AIRA
AMERICAN IMMUNIZATION REGISTRY ASSOCIATION
Immunization Information Systems for a New Era

UPCOMING CONFIDENTIALITY GUIDANCE

AIRA Discovery Session
August 29, 2016
4pm Eastern

OVERVIEW

Brief background and context on Guidance Documents

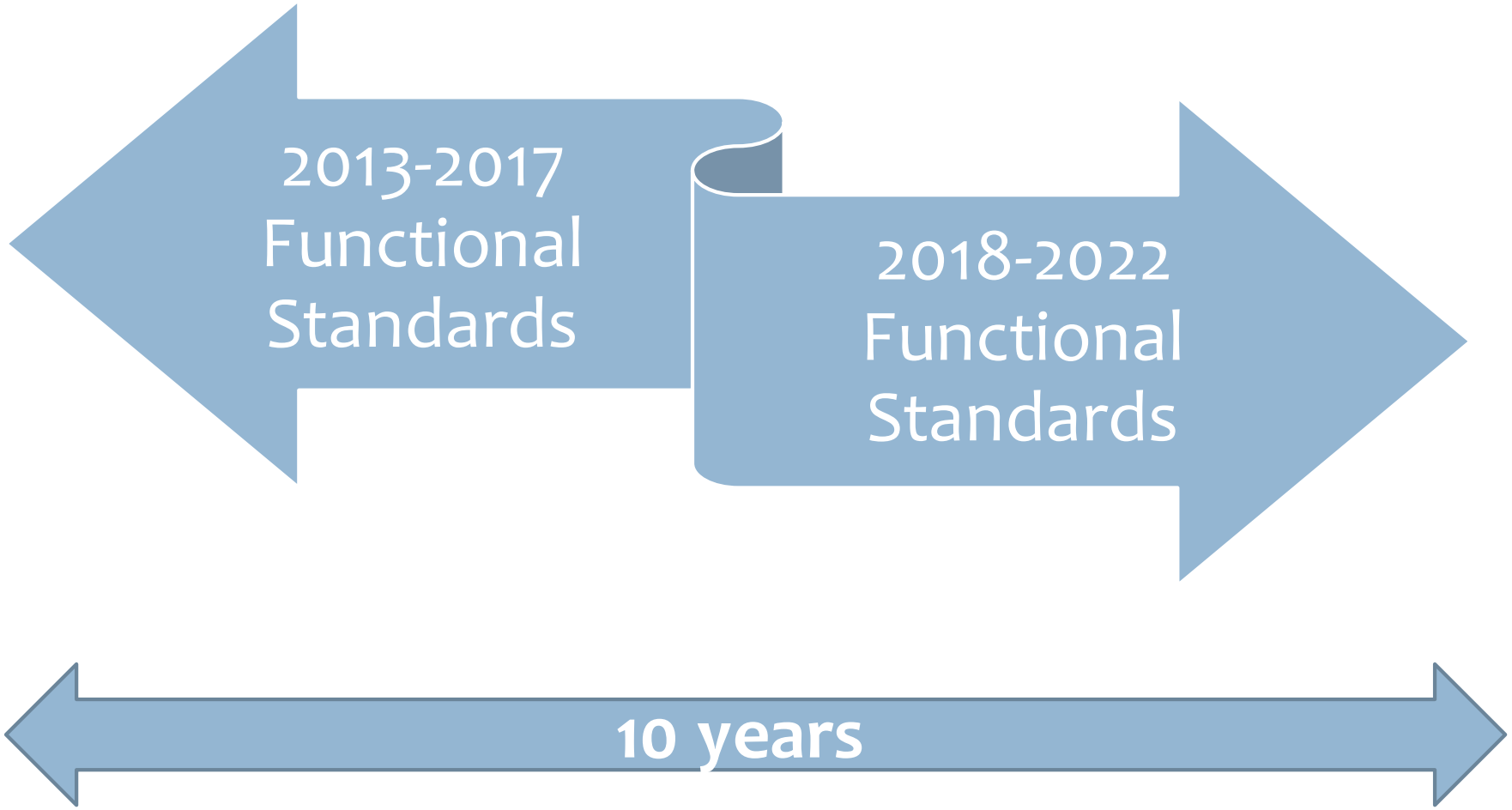
Confidentiality Guidance Document – Elaine Lowery

Upcoming Security Guidance Document – Nichole Lambrecht

Questions, Comments and Discussion

BACKGROUND AND CONTEXT

Last Published Guidance on Confidentiality: Community Registries Manual, 2000



Privacy and Confidentiality Considerations for Immunization Information Systems

Elaine Lowery, AIRA Public Health Consultant

AIRA Discovery Session

August 29th, 2016

4:00 – 5:00 pm EST

AIRA AMERICAN IMMUNIZATION REGISTRY ASSOCIATION

Immunization Information Systems for a New Era

Agenda

- Discuss Two Year Project Overview
- Review of Privacy and Confidentiality Considerations
- Review of Security Scope
- Timeline of Project

Project Overview

- AIRA developed project scope for privacy/confidentiality/security in 2015.
  - Divided up into two phases:
    - Privacy and Confidentiality
    - Security
- Goal for both phases is to develop considerations for IIS in each topic.

