Connecting Healthcare®
Engaging Patients™

HIPAASuccess - Physician Education Series

Privacy and Security Intersections

Your Faculty:
Walt Culbertson

- President and Founder, Connecting Healthcare®
- Host and Producer, Medical Update Show
- Served as Technical and Operations Lead, HIE Project Manager Florida Health Information Exchange
- Served as the State of Florida - Technical SME for the ONC State Health Policy Consortium, Southeast Regional HIT-HIE Collaboration (SERCH)
- Founding Executive Director ePrescribe Florida and President, ePrescribe America
- Founding Chair of the Southern Healthcare Administrative Regional Process (SHARP), a regional collaborative workgroup alliance of private and public health care organizations and HHS, HRSA and CMS
- Founding Co-Chair of the CMS Sponsored Southern Insurance Commissioner Task Force, a regional collaborative workgroup alliance for State-level HIPAA Education
- Founding Security and Privacy Co-Chair for the Workgroup for Electronic Data Interchange (WEDi) Strategic National Implementation Process (SNIP)

Agenda

- HIPAA Privacy Versus Security
- Privacy and Security Intersections
- Security Issues with Privacy Intersections
- Privacy Issues with Security Intersections

Privacy Vs. Security

- *Privacy* is an individual's rights to control access and disclosure of their protected or individually identifiable healthcare information (IIHI)
- *Security* is an organization's responsibility to
  - control the means by which such information remains confidential
  - Ensure it is not altered, destroyed or lost

Security is a P.A.I.N.

P rivacy	is what you have to safeguard
A uthentication	identifying those sending & receiving information and accessing systems
I ntegrity	guaranteeing non-altered information
N on-Repudiation	being able to prove that the sender did in fact send the information

HIPAA Security

- HIPAA Security provides covered entities with a series of requirements to provide for the confidentiality, integrity and the availability of protected health care information:
  - Administrative Procedures
  - Physical Safeguards
  - Technical Security Services
  - Technical Security Mechanisms

HIPAA Privacy

- HIPAA Privacy establishes a series of requirements and patient rights to control access and disclosure of their protected healthcare information
  - Establish authorization requirements
  - Establish administration requirements
  - Establish individual rights
  - Establish regulations for use or disclosure of Protected Health Information (“PHI”)

