

# HIPAA And Human Service Organizations

By Lorrie L. Lutz and Henry Yennie  
L<sup>3</sup> P Associates, LLC  
www.L3PAssociates.com

**HIPAA** (The Health Insurance Portability and Accountability Act) was passed with broad bi-partisan congressional support in 1996.

On April 12, 2001, Health and Human Services (HHS) Secretary Tommy G. Thompson announced that the effective date of the final privacy rule of the Health Insurance Portability and Accountability Act (HIPAA) will not be delayed. HIPAA's privacy rule became effective on April 14, 2001 as planned. **Covered entities have until April 2003 to implement the privacy rule provisions.**

"President Bush wants strong patient privacy protections put in place now. Therefore, we will immediately begin the process of implementing the patient privacy rule that will give patients greater access to their own medical records and more control over how their personal information is used," said Mr. Thompson. "This rule makes sure that private health information doesn't fall victim to the progress of the information and technology age, where an array of data is readily available in computer systems and too often just a keystroke away from being accessed. We are giving patients peace of mind in knowing that their medical records are indeed confidential and their privacy is not vulnerable to intrusion. "

## What Are the privacy Objectives?

- Define and limit the circumstances in which covered entities may use and disclose protected health information;
- Establish certain individual rights regarding protected health information;
- Require covered entities to adopt administrative safeguards to protect the confidentiality and privacy of protected health information.
- Penalties for noncompliance include civil fines up to \$25,000 per calendar year for each violation, and criminal penalties which increase in severity based on intent.

Janna Malamud Smith, *Private Matters: In Defense of the Personal Life* (1997) writes "The bottom line is clear. If we continually, gratuitously, reveal other people's privacies, we harm them and ourselves, we undermine the richness of the personal life, and we fuel a social atmosphere of mutual exploitation. Let me put it another way: Little in life is as precious as the freedom to say and do things with people you love that you would not say or do if someone else were present. And few experiences are as fundamental to liberty and autonomy as maintaining control over when, how, to whom, and where you disclose personal material."

Ellen Alderman and Caroline Kennedy describe the importance of privacy in this way: "Privacy covers many things. It protects the solitude necessary for creative thought. It allows us the independence that is part of raising a family. It protects our right to be secure in our own homes and possessions, assured that the government cannot come barging in. Privacy also encompasses our right to self-determination and to define who we are. Although we live in a world of noisy self-confession, privacy allows us to keep certain facts to ourselves if we so choose. The right to privacy, it seems, is what makes us civilized."

## **Are We Overreacting? Maybe Not!**

Until recently, health information was recorded and maintained on paper and stored in the offices of community-based physicians, nurses, hospitals, and other health care professionals and institutions. In some ways, this imperfect system of record keeping created a false sense of privacy among patients, providers, and others. Patients' health information has never remained completely confidential. Until recently, a breach of confidentiality involved a physical exchange of paper records or a verbal exchange of information.

Today, however, more and more health care providers, plans, and others are utilizing electronic means of storing and transmitting health information.

In 1996, the health care industry invested an estimated \$10 billion to \$15 billion on information technology. The electronic information revolution is transforming the recording of health information so that the disclosure of information may require only a push of a button. In a matter of seconds, a person's most profoundly private information can be shared with hundreds, thousands, even millions of individuals and organizations at a time.

This ease of information collection, organization, retention, and exchange made possible by the advances in computer and other electronic technology affords many benefits to individuals and to the health care industry.

- •Use of electronic information has helped to speed the delivery of effective care and the processing of billions of dollars worth of health care claims.
- •Greater use of electronic data has also increased our ability to identify and treat those who are at risk for disease, conduct vital research, detect fraud and abuse, and measure and improve the quality of care delivered in the U.S.
- •The National Research Council recently reported that "the Internet has great potential to improve Americans' health by enhancing communications and improving access to information for care providers, patients, health plan administrators, public health officials, biomedical researchers, and other health professionals."

Concerns about the lack of attention to information privacy in the health care industry are not merely theoretical. In the absence of a national legal framework of health privacy protections, consumers are increasingly vulnerable to the exposure of their personal health information.

Examples of recent privacy breaches include:

- A Michigan-based health system accidentally posted the medical records of thousands of patients on the Internet (The Ann Arbor News, February 10, 1999).
- A Utah-based pharmaceutical benefits management firm used patient data to solicit business for its owner, a drug store (Kiplingers, February 2000).
- An employee of the Tampa, Florida Health Department took a computer disk containing the names of 4,000 people who had tested positive for HIV, the virus that causes AIDS (USA Today, October 10, 1996).
- A patient in a Boston-area hospital discovered that her medical record had been read by more than 200 of the hospital's employees (The Boston Globe, August 1, 2000).
- In 1993, the Boston Globe reported that Johnson and Johnson marketed a list of 5 million names and addresses of elderly incontinent women. (ACLU Legislative Update, April 1998).

- • A few weeks after an Orlando woman had her doctor perform some routine tests, she received a letter from a drug company promoting a treatment for her high cholesterol. (Orlando Sentinel, November 30, 1997).

