HIPAASuccess - Physician Education Series

Privacy Policies and Procedures

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

- Quick review of Privacy rule

- Areas requiring development of Privacy Policies and Procedures

- Getting Started

- Exercise: Developing Policies and Procedures to meet "Minimum necessary" requirements

Who Must Comply?

- Covered Entities defined under law
  - Health Plans
  - Clearinghouses
  - Providers who submit electronic transactions

- Business associates of covered entities
  - Indirectly covered through contracts with covered entities
  - Expected to comply with requirements specified for business associates

What is Protected?

Protected health information (PHI) includes all individually identifiable health information

- Held or transmitted by a covered entity in any form - electronic, paper or oral
- That relates to an individual's
  - Physical or mental health or condition
  - Provision of health care
  - Payment for health care

Use vs. Disclosure

Use is what you do with individually identifiable health information *within* your organization

Disclosure is what happens to individually identifiable health information when it goes *outside* your organization

Consent/Authorization

Consent requires written permission for uses and disclosures to carry out treatment, payment or health care operations

Authorization requires written permission for all uses and disclosures

- Other than treatment, payment, and health care operations
- Not otherwise permitted or required by the Privacy rule

Key Requirements of Privacy Rule

Covered entities must implement requirements related to:

– Use, disclosure, and request of only minimum necessary PHI

– Notice of privacy practices

– Consent form (providers)

– Authorization form

– Individual's right to inspect, copy and request amendment of health information (except clearinghouses)

– Accounting of disclosures to individuals

– Staff training in privacy practices

How to Meet These Requirements?

Develop *policies and procedures* that specify

– How your organization will implement the requirements of the Privacy Rule

– How you will monitor compliance on an on-going basis

Step one: Understand the Terminology

- Policy

  A general principle or plan that guides the actions taken by an individual or group

- Procedure

  A way of performing or accomplishing something; a series of steps or a course of action

Areas Requiring Policies & Procedures

- Minimum necessary
- Uses and disclosures of PHI
- Business associate contracts
- Complaint and grievance process
- Administrative requirements
- Awareness training for staff
- Sanctions and mitigations for violations

More Areas Requiring Policies & Procedures

- Notice of privacy practices
- Consent forms
- Authorization forms
- Revisions necessitated by changes in law
- Research activities
- Documentation creation and maintenance

More Areas Requiring Policies & Procedures

Protection of individual's rights to

- Inspect, copy and request amendment of medical records

- Request restriction on use/disclosure of PHI

- Confidential communication of PHI

- Accounting of disclosures of PHI

- Clearly written explanations of organization's privacy practices

How Do I Get Started?

Read the rule to find out what it requires for each area

– Use the "Find" option in Adobe Acrobat to search the document

– Search on the topic (e.g., minimum necessary), the section number, and the term "Policies and Procedures"

– Search both the rule and the preamble

Get Executive Buy-in

Compliance takes effort and time – must have support at executive level

– Critical that senior executives appreciate importance of compliance with Privacy rule

– Support at executive level will allow assignment of resources necessary to reach goals

– Need commitment of TIME from resources

  • Team leads and managers – development and staff training

  • Staff level - time to attend staff training and resources necessary to achieve compliance

Form a Workgroup

- Job is bigger than one person
- Need to enlist help of each unit's managers and team leads
  - Group will formulate the general, overall Privacy *policy* for organization
  - *Procedures* must come from the unit level – from the people who will live with them

Privacy Awareness Training Session

Start by explaining key concepts of Privacy Rule to entire staff – cannot skip this step!

- Terminology

- Requirements

- Importance to your organization

- Non-compliance penalties

- Include a general "HIPAA 101" and Security rule orientation if this hasn't been done previously

Policies/Procedures Workshop

Conduct a policy and procedures workshop with managers and team leads

- Provides a knowledge base of requirements for policies and procedures
- Gives managers and team leads a running start on development
- Allows sharing of ideas and enthusiasm
- Provides a model to follow for subsequent work

Review P&P with Team Leads

Review policies & procedures team leads develop to ensure they

– Meet requirements of Privacy rule

– Meet corporate goals and standards

– Are properly documented

– Have HR approval where necessary – add section to employee handbook especially as concerns sanctions for violations

Present P&P to Staff

Team leads and managers present policies and procedures to staff to

- Review Privacy rule requirements and promote high level of Privacy awareness
- Explain importance of compliance
- Explain in detail policies and procedures must follow
- Explain on-going compliance monitoring and sanctions for violations

Policies & Procedures: Minimum Necessary

General requirements of Privacy Rule regarding minimum necessary:

"When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request." §164.502(b)

Exceptions to Minimum Necessary

Situations in which minimum necessary requirement does NOT apply

- Disclosures or requests by a health care provider for treatment purposes
- Uses or disclosures made to the individual or authorized by the individual
- Uses or disclosures required by law - see §164.512(a)
- Uses or disclosures required to comply with the Privacy rule

Goals of Minimum Necessary P&P

Policies and procedures implementing the minimum necessary requirement must

1. Restrict access and use based on specific roles of members of your workforce
2. Establish criteria to limit routine disclosures to the minimum necessary to achieve the purpose of the disclosure
3. Limit requests for information to what is reasonably necessary for the particular use or disclosure

Uses by Your Workforce

We will develop policies and procedures regarding *use* of protected health information (PHI) by our own workforce that

– Identify the persons or group of persons who need access to PHI to carry out their job functions

– Identify type of PHI to which each person or group needs access and conditions under which need access

– Make reasonable efforts to limit access to only the information appropriate to their job requirements

![Connecting Healthcare® Engaging Patients™ logo]

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 🌐