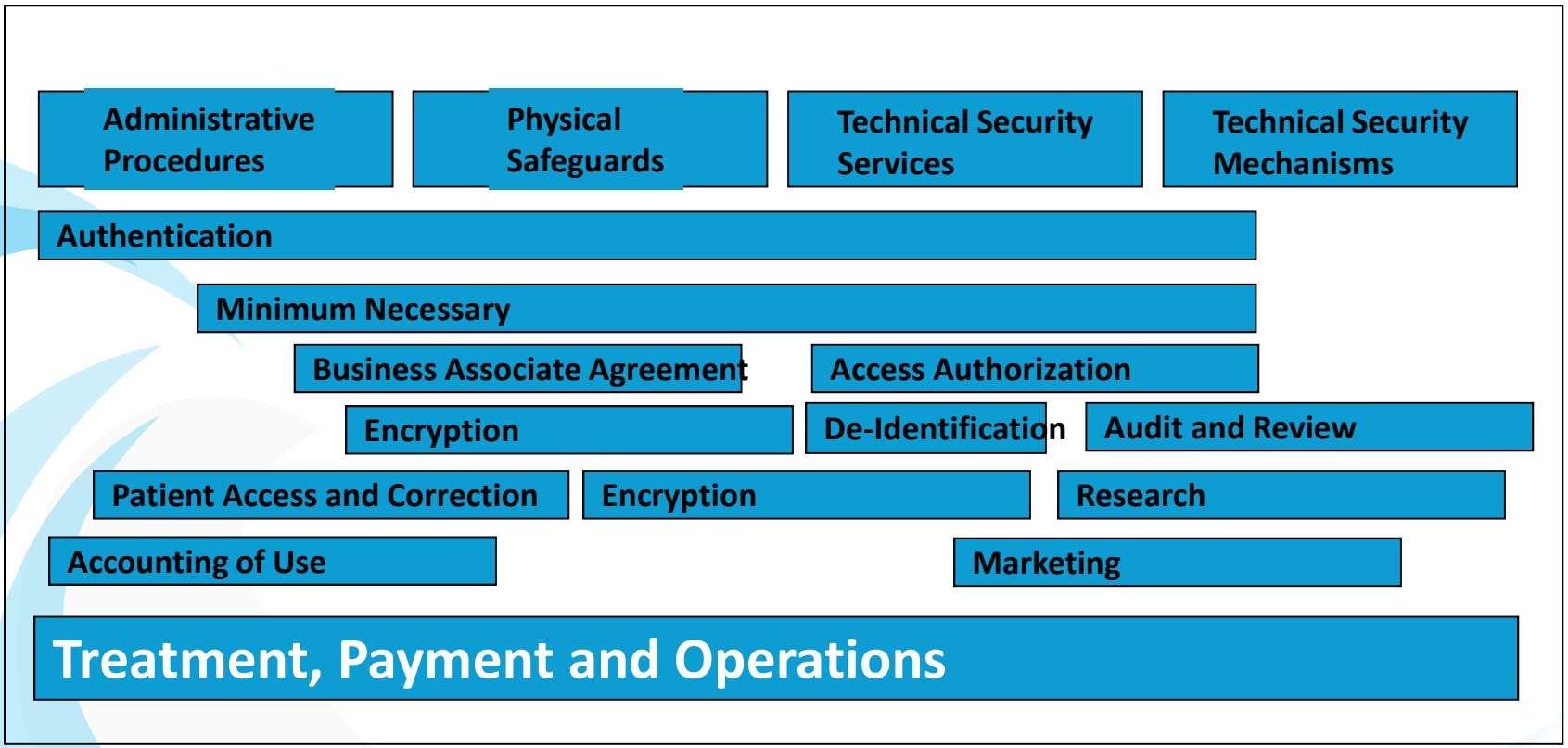
Relationship between Privacy and Security

- There is a direct relationship between privacy and security:
  - Security is the ‘how’... privacy is the ‘who’, ‘what’ and often the ‘why’
  - Security is the structure established to protect IIHI
  - One of the implementation barriers to privacy is the security infrastructure of the Covered Entity
  - Security awareness and education addresses ‘what’ is being protected

Privacy and Security Intersections

- Protected Health Information (PHI) versus Individually Identifiable Health Information (IIHI):
  - Two distinct areas of information
  - PHI is IIHI that is transmitted or stored in any form
  - IIHI is information that is created by or received from a covered entity that can be reasonably assumed to identify the individual

Intersection of Security and Privacy



Intersections - Required Safeguards

- While the proposed ***security*** regulations create a technology based verification system, the ***privacy*** regulations apply to oral statements and written documentation
  - Could result in duplication of electronic and written documentation
  - Not clear whether security standards will also be expanded to apply to oral and written communications (that compliance with the security standards will be considered as same for the privacy regulations)

Intersections - BAC Vs. Chain of Trust

- The privacy regulations definition of a Business Associate includes a wide range of entities:
  - Excludes individuals in the entity's workforce
  - Reaches far beyond electronic transactions
  - Specifies the content of the contracts
  - Covered entity must take action if it knows of a "pattern of activity or practice" by BA in violation of agreement
- Security regulations provide less detail on chain of trust agreement

Minimum Necessary Vs. Need to Know

- The Privacy regulations require covered entities to make reasonable efforts to use and disclose only the “minimum necessary” PHI to accomplish the stated purpose (excluding treatment)
- The Security regulations require “need-to-know” procedures which can be technologically implemented (role based access controls)

Security Issues with Privacy Intersections

Awareness Training and Education

- The Security NPRM only defines the “what” not the “how” the Privacy Rule defines both
- Building a sense of urgency but not panic – why organizations need to start NOW!
- Determining the hot buttons that will garner executive support and commitment
  - Financial return
  - Customer need
  - Differentiation
  - Cost factors

Organization Change Management

- HIPAA has broad and extensive implications across the entire enterprise
- Anticipate changing deep rooted organizational cultures & beliefs
- The key is a balance between the timely retrieval of health information and the maintenance of confidentiality and sensitivity

