Connecting Healthcare®
Engaging Patients™

HIPAASuccess - Physician Education Series

Privacy Implementation

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)

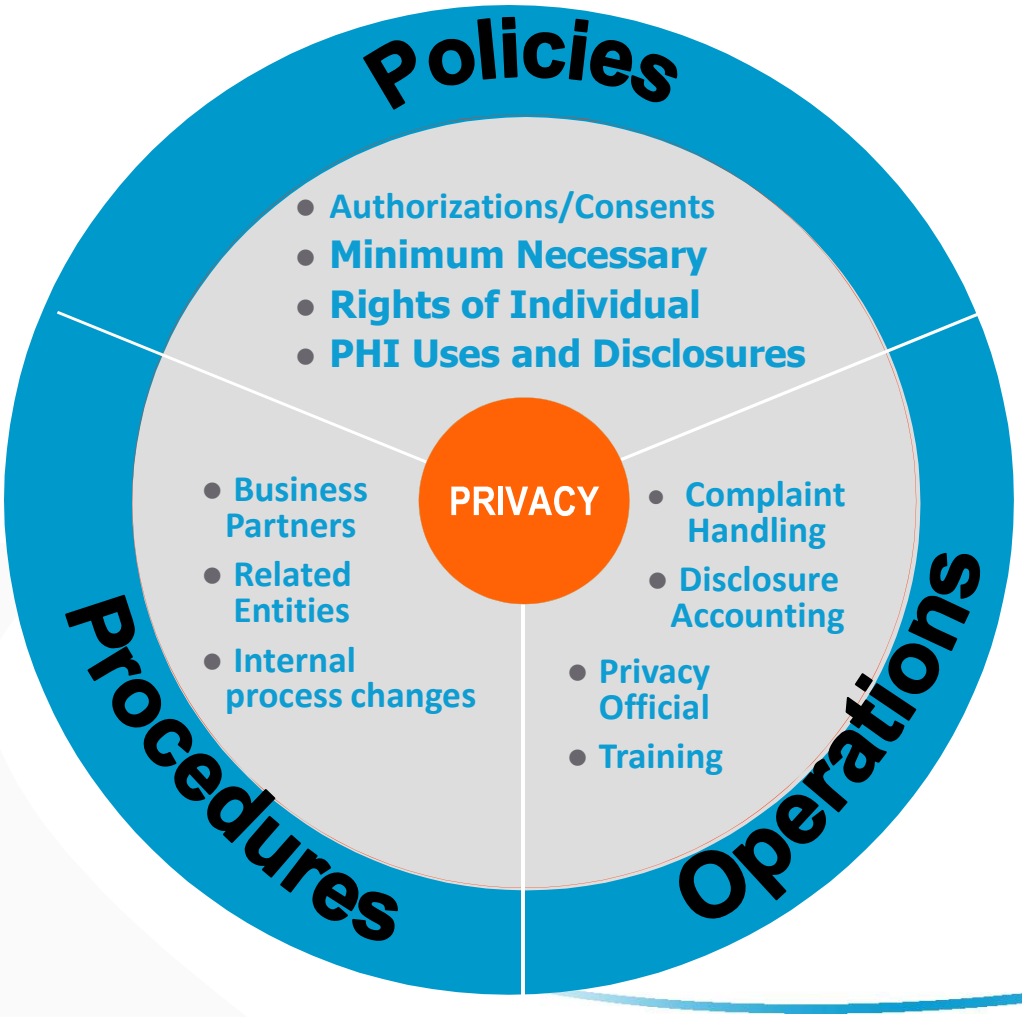
Agenda

- Privacy Rule Considerations
- Privacy Impacts
- Meeting Privacy Compliance
- De-Identification Impacts on Privacy
- Business Associate Agreements

Privacy Considerations

- Use of health information offers opportunities to improve healthcare and reduce overall costs
- Efficiencies can occur when health information is used as a source for developing health policy, trends, and relationships of cost to outcomes
- Aggregation of data is needed and requires the sharing of information from various data sources.
- This sharing of information needs to be done responsibly to maintain the privacy of individuals

