

September 2007

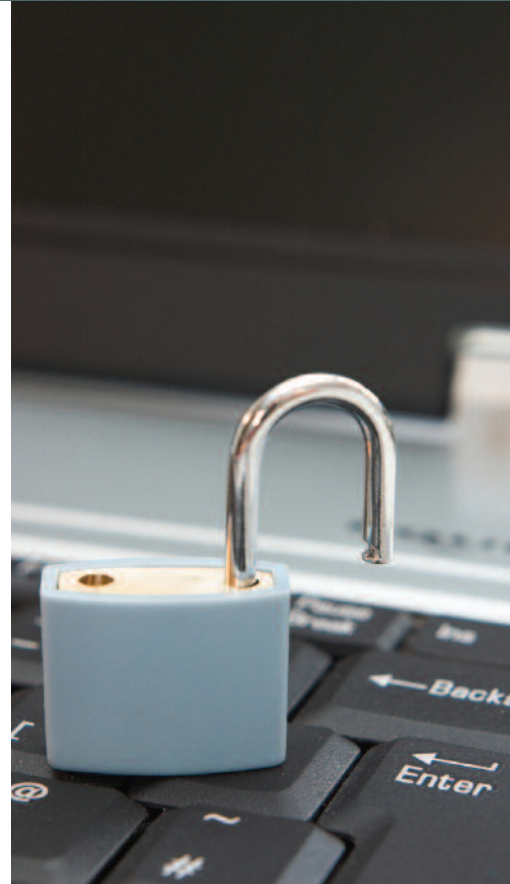
Managing Data Privacy Risks: Traditional Solutions and Beyond

As health plans, medical providers and hospitals utilize personal health records, electronic medical records and software programs to expedite claims processes, the need to protect personal data has created new business and liability risks. In addition, mounting pressure from both state and federal legislation such as the Health Information Portability and Accountability Act (HIPAA) governing the use and protection of personal data is driving the costs and risk of non-compliance beyond the cost of compliance.

The use of electronic medical records is by no means new, but the scope and cost of civil lawsuits resulting from third-party identity theft or disclosure of personal data are becoming difficult to predict and quantify. The cost of complying with consumer notification laws, meanwhile, is high. When non-financial personal information is leaked, notification costs run about \$15 per affected individual.¹ When financial information is involved, the cost of notification soars to about \$35 per person.² A breach affecting 50,000 persons, comparable in size to several recent data breaches, could cost a health care provider \$1.75 million for notification costs alone.³ Such events will certainly attract the attention of shareholders.

This much is certain: data disclosure and availability incidents can impact an organization's finances, operations and reputation.

The increase of frequency and potential cost associated with these types of incidents are forcing healthcare organizations and professionals to balance compliance concerns with risk mitigation and shareholder value concerns in a crisis atmosphere where information is limited and outcomes are unknown. This much is certain: data disclosure and availability incidents can impact an organization's finances, operations and reputation. Risk managers and executive decision makers must evaluate the adequacy of protection provided by traditional Property and Casualty insurance coverages, especially Commercial General Liability and Professional Liability policies, as part of the risk management process.



By Frank Castro
Senior Vice President
Willis Healthcare Practice
Managed Care Practice Leader

The Risks

Data breaches come from a variety of sources – people, technology and processes – and produce many exposures. They can be grouped into three categories.

Confidentiality

Unwanted data disclosure can lead to expenses related to notification, credit monitoring, ID theft insurance and other services for affected individuals, call centers, public relations and other crisis management activities. Disclosures can be caused by:

- Unauthorized access or unauthorized use (insider or outsider)
- Loss or theft of laptop/blackberry/portable media
- Administrative error (such as improper sharing of information, negligent release, HIPAA violations)
- Spyware, password theft, or social engineering
- Disclosure or release by contractor, vendor, physician or business partner

Availability

A cyber attack or other incident can interrupt access to electronic medical records, account information, or other important data and systems, causing operational delays, additional expenses, or worse. System outages can be caused by:

- Hacker/virus attack
- Distributed denial-of-service attack
- Software/hardware failure
- Administrative errors
- Disgruntled/former employee or contractor sabotage
- Physical perils (fire, windstorm, network service interruption)

