Managing Information Privacy & Security in Healthcare

United States Laws Relating to Health Care Information Privacy/Security

By Barbara Demster, MS, RHIA, CHCQM, Edited by Margaret Marchak

While the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as amended by the American Recovery and Reinvestment Act of 2009 in the Health Information Technology for Economic and Clinical Health (HITECH) Act provisions, has taken center stage in the health privacy world in recent years, however, there are many other privacy laws. The number of laws that address the security and privacy of health care information is increasing, and that trend is expected to continue. The primary laws are briefly summarized below; however, it is important to remember that this is a dynamic area of the law. It is critical to update information, and work with experts in these laws. It is also important to remember that laws may exist on both federal and state levels, and that additional obligations may be found in voluntary standards or terms. The primary federal laws addressing the security of healthcare information and technology are as follows:

- Federal Trade Commission (FTC) implemented a Health Breach Notification Rule at 16 C.F.R. Part 318 to require vendors of personal health records (PHRs) and related entities and third-party service providers not covered under the HIPAA Security Rule to notify certain individuals when a security breach of health information occurs.
- Title III of the E-Government Act of 2002, entitled the Federal Information Security Management Act (FISMA)
- The Privacy Act of 1974 at <http://www.usdoj.gov/foia/privstat.htm>
- Family Educational Rights and Privacy Act (FERPA) at <http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- Financial Services Modernization Act of 1999 commonly called Gramm-Leach-Bliley Act (GLB) <http://library.ahima.org/xpedio/groups/public/documents/government/bok1_019068.hcsp>
- Federal Policy for the Protection of Human Subjects (Common Rule) <http://www.hhs.gov/ohrp/policy/#common>
- Confidentiality of Alcohol and Drug Abuse Patient Records <http://www.access.gpo.gov/nara/cfr/waisidx_00/42cfr2_00.html>
- Conditions of Participation (CoP) (42 CFR Part 418, 482, 484) <http://www.access.gpo.gov/nara/cfr/waisidx_02/42cfr418_02.html>
- Standards and Certification (42 CFR Part 483) <http://www.access.gpo.gov/nara/cfr/waisidx_00/42cfrv3_00.html >

- Clinical Laboratory Improvements Act (CLIA) (42 CFR Part 493) <http://www.access.gpo.gov/nara/cfr/waisidx_00/42cfrv3_00.html>

As a voluntary standard, the Payment Card Industry Data Security Standard (PCI DSS) requires certain protections for payment card data, which may affect health care organizations.

The following two part series of articles "Getting 'Hip' to Other Privacy Laws" provides an introduction to the major privacy statutes, rules, and regulations that co-exist with HIPAA to assist in building a compliant, confidential, and secure organizational information system.

"Getting 'Hip' to Other Privacy Laws" Part 1
<http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_022442.hcsp >

Part 2 introduces privacy provisions of regulations known more to their applicable niche (research, substance abuse, clinical laboratories, licensure and certification) rather than to the general industry.

Getting "Hip" to Other Privacy Laws Part 2
<http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_022552.hcsp>

Other statutes and regulations that have privacy related content and require mentioning include the following:

Occupational Safety & Health Administration (OSHA) regulations allow employee access to information on their exposure to toxic or hazardous substances and to their medical records.
<http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=STANDARDS&p_id=10027
>

The Sarbanes-Oxley (SOX) Act, enacted in 2002, applies to publicly traded companies that report to the Securities and Exchange Commission (SEC) and requires certain information security controls.

The USA Patriot Act passed in October 2001 followed shortly thereafter by the Homeland Security Act in 2002 created new challenges in the privacy field.

While a number of national privacy bills have been introduced in Congress over the last several years, no comprehensive legislation for health information privacy has been enacted. The text and legislative status of each bill is available at http://thomas.loc.gov (search for "medical privacy").

For more information and summaries of all bills related in any way to the general issue of privacy, consult the website of the Electronic Privacy Information Center (EPIC) at http://www.epic.org/privacy/bill_track.html.

There are also privacy initiatives going on outside the United States that impact how Americans conduct business across borders. A detailed discussion of the European Union Privacy Directive may be found elsewhere in the Toolkit.

Canadian privacy legislation along with their Privacy Commissioners and Oversight Agencies are included in the Toolkit as well.