A breach of a person's health privacy can have significant implications well beyond the physical health of that person, including the loss of a job, alienation of family and friends, the loss of health insurance, and public humiliation.

For example:

- A banker who also sat on a county health board gained access to patients' records and identified several people with cancer and **called in their mortgages**. See the National Law Journal, May 30, 1994.
- A physician was diagnosed with AIDS at the hospital in which he practiced medicine. **His surgical privileges were suspended**. See *Estate of Behringer v. Medical Center at Princeton*, 249 N.J. Super. 597
- A candidate for Congress nearly **saw her campaign derailed** when newspapers published the fact that she had sought psychiatric treatment after a suicide attempt. See *New York Times*, October 10, 1992, Section 1, page 25.
- • A 30-year **FBI veteran was put on administrative leave** when, without his permission, his pharmacy released information about his treatment for depression. (Los Angeles Times, September 1, 1998)

### What Exactly Does HIPAA Entail?

At the time the legislation was enacted, most human service providers were focused on three important provisions of HIPAA:

- The legislation set into law the “portability” of pre-existing condition exemptions between employer group health plans. This feature was designed to broaden the parity of insurance coverage for Americans by preventing the common practice of denying coverage due to “pre-existing conditions.” This feature of HIPAA obtained the most press coverage at the time of passage because of broad public sentiment against the “pre-existing excuse”.
- The second major feature of HIPAA was a set of measures to implement stronger fraud and abuse protections in healthcare.
- The third major feature of HIPAA was summarized in the innocuous sounding phrase of “administrative simplification.” Because many in the field were focused, in large part by press coverage, on the two other provisions of the legislation, we didn’t fully appreciate the significance of that little phrase.

Today, that little phrase “**administrative simplification**” makes the other two provisions of the act pale in the significance when it comes to the impact on the health care system over the next two to four years. Because of this, many experts have characterized HIPAA as one of the most far-reaching pieces of health care legislation ever enacted.<sup>1</sup>

**The “administrative simplification” features of HIPAA are composed of two major parts:**

<sup>1</sup> DeMuro, P. and McAuley, L., “Health Insurance Portability and Accountability Act,” HFMA 10th Annual Conference on Managed Care, September 18, 2000.

- The first part is truly aimed toward simplification, and it outlines broad measures for the standardization of a variety of healthcare transactions. It is composed of the following:
  - Standardized health information transactions
  - Standardized code sets (e.g.. CPT, ICD-9, etc.)<sup>2</sup>
  - Single national identifiers (numbers) for providers, health plans/payers and employers. The legislation also included provisions for single national patient identifier, but Congress delayed the implementation of this feature due to its controversy.
- The second part of “administrative simplification” addresses security and privacy issues. It is this second part of administrative simplification that is the focus of much concern in the field.

Overall, the legislation covers health plans, health care clearinghouses, health care providers, and employers. The specific definitions of these entities are as follows:

- “Health Care Provider” includes those defined in relevant Medicare provisions as well as any other person or organization that furnishes, bills, or is paid for health care services or supplies in the normal course of business.
- “Health Plan” includes any individual or group plan that provides or pays the cost of medical care. We believe this includes behavioral health organizations acting as managed care organizations, and it may cover Employee Assistance Programs.
- “Clearinghouse” includes a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements.

For those still doubtful about their HIPAA “exposure,” let’s look at the specific definitions of the act. It specifically states that the definition of a “Health Care Provider” is:

- A provider of services as defined in section 1861(u) of the Act<sup>3</sup>, 42 U.S.C. 1395x(u),
- A provider of medical or other health services as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s), and
- Any other person or organization that furnishes, bills, or is paid for health care in the normal course of business.

**Among other things, “health care” is defined as follows:**

- Services or supplies furnished to an individual and related to the health of the individual. Health care includes the following:

---

<sup>2</sup> On a somewhat disturbing note, the final security and privacy regulations were released by HCFA on December 20, 2000, and there is not one reference to the DSM-IV code sets. The implications of this oversight are unclear at this point, and may, at the extreme, mean that behavioral health providers may not be able to use DSM codes as part of a “standard” transaction.

<sup>3</sup> The “Act” refers to the Social Security Act.

- ⇒ Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care; counseling; service; or procedure with respect to the physical or mental condition, or functional status, of an individual or affecting the structure or function of the body.

In addition, HIPAA covers any “Business Partner” of a covered entity. A “Business Partner” includes a person to whom the covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity.

- Examples include contractors or other persons who receive information for purposes noted above including lawyers, accountants, auditors, consultants, billing firms, or other entities.

Covered entities may not disclose protected health information to business partners without satisfactory assurances that the partner complies with relevant HIPAA standards.

Assuming that most human service organizations are covered we recommend completing Steps 1 – 3 in our compliance plan that is discussed below.

### ***How to Prepare For HIPAA***

---

**Step 1:** Educate yourself, and promote awareness and education among senior management and the Board of Directors. HIPAA should be considered a serious compliance initiative, and every effective compliance program begins with a formal commitment from the governing body.