Integrity

An attack or programming error can cause failure in the integrity of data, meaning that information cannot be retrieved or incorrect information may be used to make business or healthcare decisions. Integrity issues have been caused by events such as:

- Insider/outsider attack/sabotage
- Programming/administrative error
- Hardware or software failure
- Malicious code (virus or worm)

Legislation

HIPAA and Beyond



Congress responded to many of these issues by passing HIPAA in 1996 and then left to the Department of Health and Human Services the task of developing rules and regulations to address the finer points. To that end, the department issued two key rules: the Privacy Rule, a regulation under HIPAA that went into effect in April 2003, and the Security Rule, which became effective in 2005.⁴ The Privacy Rule establishes individual rights as well as a federal floor for privacy with respect to most

health information. It imposes restrictions on the use and disclosure of individually identifiable health information. The Security Rule sets safeguard standards for protected health information (PHI) in electronic form.⁵ PHI is broadly defined. It includes any individually identifiable health information relating to past, present or future physical or mental health conditions, treatments or payments for healthcare services. The mere fact that an individual received healthcare is protected by the regulations.⁶



The protections afforded by the Privacy Rule include the right to:

- Access, inspect and copy PHI maintained by covered entities, including hospitals, clinics and health plans, among others (subject to some limitations)
- Request that PHI maintained by covered entities be corrected
- Request disclosure of all releases of PHI made without authorization for any purpose other than treatment, payment and healthcare operations
- Receive a notice of privacy practices from doctors, hospitals, health plans and others in the healthcare system
- Preserve the confidentiality of PHI by having it communicated only to a designated address or telephone number
- Request restrictions on the use or disclosure of PHI (although such a request is not binding on the covered entity)
- Seek redress from the Secretary of Health and Human Resources in the event that PHI has been handled improperly⁷

The Privacy Rule permits covered entities, including health plans, healthcare clearing houses and healthcare providers⁸ to use PHI for limited purposes, including treatment, payment and healthcare operations.⁹ Other uses of PHI, such as for marketing, fund raising and research, are prohibited, unless the patient provides written authorization. Healthcare providers must ensure that vendors and business associates who receive PHI preserve its confidentiality.¹⁰ This becomes particularly important when data entry management functions are outsourced to domestic or overseas operations.

Healthcare providers are also granted discretion to make limited disclosures of PHI to family and friends, if, in the professional judgment of the provider, those disclosures are in the patient's best interests.¹¹ Confusion over this aspect of the Privacy Rule has given rise to many complaints, because many healthcare providers refuse to share PHI with anyone not specifically authorized by the patient. If the patient is not communicative, a refusal by healthcare practitioners to share information with those who know the patient may have adverse health

consequences. The potential litigation consequences of an outright refusal to share PHI are clear.

The civil and criminal consequences for an incident of non-compliance that results in an invasion of a patient's privacy can be severe, but generally require bad intent on the part of the disclosing party. Civil penalties are \$100 per violation with a cap of \$25,000 per person per year.¹² If the disclosure occurs in the context of an attempt to commercially exploit or maliciously harm the patient, criminal penalties of up to \$250,000 or 10 years imprisonment or both may be imposed.¹³



The Security Rule goes into much more detail about preventing improper disclosure of electronically stored PHI. The rule identifies three levels of safeguards.

- Administrative safeguards require risk analysis and management, assignment of security responsibilities, implementing policies and procedures, training employees and executing appropriate contractual safeguards with vendors and associates
- Physical safeguards include limiting access to facilities and workstations and adopting appropriate device and media protection
- Technical safeguards include access controls and audits, authentication and transmission security



Because substantial costs are associated with these safeguards, a rule of reason is applied by the Department of Health and Human Services. Some standards are mandatory but others may be avoided in appropriate circumstances. A covered entity must, however, document why it is not meeting a non-mandatory standard. The entity must also document identified threats to the confidentiality of PHI and steps taken to prevent disclosure. Obviously, this may be used against the entity in litigation.

