronic health information
• 171.204 Recovering costs reasonably incurred
• 171.205 Responding to requests that are infeasible
• 171.206 Licensing of interoperability elements on reasonable and non-discriminatory terms
• 171.207 Maintaining and improving health IT performance
Information Blocking

- Applies to certified health IT developers, health information exchanges, health information networks, & health care providers
- Electronic health information is expected to be accessible, exchangeable, & useable unless an “interference” is required by law or covered by an exception(s)
- An action(s) covered by an exception(s) would not be subject to penalties or disincentives

Conditions of Certification

- Applies only to health IT developers
- Also include maintenance of certification requirements

Certification Criteria

- Specify the technical requirements that software products presented for certification need to meet.
Who’s covered?
Information Blocking vs HIPAA

(Actors)
• Developers of certified health IT
• Health information exchanges
• Health information networks
• Healthcare providers

(Covered Entities)
• Healthcare providers
• Health plans
• Healthcare clearinghouses

(Business Associates)
• All shapes and sizes

Points to consider:
• Likelihood that most info blocking actors will be a covered entity or business associate
• Healthcare provider is a term shared between the two regulatory structures
“[T]he National Coordinator shall convene appropriate public and private stakeholders to develop or support a trusted exchange framework for trust policies and practices and for a common agreement for exchange between health information networks. The common agreement may include—

“(I) a common method for authenticating trusted health information network participants;

“(II) a common set of rules for trusted exchange;

“(III) organizational and operational policies to enable the exchange of health information among networks, including minimum conditions for such exchange to occur; and

“(IV) a process for filing and adjudicating noncompliance with the terms of the common agreement.”

“[T]he National Coordinator shall publish on its public Internet website, and in the Federal register, the trusted exchange framework and common agreement developed or supported under paragraph B...”
• ONC Proposed Rule with respect to APIs
  o App registration
  o Secure connection
  o User authentication
  o App authorization

• TEFCA: minimum required terms and conditions (MRTCs) provisions that address:
  o data integrity
  o identity proofing
  o access control
  o user authentication
  o auditing
Ways to Engage

• Health IT Feedback
  o https://www.healthit.gov/healthit-feedback

• Interoperability Standards Advisory
  o https://www.healthit.gov/isa/

• Guide to Getting & Using Your Health Records
  o https://www.healthit.gov/how-to-get-your-health-record/

• Interoperability Proving Ground
  o https://www.healthit.gov/techlab/ipg/

• Certified Health IT Product List
  o https://chpl.healthit.gov/
Thanks & Questions