Privacy Requirements



Privacy Impacts

- Increased complexity of administrative operations
- Privacy program infrastructure
- Formal systems for health information authorization
- “Minimum necessary disclosure” determination process
- Business associate contractual requirements, compliance monitoring
- New privacy policies and procedures
- User training and awareness

Privacy Impacts

- Increased accountability to patients and members
- Right to access, inspection, copying, amendments
- Culture change toward protecting patient information
- Increased regulatory and legal risks
- Compliance with complex federal standards
- Legal exposure for inadvertent disclosures

Increased Complexity of Operations

- Privacy program infrastructure
- Formal systems for health information authorization
- “Minimum necessary disclosure” determination process
- Business partner contractual requirements, compliance monitoring
- New privacy policies and procedures
- User training and awareness

Privacy Policies and Procedures

- Authorization forms
- Business associate contracts
- Individual's right to inspect, copy and request restrictions of disclosures
- Individual's right to request amendment
- Minimum Necessary
- Protected Health Information
- Privacy notice
- Tracking disclosures

Privacy Policies and Procedures

- Administrative requirements
- Awareness training for staff
- Complaint and grievance process
- Sanctions and mitigation for violations
- Revisions necessitated by changes in law
- Research activities
- *Documentation required for policies and procedures*

Privacy Policies and Procedures

- Uses and disclosures
  - Consistent with privacy notice
  - Subject to agreed upon restriction
  - De-identified information
  - Business associates
  - Deceased individuals
  - Personal representatives

Privacy Policies and Procedures

- Uses and disclosures
  - By whistleblowers, workforce, crime victims
  - Requiring opportunity for individual to agree or object
  - Marketing, fundraising
  - Underwriting and related purposes
  - Required by law
  - Permitted under Privacy rule

Meeting Privacy Compliance

Why Perform an Assessment?

- HIPAA is an enterprise-wide issue that will impact each organization differently
- Establishing budget levels and effectively understanding future capital and resource needs requires a base-line level of analysis
- There is no magic formula to reach these conclusions
- You need to evaluate your unique environment
- An assessment positions your organization to make informed decisions about how you will address HIPAA

Strategic Assessment

- Consider a Strategic Assessment component of the HIPAA Assessment engagement
- Focused on identifying and evaluating the impacts of HIPAA on your organization's strategic direction and applicable business strategies

Strategic Assessment

- Tools and techniques utilized in the assessment process:
  - Review of all corporate mission, vision, and strategy documents
  - Review of business plans, marketing strategies, and E-Business strategies
  - Evaluation of technology strategies and organizational structure
  - Interview key stakeholders in your organization
  - Consider opportunities to leverage changes related to HIPAA compliance to improve competitive positioning
  - Evaluate external and industry trends

Privacy Gap Analysis Overview

- Organizational structure
  - Corporate activities
  - Business unit activities
- Existing HIPAA data use, storage, and disclosure
- Existing policy and procedure documentation
  - Corporate
  - Business unit
- Business partner contracting

Privacy Assessment & Gap Analysis

General Provisions

	Responsibility	Procedures	Operations	Gap	Risk	Solution
Privacy Official	✍	○	○	There is a privacy official	none	
Document retention	✍	○	○	The privacy official is responsible for maintaining documentation	low	
Training and Certification	✍	◒	◒	Training is inadequate, and there is no formal certification program	high	New employee orientation training program, and current employee continuing education must be modified to include Privacy. Security training/education should be incorprated into compliance training program.
Sanctions	✍	○	○	P&P define sanctions. HR administers	low	
Complaint management	✍	●	◒	Although operationally complaints are handled by the Privacy official, this is not documented in the policies and procedures	low	Current operations should be memorialized in policy
Duty to mitigate		●	●	Although there is nothing in place regarding mitigation, this will normally be handled ad hoc.	low	Amend P&P to acknowledge duty and assign responsibility. This is not a high exposure or high risk concern.
Notification of Privacy Practices	✍					
Content of notice		○	◒	Notice is in compliance, except for contact phone # (see above)	low	Amend notice
Delivery of Notice		○	◒	Policies and procedures c/w 164.512, but in practice notification is spotty	high	Privacy official needs to monitor notification