Organization Change Management

- Requirements affecting change:
  - Information Access Control
  - Security Incident Procedures
  - Security Awareness Training
  - Personnel Security
  - Security Management Process
  - Physical Access Controls
  - Policy/Guideline on workstation use

Audit Trail Clarification

- Identify and define audit trail issues
- Provide guidance relating to audit trails during Business Impact Analysis (BIA)
- Identify risks surrounding audit control issues
- Platform, environment, size may impact decisions
- Impacts on current operational process
- How often must audit trails be reviewed?
- Costs to implement required audit trails
- Hardware, Software, Personnel
- State law issues or best practices

Certification and Accreditation

- Certification/Accreditation provides an independent peer evaluation of the organization's HIPAA compliance, based upon a set of criteria
- Sets a common denominator in the methodology utilized to ensure compliance
- Provides a mechanism to ensure compliance that is both comprehensive and objective

Certification and Accreditation

- Aids in building HIPAA awareness within the organization
- Offers a methodology that utilizes industry “best practices”
- Identifies security and business risk exposures

Vendor Interdependencies

- Make global recommendations about Legacy Systems
  - Low level and value added solutions specific to Services and Mechanisms
- Providers and Plans should assess vendor awareness of HIPAA compliance as it relates to Information Technology Goals
- A health care entity's decisions about the depth and breadth of its BIA can be influenced by:
  - Physical Factors/ Size
  - Business Factors/ Acceptable Level of Risk

Privacy Issues with Security Intersections

Preemption

- Issues will exist over preemption floor/ceiling
- Since HIPAA does not preempt all state laws, then HIPAA ***is not*** the only law of the land
- HIPAA preempts all contrary state laws, except where state laws are “more stringent” than HIPAA
- Explore industry standards. Assess how HIPAA will interplay with state requirements, focus on procedural issues for privacy and security policies and procedures

Electronic Vs. Paper

- Policy and procedural issue
- Since the final rule ended up covering paper, Suggest covering “both sides of the house”
- “Protected health info” made more clear in final rule
- Data equals: demographic, health and clinical
- Protected and unprotected information
- Consider establishing categories of information regardless of source medium which need protection

Minimum Necessary

- Incumbent upon those disclosing on an individual basis
- Unique patient identifier could offer some solution
- Question; Define difference between minimum necessary and need to know. Need to review S&P requirements in more detail
- “Necessary data” could be issue for Change/ Management

Minimum Necessary

- Need to develop guidelines, recommendations
- Concern of cost of process and potential quality of care considerations, accountability of disclosure
- Two terms separated; use and disclosure
- Determine which of the disclosures and then the minimum data elements and finally, record what is disclosed

Notice Vs. Patient Consent

- From a provider perspective, consent to treat needs to be obtained initially and any time invasive procedures completed
- Three types of consent:
  - Institutional
  - State consent
  - Treatment consent

Addendum and Amendment

- It is illegal to change what has been written in a medical record, language in final rule needs to be more clear
- Cannot change what was written initially. Issue which may be different for providers vs. covered business entities. As a provider the record “stands as it is”
- An addendum/amendment is the only acceptable forum, not a strike out or change to medical record. Consider SOP and state law regarding this issue. Patient has a right to say “no”

Privacy - Addendum and Amendment

- Two types of information contained in the medical record; clinical vs. demographic
  - If demographic info is part of the medical record, it can not be changed
- Goal of this language is to allow the patient to have the right to make the amendment
  - Similar to credit history verification and amendment procedures

De-identify and Re-identify

- 18 data elements in the preliminary rule which are fairly common, #19 equals anything else!
- Depends upon the setting how it is used
- When data elements appear on screens (specific labels) / if content appears in free text field, then difficult to determine if that free text field contains those elements/ technology issues
- Key Security fields to be protected and monitored
- MANY factors will affect this classification

Connecting Healthcare®
Engaging Patients™
Communicate Educate Motivate™

Have Questions?

Visit our Website,
send us an email,
or give us a call!

(904) 435-3456
(904) 435-3457
Questions@
ConnectingHealthcare.com