Because this compliance will require resources in the form of funding and staff time, senior management must be forthright in its charge to the compliance effort. At the end of this article, we provide some web sites that offer downloadable presentation materials that can be used in organizations.

**Step 2:** Develop an organization project team for managing HIPAA compliance. Most organizations have some sort of compliance committee or team in place due to JCAHO, COA, CARF, or other accrediting and regulatory concerns. These groups can serve as a logical point to begin HIPAA compliance assessments and planning.

**Step 3:** Conduct an organization risk assessment. [*L<sup>3</sup> P Associates has developed an agency risk assessment*]. Because this can be a complicated and time-consuming task, we suggest the following approach:

- Examine current policies and procedures regarding information security and confidentiality. This should encompass both process security/confidentiality and technical security/confidentiality.
- Perform a “gap analysis” on this set of policies and procedures to identify where adaptation, modification, and additional policies and procedures are needed
- Set realistic, practical goals and objectives for developing and implementing compliance activities. Most organizations will, we believe, have some work to do in this area. A reasonable schedule backed by a detailed project plan will avoid “panic” once staff begins to realize the implications.
- The assessment should include a clear understanding of the resources needed to address each identified risk, as well as the potential impact on the organization of adapting and modifying existing procedures and adding new ones. Many of the procedural revisions will involve the

acquisition and deployment of resources. The team should be able to clearly quantify and explain the nature and extent of the resource need.

**Step 4:** Develop and implement policies and procedures to address identified risks. The most important point of this step is to “implement” the policies and procedure revisions and additions. There may be adjustments to the overall project plan in this phase due to the following:

- Staff will actually have to start learning and adapting to new practices.
- New regulations or interpretations of new regulations will occur as the deadline for compliance approaches.

**Step 5:** Develop and implement staff education and training. This type of staff training is specifically required by the legislation, and it is not a one-time event. Staff will need to be retrained when new technology and operational practices are developed and deployed. Organizations with high staff turnover will face the most cost and management burdens. **Additionally, staff will have to be re-certified at least once every three years.**

**Step 6:** Provide continual auditing and monitoring of compliance activities. This is related to the “deployment” of policies and procedures, and it goes beyond putting something on paper. In order to be judged compliant, an organization will have to document that it has followed those policies and procedures approved by senior management and the Board of Directors. This means training and tracking of actions.

### ***Specific Impacts on Human Service Providers***

---

We believe that human service organizations will face the most scrutiny from consumers. The reasons for this belief are:

- Compliance with the privacy requirements implies a technological capability that many organizations in the field do not currently have.
- The social service and behavioral health industry deals with some of the most sensitive client information in the healthcare field. Our consumer population is highly sensitive about the release of information, and this legislation gives consumers a powerful mechanism to demand an accounting of who has seen what information when and for what purpose.
- The nature of some of our consumer’s problems lend itself to suspicion and a need for verification. And the remedies for consumers who can demonstrate an organization’s non-compliance include both civil fines and criminal penalties.
- There are requirements limiting the disclosure of psychotherapy notes that we believe will cause serious concern once the privacy and security regulations are finalized.

Based on our understanding of the regulations and the potential cost impact to organizations, we believe there may be a positive cost/benefit to compliance. We have completed development of some initial cost models based on various organization sizes, and our conclusions are as follows:

- There is a potential cost/benefit of \$2: \$7. This can be interpreted as \$3.59 in benefits for every \$1 of cost incurred.

- The model is based on compliance modeling that involved the following costs for a **large human service organization (over \$30 million)**:

<b>COST ITEM DELTAS</b>	<b>YEAR 1</b>	<b>YEAR 2</b>	<b>YEAR 3</b>	<b>YEAR 4</b>	<b>YEAR 5</b>	<b>TOTAL</b>
Hardware Costs	31,901	402	1,526	402	402	34,632
Software Costs	117,223	5,200	5,200	5,200	5,200	138,022
Personnel Costs	229,735	79,124	44,669	44,669	44,669	442,866
Network & Communications Costs	147,917	69,826	69,826	69,826	69,826	427,220
Other IT Costs	213,733	99,528	99,528	99,528	99,528	611,844
Avoided Costs	0	0	0	0	0	0
<b>Totals</b>	<b>\$740,509</b>	<b>\$254,078</b>	<b>\$220,748</b>	<b>\$219,624</b>	<b>\$219,624</b>	<b>\$1,654,584</b>

The benefit items calculated included the following and totaled \$5.9 million over a five-year period:

Reduced Days in A/R
Additional fee collection
Reduce claim denials
Lower cost per bill
Reduce chart handling/costs
Reduce Staffing Requirements
Reduce documentation re-work
Increase clinical staff productivity

While there is certainly variation in these estimates, our simulation modeling demonstrated 90<sup>th</sup> percentile cost benefit value of \$1.34. We believe that, overall, an organization can experience a positive long-term benefit for organizations.

**For further information please contact:**

Lorrie L. Lutz at L<sup>3</sup> P Associates, LLC  
 24 North Spring Street  
 Concord, NH 03301  
 603-224-4687 or [Lorrie@L3Passociates.com](mailto:Lorrie@L3Passociates.com)