Interplay of Federal Law

These rules are not the exclusive source of federal protection of PHI. The preamble to the Privacy Rule expressly lists a number of federal laws that also protect an individual's privacy, including the Privacy Act of 1974, the Gramm-Leach-Bliley Act, the US Safe Harbor Privacy Principles (European Union Directive on Data Protection) and the Employee Retirement Income Security Act of 1974. The interplay of federal laws requires a covered entity to carefully scrutinize whether disclosure is prohibited or permitted under HIPAA and the other applicable laws.



A number of conflicts exist between the protections afforded by HIPAA and other provisions of federal law. Because HIPAA permits but does not require many disclosures, conflicts are resolved by allowing disclosure of PHI when mandated by another federal authority. If other federal law prohibits a disclosure permitted under HIPAA, the other law controls. If a federal law permits but does not require disclosure of PHI, the covered entity must determine whether disclosure is authorized under HIPAA and, if so, comply with HIPAA.

Interplay of State Laws

As is usually the case when the states and federal governments attempt to regulate the same subject matter, federal statutes contain a preemption provision. HIPAA is no exception. There are, however, a number of areas where state law is not preempted, and in fact the Privacy Rule allows each state to adopt more stringent privacy protections (and many have done so).¹⁴ Preemption does not apply if the state law:

- Is necessary to regulate insurance or health plans, prevent fraud and abuse or report on healthcare system operations and costs
- Addresses controlled substances
- Relates to reporting disease, injury, child abuse, birth, death and other matters relating to public health
- Provides greater protection to the PHI than does HIPAA¹⁵

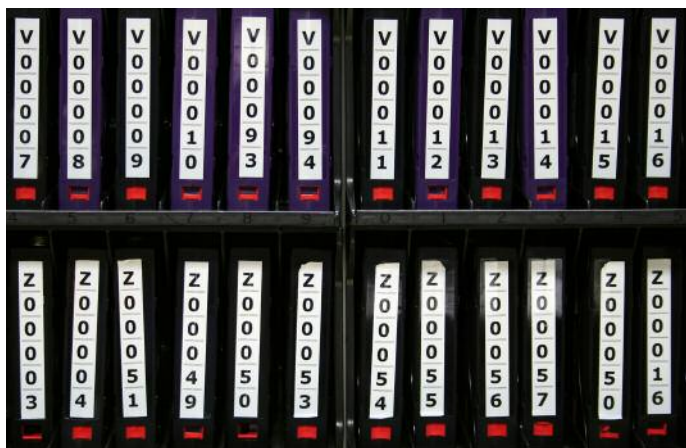
As is usually the case when the states and federal governments attempt to regulate the same subject matter, federal statutes contain a preemption provision. HIPAA is no exception. There are, however, a number of areas where state law is not preempted...

Determining whether a state law is more protective of PHI than is HIPAA is by no means an easy or automatic task. The possibilities for error are numerous. The most common source of conflict is state legislation protecting the privacy interests of persons undergoing treatment for particular diseases or conditions. Treatments involving mental health, sexually transmitted diseases and other potentially embarrassing conditions are often subject to specific protection under state law. The enhanced privacy protection is often deemed essential for public health purposes. For example, if persons with sexually transmitted diseases think their treatment will not be confidential, they might forego treatment. Resolution of conflicts between state law and HIPAA will probably lie in the hands of the courts.



State and Federal Laws Requiring Notification of Data Breaches

State legislatures have responded vigorously to citizens' outrage over breaches of confidentiality relating to personal data. California was the first to adopt a comprehensive security breach notification law, which became effective July 1, 2003.¹⁶ Generally, these laws apply to any organization that maintains electronic personal information – and healthcare providers often maintain not only PHI, but also economic data and other personal identifying information, such as Social Security and driver's license numbers. If data security is breached, the entity must promptly notify the individuals affected. As of now, at least 32 states have adopted similar laws providing the aggrieved consumer with a private right of action and liquidated damages in the form of a monetary award.