Phase I: Privacy and Confidentiality

Privacy and Confidentiality

- Privacy is the right of an individual to limit access by others to some aspect of the individual---such as information
- Confidentiality is the treatment of information that an individual has disclosed in a relationship of trust with the expectation that it will not be divulged to others in ways that are inconsistent with the understanding of the original disclosure

Privacy and Confidentiality: Overview

- Provide considerations for how IIS can meet requirements to protect the privacy of individuals and maintain the confidentiality of IIS information
- Overview of regulatory framework
  - Federal laws
    - Health Insurance Portability and Accountability Act of 1996 (HIPAA)
    - Family Educational Rights and Privacy Act (FERPA)
  - State laws
- Confidentiality policies and procedures

Privacy and Confidentiality: Disclosure TO an IIS--HIPAA

- In general, covered entities may not use or disclose protected health information unless authorized by the individual or pursuant to an exception
- In general, health care providers are covered entities
- Disclosure TO an IIS by a covered entity is, in general, exempt from HIPAA authorization as a disclosure to a public health authority

Privacy and Confidentiality: Disclosure TO an IIS----FERPA

- FERPA is a federal law that protects student education records
- FERPA (and not HIPAA) governs disclosure of school education records
- In general, personally identifiable information contained in an education record (including immunization information) cannot be disclosed without written consent of the parents or an eligible student

Privacy and Confidentiality: Disclosure FROM an IIS--HIPAA

- IIS may or may not be a covered entity under HIPAA---about half of IIS are covered entities
- If HIPAA applies, examples of HIPPA exceptions:
  - Disclosures for treatment and operations do not require authorization
  - Disclosure for research does not require authorization but has some restrictions
  - Disclosures to schools (HIPAA and not FERPA) applies) requires that the parent request the release (oral or written) and is limited to proof of immunization

Privacy and Confidentiality: State Laws

- State laws authorize and set parameters for operation of IIS and must always be examined for privacy and confidentiality considerations
- State laws
  - Specific to IIS
  - Specific to vaccination information
  - General laws relating to public health, medical information and privacy
- If state laws do not address a particular aspect of privacy and confidentiality HIPAA sets a floor

Privacy and Confidentiality Policies

- CDC IIS Programmatic Goal 4
  - IIS must "preserve the integrity, security, availability and privacy of all personally-identifiable health and demographic data in the IIS."
- CDC Functional Standard 4.1
  - IIS must have "written confidentiality and privacy practices and policies based on applicable law or regulation that protect all individuals whose data are contained in the system." http://www.cdc.gov/vaccines/programs/iis/func-stds.html

Privacy and Confidentiality Policies: General Provisions

- Written (electronic) form applicable to information in all formats available to anyone who asks for them, e.g., posted on IIS web site
- Reviewed regularly (for example, annually) by appropriate authority to ensure consistency with federal and state laws
- Applicable to everyone who has authorized use of information in the IIS: workforce, consultants, authorized users and contractors

Privacy and Confidentiality Policies: Applicable Law

- Citations to applicable laws
  - Determine if the IIS is subject to HIPAA
  - Identify state laws that authorize IIS
  - Identify other state laws that put parameters on IIS collection, use and disclosure of information
- These laws will guide development of the remainder of the Confidentiality Policy

Privacy and Confidentiality Policies: Authority to Collect Information

- Authority to collect/report information to the IIS
  - By age group
  - By types of individuals/entity
  - Voluntary or mandated reporting---by age group and type of individual/entity
  - Purpose of data collection

Checklist for authority to collect information:

- Examine state laws and regulations to determine authority to operate the IIS for each age group included in the IIS.
- Examine state laws and regulations to determine the purpose for collection of the information in the IIS, by age group included in the IIS.
- Develop IIS policies based on applicable state laws including:
  - reference to the citation for the authorizing statute and any implementing regulations
  - statement of the purposes for which the data can be collected

Privacy and Confidentiality Policies: Notice of Inclusion in IIS

- Examine state law to determine notice requirements, if any
  - Vary by age group
  - Who must give notice
  - Contents
  - Timing
- If IIS is governed by HIPAA, a notice of privacy practices is required
  - Specific requirements under HIPAA
  - Could be combined with notice of inclusion in IIS or separate---consult local authorities

Privacy and Confidentiality Policies: Consent

- HIPAA does not require consent (authorization) to disclose information to an IIS
- State laws will control if they are more restrictive than HIPAA
- Examine state laws for consent requirements
- Types of laws to examine
  - IIS authorizing law
  - Specific laws for data sources (e.g., vital records)
  - Scope of practice laws (e.g., pharmacists)

Privacy and Confidentiality Policies: Consent (Cont.)

