HIPAA Privacy Checklist

Save to myBoK

This practice brief has been retired. It is made available for historical purposes only.

The standards for privacy of individually identifiable health information, also known as the final privacy rule, represent one portion of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This legislation became effective on April 14, 2001, with an April 14, 2003, compliance date. Small health plans are allowed an additional 12 months.

When the privacy rule was released in December 2000, it generated sufficient concern from affected groups and organizations that the secretary of the Department of Health and Human Services (HHS) reopened the legislation for a 30-day comment period. Following expiration of this comment period, HHS intends to review comments to determine whether changes to the rule are in order. If released, proposed changes are expected to necessitate an additional comment period in the form of notice of proposed rulemaking.

The HIPAA legislation itself provides the secretary of HHS with a one-year period from the effective date for modifications in the regulation. Even with potential changes in the rule, organizations are advised to proceed toward compliance, employing corrective measures should the changes require redirection.

Healthcare providers, health plans, and healthcare clearinghouses are considered "covered entities" under the privacy rule and are compelled to comply with this regulation, governing individually identifiable health information in electronic, paper, and oral form, also known as protected health information (PHI). The undertaking is clearly a multidisciplinary one. Where does an organization begin in coming into compliance with the privacy rule? The following checklist is intended as an aid in defining a manageable approach:

- Familiarize yourself with the privacy rule[1]
- Recognize that the privacy rule represents the initial phases of an industry progression toward standardized handling of individually identifiable health information. This process will be unfolding for a long time to come
- Champion the support of organizational leadership, the president/ CEO, and senior management in understanding and implementing this powerful rule
- Establish a privacy oversight committee as the decision-making body to lead the initiative.[2] Committee members should have positions or functions that make important contributions to HIPAA implementation, such as senior management, chief information officer, information security officer, privacy officer, HIM, information systems, risk management, human resources, quality management, and the medical staff
- Appoint the mandated privacy officer.[3] Place this individual in a leadership position or coordinating capacity on the privacy oversight committee
- Track the privacy rule, other state or federal privacy legislation, and applicable accreditation standards as an ongoing process, recognizing the obligation for simultaneous adaptation and compliance. Be aware of the potential for more stringent state laws to supercede HIPAA and a state's right to apply for HIPAA exemption for existing or new state laws when there is conflict or uncertainty of relative stringency
- Make use of networking opportunities and available resources: Web sites, publications, models, and listservs offering HIPAA guidance. The Office of Civil Rights has a privacy Web site where inquiries can be e-mailed

- Establish an overseeing body for research practices such as a privacy board or institutional review board (IRB).[4] This group serves to approve and oversee activities related to biomedical research involving and protecting human subjects

- Perform a risk assessment to compare current practices against HIPAA directives. Develop an action plan from identified and prioritized findings for progressing to compliance. Provide for future periodic risk analyses, as required, in coordination with other compliance and operational assessment functions

- Evaluate all information privacy policies and procedures in coordination with organization management, the privacy oversight committee, and legal counsel. Ensure inclusion of the entire organization where disclosure and release of information are handled (for example, physician offices, long-term care facilities, marketing departments, and so on). Include an evaluation of:

    - internal and external information access, disclosure, and release of information practices against the minimum necessary requirement

    - the need to update or develop privacy and confidentiality consents, authorization forms, and notice of information practices and materials reflecting current organization and legal practices and requirements

    - the existence of organizational policy for patient inspection, amendment, and access restriction of personal protected health information

    - practices related to marketing, facility directories, deidentification of health information, and access to psychotherapy notes

- Develop or update privacy training and orientation for all employees, volunteers, medical and professional staff, contractors, alliances, business associates, and other appropriate third parties

- Develop a mechanism for ongoing information privacy awareness reminders and updates within all organizational entities

- Review or initiate business associate agreements according to the HIPAA mandate. Ensure ongoing compliance monitoring of all business associate and chain of trust partner agreements to ensure that privacy issues are addressed and that business associates, subcontractors, and chain of trust partners are compliant with the privacy standards

- Establish a mechanism to track access to protected health information and allow qualified individuals to review or receive a report on such activity

- Establish a process for handling privacy complaints that ensures the tracking of all complaints from point of receipt through resolution with communication to the initiator. Be aware of consumer option to register complaints with the Office of Civil Rights for registering complaints

- Develop consistent sanction policies for failure to comply with privacy policies for all individuals in the organization's work force, extended work force, and for all business associates

- Recognize the overlap and coordinate privacy activities with security activities within the organization

- Establish positional responsibility for coordination of any investigation or survey activities initiated by the Office of Civil Rights, the HHS-appointed policing body for the privacy rule

- Consult legal counsel on facets of the rule that are unclear or difficult to understand