Privacy Assessment & Gap Analysis

Patient Rights

	Responsibility	Procedures	Operations	Gap	Risk	Solution
Access (view/copy)	✍	○	◒	Patients are provided access to billing records, EOB's etc. Policies and procedures need updating to reflect this	low	Revise P&Ps
Request correction/amendment	✍	◒	◒	Pt accounting has a formal mechanism for investigation pt complaint. Need to add allowance for attaching explanation when request denied	low	Create mechanism for attaching explanation when request denied
Request restriction on use	✍	◒	●	There is no mechanism by which a patient can request restriciton on use	low	Create a general policy precluding special restrictions, with head of Pt accounting reviewing each request for special circumstances
Authorization management	✍	◒	◒	Currently, only a signature by pt is required for release of paper record.	high	Develop photo-ID authentication for paper record access, trusted 3rd party authentication (PKI?) for electronic access
Authorization Control	✍	◒	◒	Documentation is mailed to address of record.	low	Require signature for release of information

Strategy Setting and Plan Development

- Review the preliminary action plans developed throughout the project to evaluate alternatives and identify recommended solutions with consideration given to:
  - e-Business strategy and it's impact on connectivity channels
  - Business unit initiatives
  - Business process impacts and opportunity leverage points
  - Cost magnitude and expected return
  - Solution project plans

Privacy Success Factors

- Enterprise-wide planning
- Align HIPAA initiatives with corporate strategy(s) and integrate into operations
- Secure management support and awareness
- Leverage historic and on-going initiatives and accumulated knowledge (E-Business, Business Transformation, etc..)
- Establish a “do it once and right” position by building HIPAA into existing change initiatives

Privacy Success Factors

- Establish clear governance structure to manage complexities and interdependencies among business units and the technology, security and privacy requirements of HIPAA
- Ensure on-going communication channels for HIPAA specific initiatives
- Raise corporate awareness of HIPAA and its potential impacts on the origination and its stakeholders
- Incorporate HIPAA into existing compliance program

De-Identification Impacts on Privacy

Best Privacy Policy - De-Identify

- The Privacy Rule permits the free transfer of health data that has been “de-identified”
- De-identification requires removing, coding, encrypting, or otherwise eliminating or concealing all individually identifiable information
- Organizations should create policies, procedures, and processes that utilize de-identified data as much as possible within their operations

Key Privacy Definitions

- Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information. [Ref: Section 164.501]
- Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable information.[Ref: Section 164.514]

De-Identification Determination Methods

- The HIPAA Privacy rule specifies two ways in which covered entities can demonstrate that they have met the standard for de-identifying individually identifiable health information:
  - Expert Determination
  - Safe Harbor

Expert Determination

- A person with appropriate knowledge and expertise:
  - Applies generally accepted statistical and scientific principles and methods for rendering information not individually identifiable
  - Makes a determination the risk is very small that the information could be used by itself or in combination with other available information by the anticipated recipients
  - Document the analysis and results in making determination

Safe Harbor Determination

- The Second method a covered entity can use to demonstrate they are meeting the standard is with the Safe Harbor method:
  - Remove all of a list of enumerated identifiers, and
  - Have no actual knowledge that the remaining information could be used, alone or in combination with other information, to identify a subject of the information

Allowable under Safe Harbor

- Allowable information using the Safe Harbor method includes:
  - Age with dates limited to the year
  - Ages 90 and over must be aggregated to 90+
  - Initial 3 digits of zip codes if geographic area covered exceeds 20,000 people
  - Gender, race, ethnicity, marital status

Allowable under Safe Harbor

- Covered entities may mark records with code or similar means to allow later re-identification if code not derived from or related to information about the subject & not otherwise capable of being translated to identify the individual
- Code is not used for any other purpose.
- Covered entity may not disclose the mechanism for re-identification