- Determine the type of consent for each age group, if required
  - No consent required (and no notice required)
  - Implicit consent, with out -out allowed
  - Implicit consent, with no opt -out allowed
  - Explicit consent (oral or written)
- If consent required, can it be withdrawn?
- Documentation
  - Who maintains---IIS, provider, both?
  - Format---written, electronic, both?

Privacy and Confidentiality Policies: Consent (Cont.)

- Determine effect of opt-out/withdrawal
  - Responsibility to inform all reporting entities---individual/parent, IIS, both
  - Information in the IIS
    - Limit access
      - IIS only
      - IIS and reporting entity
    - Purge

Privacy and Confidentiality Policies: Use/Disclosure by IIS

- Examine state laws for permitted purposes for use/disclosure of IIS information
  - Type of individual/entity
    - Health care providers
    - Schools
    - Public health
    - Researchers
  - Purposes---treatment, school entry, surveillance, public health interventions
- If HIPAA applies, examine each use/disclosure for HIPAA requirements

Privacy and Confidentiality Policies: Data Retention and Disposal

- Examine state laws
- What must be retained
- Time to retain
- If the IIS is governed by HIPP, there is a general six-year retention period

Privacy and Confidentiality Policies: Rights of Individuals

- Examine state laws
  - Right to access
  - Right to inspect
  - Right to amend
- Methods
  - Directly through IIS or portal
  - Through health care provider, public health
- If IIS is governed by HIPAA, examine HIPPA to determine if state law, HIPAA or both apply

Privacy and Confidentiality Policies: Breach Notification

- Examine state laws to determine if it contains breach notification requirements
- If the IIS is governed by HIPAA, notice must be given to:
  - Affected individuals
  - The Secretary of Health and Human Services
  - Media (in some cases)
  - To the covered entity if breach is at a business associate

Privacy and Confidentiality Policies: Sanctions

- Examine state laws for civil and/or criminal sanctions for unauthorized use/disclosure of IIS information
- Workplace sanctions
- IIS sanctions (e.g., no access to IIS)
- If the IIS is governed by HIPAA, there are penalties provided

Privacy and Confidentiality: Site and User Agreements

- IIS ensure confidentiality by requiring that each individual who accesses IIS information agrees to abide by the IIS confidentiality policy and applicable state and federal laws
- Methods to ensure compliance:
  - User agreement with each individual user
  - Site agreement with an entity
    - The entity requires anyone it gives access to comply with the IIS confidentiality policy and applicable state and federal laws

Privacy and Confidentiality: Agreements

- User agreement
  - Pros:
    - IIS control over authentication (passwords)
    - State law may require user agreement
  - Cons:
    - Burdensome for the IIS
    - Less feasible with electronic submissions
- Site agreement
  - Pro:
    - More feasible with electronic submissions
  - Con:
    - IIS must rely on signing authority to enforce confidentiality at the individual level

Privacy and Confidentiality: Site Agreement

- Considerations for provisions in a site agreement
  - Reviewed regularly by appropriate authority (e.g., annually, but automatic renewal)
  - The site could agree to:
    - enforce the IIS confidentiality policies and state and federal laws and require employees to sign agreement
    - issue passwords to individuals and enforce prohibitions on sharing passwords
    - inform the IIS if any authorized IIS user becomes ineligible to be an IIS authorized user
    - impose sanctions including warnings and severing employment for repeated violations
    - keep an audit trail of all persons who access/use information received from the IIS

Privacy and Confidentiality: User Agreement

- Considerations for provision in a user agreement. The individual:
  - has read the IIS confidentiality policies
  - agrees to comply with the IIS confidentiality policies and federal and state law with respect to IIS information
  - will only access information that the individual has a need to know to perform her/his duties
  - will not share her/his IIS password with anyone
  - will notify the IIS immediately about any unauthorized use/disclosure of IIS information

Phase II: Security

Security Project Scope

- Written Security and Retention of Health Data Policies
  - Review of HIPAA Security Rule
  - Components of data security policies/protocols (administrative, physical, and technical safeguards; organizational standards; and policies and procedures)
  - Data disposal policies
- Hardware/Software Security (physical safeguards)
  - User access controls/auditing
  - Individual authentication of users and entities
  - Digital signature, two -factor authentication, and use of certificates
  - Physical security of hardware, data encryption, and disaster recovery
  - Protection of external electronic communications
- Discuss Implementation Considerations and Recommendations where applicable

Timeline

- Privacy and Confidentiality
  - Community review completed by 8/29
  - Document formal design by 10/10
- Security
  - Gather and Review Resources (including subject matter expert interviews) ~Oct – Jan
  - Develop draft document ~Jan – March
  - Draft available for community review ~April
  - Document formal design by end of June

Q & A

Contact

- Elaine Lowery
- AIRA Public Health Consultant
- Email: elaine.lowery@Comcast.net

- Nichole Lambrecht
- AIRA Sr. Project Manager
- Email: nlambrecht@immregistries.org