HIPAA Resources

The AHIMA Web site provides a number of new and recently updated HIPAA-related practice briefs, including patient anonymity, patient access and amendment to health records, consent for the use or disclosure of individually identifiable health information, laws and regulations governing the disclosure of health information, release of information for marketing or fund-raising purposes, notice of information practices, facsimile transmission of health information, and patient photography, videotaping, and other imaging. You can also subscribe to *In Confidence*, AHIMA's newsletter focusing on health information privacy, here. Go to https://secure.ahima.org/commerce2/index.inconfidence.html

The Computerized Patient Record Institute (CPRI) offers the CPRI Toolkit (free download), and security and education guidelines. Go to www.cpri-host.org.

The HHS Administrative Simplification Web site has the Health Insurance Portability and Accountability Act of 1996, the standards for privacy of individually identifiable health information proposed and final rules, and HIPAA REGS listserv at http://aspe.os.dhhs.gov/admnsimp/.

The HHS Office of Civil Rights, available at www.hhs.gov/ocr/hipaa, includes FAQs and an e-mail feature for inquiries.

The HHS Privacy Committee is available at http://aspe.os.dhhs.gov/ datacncl/privcmte.htm.

The National Center for Vital and Health Statistics (NCVHS) Web site is available at http://ncvhs.hhs.gov/.

The National Information Center for Health Sciences Administration is available at www.nichsa.org.

The Workgroup for Electronic Data Interchange, including the Strategic National Implementation Process, is available at www.wedi.org.

Apple, Gordon and Mary D. Brandt. "Ready, Set, Assess! An Action Plan for Conducting a HIPAA Privacy Risk Assessment." *Journal of AHIMA* 72, no. 6 (2001): 26-32.

Dennis, Jill Callahan. *Privacy and Confidentiality of Health Information.* San Francisco, CA: AHA Press/Jossey-Bass, 2000. A risk assessment protocol is included in the appendix.

Prepared by

Beth Hjort, RHIA, HIM practice manager

Acknowledgments

Gordon Apple, JD
Jill Callahan Dennis, JD, RHI
Gwen Hughes, RHIA
Harry Rhodes, MBA, RHIA
David Sobel, PhD

Notes

1. The final privacy rule is available in the December 28, 2000, Federal Register online at www.access.gpo.gov/su_docs/fedreg/a001228c.html. The rule can be downloaded for free using Adobe Acrobat Software, which is available free at the Government Printing Office Web site, www.access.gpo.gov/su_docs/aces/aces140.html. Copies of the Federal Register can also be purchased from the Superintendent of Documents. Each copy is $8; specify the date of the Federal Register and send a check or money order to New Orders, Superintendent of Documents, PO Box 371954,

Pittsburgh, PA 15250-7954. Copies can take up to 12 weeks for delivery. For credit card orders, call (202) 512-1800. Orders can be faxed to (202) 512-2250.

2. The privacy oversight committee is a recommendation of AHIMA and is not the same as the privacy board described in the HIPAA privacy regulation. A privacy oversight committee could include representation from the organization's senior administration in addition to departments and individuals who can lend an organization-wide perspective to privacy implementation and compliance.

3. Use AHIMA's sample privacy officer position description to aid the selection and recruitment process.

4. Not all organizations currently have an institutional review board (IRB) for oversight of research activities. If you work in a teaching hospital, most likely an IRB already exists. If not, one could be created in tandem with the Common Rule. Alternatively, this function could be administered by a privacy board consisting of members with professional qualifications appropriate to oversee research and related privacy practices. HIM professionals (for example, the privacy officer) should work with this group to ensure authorizations and awareness are established where needed or required.

References

AHIMA Policy and Government Relations Team's analysis of the final rule for standards for privacy of individually identifiable health information.

AHIMA's Sample (Chief) Privacy Officer Position Description.

Carpenter, Jennifer E. "Practice Brief: Information Security: A Checklist for Healthcare Professionals (Updated)." *Journal of AHIMA* 71, no. 1 (2000): 64A-64D.

Fleming, Laurel. "Research: One of HIPAA's Exceptions." *In Confidence* (forthcoming).

Hughes, Gwen "Getting Your Arms Around HIPAA." *Journal of AHIMA* 72, no. 4 (2001): 62-65.

"Standards for Privacy of Individually Identifiable Health Information; Final Rule." 45 CFR Parts 160 and 164. Federal Register 65, no. 250 (December 28, 2000). Available at http://aspe.hhs.gov/admnsimp/.

Article citation:
Hjort, Beth. "A HIPAA Privacy Checklist (AHIMA Practice Brief)." *Journal of AHIMA* 72, no.6 (2001): 64A-C.