



Managing Information Privacy & Security in Healthcare

United States Laws Relating to Privacy

By Barbara Demster, MS, RHIA, CHCQM

While the Health Insurance Portability and Accountability Act of 1996 (HIPAA) has taken center stage in the health privacy world in recent years, there are many other privacy laws that deal with information privacy. 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 and must be taken into consideration 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 1 of the series discusses and compares the content of:

- The Privacy Act of 1974 <http://www.usdoj.gov/foia/privstat.htm> >
- Family Educational Rights and Privacy Act (FERPA)
<http://www.ed.gov/policy/gen/guid/fpc/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 >

A table included in Part 1 compares nine attributes of the three laws:

1. Entities covered by the particular law.
2. Information protected by the law.
3. Persons protected by the law.
4. Notice requirements.
5. Disclosure requirements.
6. Account of Disclosure Requirements.
7. Amending Information.
8. Safeguarding Information.
9. Enforcement.

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 >

The regulations discussed in Part 2 are:

- 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>

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 USA Patriot Act passed in October 2001 followed shortly thereafter by the Homeland Security Act in 2002 created new challenges in the privacy field. These are discussed in [Section 7.6](#) in this chapter.

While a number of national privacy bills have been introduced in Congress over the last several years, no comprehensive legislation for medical 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 we do 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.

Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act)

The Financial Services Modernization Act of 1999 (commonly referred to as Gramm-Leach-Bliley, GLB or GLBA) applies to financial institutions such as banks, http://library.ahima.org/xpedio/groups/public/documents/government/bok1_019068.hcsp brokerage houses, and insurance companies. GLB requires these institutions to provide notice to an individual when the institution shares the individual's information with a third party. The individual must be provided the ability to opt out of the process. One of the loopholes in the law (from the individual's point of view) is that these financial institutions are allowed to share information among affiliated companies. For instance, should you pay your clinical specialist with a credit card, the information on that transaction may be shared with the bank's affiliated companies. The name of a specialist or specialty treatment facility may often provide the next best thing to a diagnosis. These institutions are required to send out notice of their privacy practices and provide the individual with information on how their information is used and what the individual may do to exercise some level of control over their information (if any).

US Patriot Act & Homeland Security Act

Six weeks after the terrorist attack on the World Trade Center in New York on September 11, 2001, the U.S. Congress passed the USA Patriot Act <http://personalinfomediary.com/USAPATRIOTACT.htm>. In giving the government remarkable powers in the fight on terrorism, the Act eroded many basic civil liberties. One provision of the Act is the ability to obtain medical records on demand in an intelligence investigation without judicial oversight. The Act remains controversial in the struggle to balance fighting terrorism and protecting civil liberties. In 2002, the Homeland Security Act was passed which also impacted the privacy of health information. The Act remains a subject of controversy. The AHIMA developed a Practice Brief: Homeland Security and HIM http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_023191.hcsp to provide guidance on how to respond to these new laws of the land. It also compares these two laws with HIPAA and provides suggestions for the workplace in complying with all.