It's Time to Finalize Your Privacy Policies

Save to myBoK

by Michelle Dougherty, RHIA

You've attended seminars, read articles, outlined systems, and developed forms for implementing the privacy rule, but there is still one step left--actually writing the policies and procedures. For many practitioners, policies and procedures are important but are often put off, then forgotten.

The HIPAA privacy rule places urgency on writing policies by requiring their development to document compliance with standards and implementation requirements. This article will define areas that need to be addressed in your organization's policies and procedures.

What Is Required?

When updating current policies and developing new ones, keep in mind the following privacy rule requirements for policies and procedures:

- The policies and procedures must **reflect** the organization's practices, standards, and implementation related to privacy and protected health information (PHI)
- They must be **reasonable** and reflect the size, scope, and activities of the organization
- When there is a change in the law, standard, practice, or implementation, they must be promptly **updated** and implemented
- If the change results in a revision to the notice of privacy practices, policies and procedures can be **revised** before the notice is updated, as long as the notice includes a statement that the covered entity reserves the right to make changes in privacy practices
- If there is no statement in the notice reserving the right to change privacy practices, policies and procedures cannot be revised or implemented until the new notice is in effect
- They can be **retained** in either written or electronic form
- All policies and procedures must be retained for **six years** from the date of creation or when it was last in effect, whichever is later
- When the privacy law requires **documentation** (i.e., an accounting of disclosures) or **communication** (i.e., denial of an amendment request), the covered entity must retain a copy in written or electronic form for six years

Cover All Areas

Not every standard of the privacy rule warrants a policy and procedure to show compliance. "Guidelines for Developing Polices," (below) provides a list of the standards that are best suited for a written policy and procedure. Determine whether to group related topics or develop policies on individual topics. This issue's HIPAA on the Job column, "Compliance in the Crosshairs: Targeting Your Training," provides additional information on policy and procedure development.

In certain areas, a policy or procedure isn't appropriate for documenting compliance. In some cases, plans and job descriptions should be developed instead. For example, a training plan and privacy officer job description will meet the need rather than a policy and procedure.

AHIMA has developed practice briefs on many of the policy and procedures listed above. These can help you get started with the documentation process as the April 14, 2003, privacy compliance date nears. Practice briefs are located at www.ahima.org under HIM Resources or in the FORE Library: HIM Body of Knowledge in the Communities of Practice at www.ahima.org.

Guidelines for Developing Policies

Policy Title and Regulation	Policy Content	Related Forms or Required Documentation/Communication
Privacy statement 164.502	• General statement that the organization will be in compliance with the HIPAA privacy rule, protect the confidentiality of PHI, and apply protections to how PHI is used and disclosed	
Authorization to disclose/release information 164.508	• When authorization will be needed • Verification of required content • Who can sign an authorization • Processing an authorization • Turnaround time	•Authorization
Access PHI/ medical record 164.524	• Right to access PHI • Request for access • Turnaround time • Copies • Charges • Denial process and documentation • Denial review process • Staff responsible	• Authorization or request form • Access denial • Extension notification
Disclosures and release of information (disclosures that generally do not require a consent or authorization) 164.502(f), (g) 164.512 164.514	• Who can act as personal representative • Verification before disclosure • Treatment (examples of disclosures related to treatment) • Continued treatment (transfer to another provider) • Payment (examples of disclosures related to payment) • Healthcare operations (examples of disclosures related to healthcare operations) • Use/disclosure by students • Research • Required by law • Public health, FDA, CDC, etc. • Abuse and vulnerable adult reporting • Health oversight (i.e., Department of Health) • Disclosures to law enforcement • Judicial and administrative proceedings • Handling subpoena (satisfactory assurance or qualified protective order) • Handling a court order/search warrant • Handling disclosure of deceased individual's information • Disclosures for special government functions • Disclosure to correctional institutions • Others outlined in the notice • Disclosures of de-identified information	
Marketing and fund raising 164.514	• Limitations for use of PHI for marketing and fund raising • When PHI can be used without an authorization for marketing • When an authorization is required for marketing • What information can be used for fund raising • Who can use PHI for fund raising • Opt-out notification and process	

Disclosing directory information 164.510(a)	• Obtaining permission to disclose directory information • What can be disclosed • To whom it can be disclosed • Handling calls to receptionist, front desk, nursing station, etc. • Directory boards • Room numbers	• Request for alternate communication
Requests for alternate communication 164.522(b)	• Submitting and processing a request • Type of requests to be honored • Fees charged (if applicable) • Individual/department who approves request	
Communication with family, relatives, or friends 164.510(b)	• Process to identify persons to whom staff members may disclose information (as identified by individual) • Disclosures when individual is present • Disclosures when individual is not present or not competent • Disclosures for disaster relief purposes	
Minimum necessary 164.502 164.514(d)	• Description • Criteria for disclosures • Criteria for requests • Staff access levels	
Notice and acknowledgment 164.520	• Right to receive notice • Distribution of notice • Acknowledgment of receipt • Review and updates • Notification of revisions • Posting notice • Making copies available	• Notice • Acknowledgment statement
Consent (if it will be used) 164.506	• Purpose of consent • Procedure for getting consent signed	
Amendment and correction to PHI/medical record 164.526	• Request for an amendment • Processing amendment request • Accepting amendment • Flagging the amended or corrected entry • Notifying others • Denying amendment • Statement of disagreement • Rebuttal • Future disclosures • Turnaround time	• Request for amendment or correction • Extension notification • Notification of decision (acceptance or denial)
Accounting of disclosures 164.528	• Individual's right to an accounting • Content of accounting • Maintaining a tracking system (integrating with other disclosure tracking systems if applicable) • Turnaround time	• Request for an accounting tracking system (paper or electronic) • Extension notification • Copy of accounting of disclosure information or log
Request restrictions to use/disclosure of PHI 164.522(a)	• Right to request • Process for handling request • Staff responsible for making decision • Notification of decision • Documentation and retention	• Request form • Denial form

Business associate (BA) contracts 164.502(e) 164.504(e)	• Responsibilities of BA • Monitoring compliance • Handling noncompliance • Terminating agreement • Return or destruction of PHI	• Sample BA contract or addendum
Designated record set 164.524, 164.526	• Definition of what is included in the designated record set	
De-identifying PHI 164.514	• Process of de-identifying	
Complaint process 164.530(d), (f), (g)	• Who handles a complaint • How a complaint is processed • Statement that organization will refrain from retaliatory acts if a complaint is filed	• Complaint form (if used)
Retention of records 164.530(j)	• Update current retention policies to reflect six-year time frame	
Safeguards (each topic could be a separate policy) 164.530(c)	Examples of policies related to safeguarding PHI: • faxing • e-mailing • viewing computer screens • password management • white boards • Web site privacy • access/security of HIM department • access/security of file rooms/cabinets where PHI is stored • chart locator procedures • confidentiality statements signed by work force	

Reference

"Standards for Privacy of Individually Identifiable Health Information; Final Rule." 45 CFR Parts 160 and 164. *Federal Register* 67, no. 157 (August 14, 2002). Available at www.hhs.gov/ocr/hipaa.

Michelle Dougherty *(michelle.dougherty@ahima.org) is an HIM practice manager at AHIMA.*

Article citation:
Dougherty, Michelle. "It's Time to Finalize Your Privacy Policies." *Journal of AHIMA* 73, no.10 (2002): 61-64.