Elements Not Allowed Under Safe Harbor

- Information that must be removed (relating to the individual, relatives, employers or household members of the individual):
  - Names
  - All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip codes if the geographic unit of combing all the same three initial digits contains more than 20,000 people.
  - If zip covers geographic area < 20,000 then first three digits must be changed to 000

Elements Not Allowed Under Safe Harbor

- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers

Elements Not Allowed Under Safe Harbor

- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)

Elements Not Allowed Under Safe Harbor

- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code
- Costs and Resources

Business Associate Agreements

Privacy and Business Associates

- Privacy, in the context of HIPAA addresses the rights of an individual regarding his or her individually identifiable health information; how to exercise those rights; the responsibilities of organizations to support an individual's rights; and the use and disclosure of that information
- See Section 164.504(e) of the proposed privacy rules covering business partner agreements and contracts for more details

Who is a Business Associate?

- A Business Associate is a person to whom the covered entity discloses PHI so that the person can carry out, assist with the performance of, or perform a function or activity for the covered entity.
- This would include contractors or others who receive PHI from the covered entity including lawyers, auditors, consultants, third-party administrators, healthcare clearinghouses, data processing firms, billing firms, and other covered entities.
- This would NOT include members of the covered entity's work force.

Determining Business Associate Impact

- A key question in sorting out HIPAA-related business associate issues is
  "Is there access to protected health information (PHI)?"
- If the answer is no, then you may not have issues.
- If yes, then you may need to review and amend existing contracts or create new contracts with these entities
- A covered entity must take action if it knows of a "pattern of activity or practice" by BA in violation of agreement (would be held responsible for violations by Business Associates)

What is a BAA?

- Business Associate Agreements are a requirement under the final privacy rule
- These agreements are required between covered entities and their business associates that receive (entities that provide access to) PHI
- Section 164.504(e) of the proposed privacy regulations would require covered entities to take specific steps to ensure that PHI disclosed to associates remains protected
- The intent is for these provisions to allow customary business relationships to continue while protecting the information shared in these relationships

Rules for Business Associates

- Business Associates would not be permitted to use or disclose PHI in ways that would not be permitted of the covered entity itself
- Other than for purposes of consultation or referral for treatment and other limited exceptions, covered entities are not allowed to disclose PHI to Business Associates
- The relationship would include a written contract that would limit the Business Associate's uses and disclosures of PHI to those permitted by the contract and would require assurances regarding security safeguards

Rules for Business Associates

- Covered entities cannot disclose PHI to BA's unless the two have entered into a written contract that meets HIPAA requirements
- Contacts must contain language that:
  - Prohibits the Business Associate from further using or disclosing the PHI for any purpose other than stated in the contract
  - Prohibits the Business Associate from further using or disclosing the PHI in a manner that would violate the requirements of the privacy rule if done by the covered entity

Rules for Business Associate Contracts

- Requires the Business Associate to maintain safeguards as necessary to ensure that the PHI is not used or disclosed except as provided by the contract. For example, if the Business Associate is a two-person firm, the contractual provisions regarding safeguards may focus on controlling physical access to a computer or file drawers, while a contract with a business partner with 500 employees would address use of electronic technologies to provide security of electronic and paper records

Rules for Business Associate Contracts

- Require the Business Associate to report to the covered entity any use or disclosure of the PHI not provided for in the contract
- Requires the Business Associate to ensure that any subcontractors or agents to whom it provides PHI received from the covered entity will agree to the same restrictions and conditions
- Specify that the Business Associate will make PHI available to assist the covered entities compliance with HIPAA patient rights provisions

Rules for Business Associate Contracts

- Requires the Business Associate to make available its internal practices, books, and records relating to the use and disclosure of PHI received from the covered entity to HHS or its agents
- Requires the Business Associate to incorporate any amendments or corrections to PHI when notified by the covered entity that the information is inaccurate or incomplete

Rules for Business Associate Contracts

- Upon termination of the contract Business Associate must return or destroy all PHI, if feasible
- Covered entity violates HIPAA if it knew of a pattern of activity or practice in violation of agreement and fails to take reasonable steps to cure, terminate the contract or report to DHHS

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