Legislation on the Horizon

In mid-July 2007, the Health Information Privacy and Security Act of 2007 (HIPSA) was introduced in the Senate. This bill requires each organization storing electronic personal health information to notify those individuals whose information is being stored about the organization's privacy practices. All organizations storing electronic personal health information would be required to implement adequate safeguards to prevent security breaches. Any failure to comply would result in civil penalties. Individuals would be entitled to access their electronic personal health information, and health data could not be used without the individual's permission. Before researchers could use personal health information, they would need to redact all unique information that might serve to identify the individuals whose records are involved. A new regulatory department would be established within the Department of Health and Human Services to provide individuals with privacy rights information.

The Identity Theft Task Force co-chaired by Attorney General Alberto Gonzales and Federal Trade Commission Chairman Deborah Platt Majoras recently recommended that a federal data breach notification law be enacted to supersede existing state law. The Task Force also recommended that federal legislation preempt state laws granting a private right of action and liquidated damages to people whose privacy has been invaded.

Congress is being lobbied by groups on all sides of the political spectrum to build strong privacy safeguards into any national electronic health record system that might be adopted. Lobbyists are armed with research surveys showing that American consumers will avoid treatment, omit critical medical data and delay care if they are compelled to share sensitive medical data without assurances that strong privacy protections are in place.

A Clear and Present Danger

Losses associated with data breaches totaled more than \$52 million in 2006, according to the latest Computer Crime and Security Institute/Federal Bureau of Investigation (CSI/FBI) survey. The survey revealed several key findings.

- Virus attacks, unauthorized access, laptop or mobile devices theft and theft of proprietary information account for 74 percent of all financial losses
- Use of cyber insurance remains low, but is on the rise
- The reporting of incidents is on the rise

Congress is being lobbied by groups on all sides of the political spectrum to build strong privacy safeguards into any national electronic health record system that might be adopted. Lobbyists are armed with research surveys showing that American consumers will avoid treatment, omit critical medical data and delay care if they are compelled to share sensitive medical data without assurances that strong privacy protections are in place.



The most notable privacy breach to date may be the ChoicePoint event, where 163,000 consumer records were exposed, resulting in 800 cases of identity theft.¹⁷ A 2006 FTC settlement included \$10 million in civil penalties and \$5 million in consumer redress.¹⁸

Healthcare organizations are also facing class action claims based upon disclosure of a privacy breach *even though no actual harm may have resulted from the security breach*.¹⁹ For example,

the Sisters of Saint Francis Health Services hospital system is being sued for \$1.3 billion (\$5,000 per person) over a recent data breach of 260,000 records.²⁰

Privacyrights.org recently estimated that 303 incidents occurred in 2006 with the potential to affect 18.8+ million individuals. A few examples of recent breaches affecting healthcare entities are listed below.

Recent Healthcare Data Breach Incidents

Type of Organization/ Month Made Public	# of Records	Incident Description
Publicly traded national HMO March 2005	140	A leading HMO was fined by the state for the publishing of confidential patient information on the web by a rogue employee.
Home health services provider January 2006	365,000	After backup tapes and disks containing Social Security numbers (SSN), clinical and demographic information, and a small amount of personal financial data were stolen, the provider and the state attorney general reached a settlement in which the provider agreed to offer free credit monitoring, credit restoration and reimbursement for direct losses.
Drug benefit management company March 2006	4,600	A stolen laptop contained SSN, birth dates and some prescription drug histories for state employees and their dependents.
Local chapter of national humanitarian organization May 2006	1,000,000	An employee gained access to blood donor records and misused SSN and other personal information to perpetrate three cases of identity theft.
Publicly traded HMO June 2006	17,000	An insurance company employee using a hotel computer exposed personal data about individuals in Medicare prescription drug plans by failing to delete data from the unsecured computer.
International insurance company June 2006	930,000	SSN, birth dates, and other personal data including some medical information was exposed when a computer server was stolen.



Type of Organization/ Month Made Public	# of Records	Incident Description
State health department June 2006	1,550	Personal data on individuals applying for state jobs as well as state employees was compromised when documents carrying names, addresses, SSN and phone numbers were removed from an office instead of being shredded.
National hospital operator August 2006	Thousands	A decade's worth of Medicare and Medicaid billing information and data on employees, patients and physicians from eight states were stored on computers stolen from a regional office.
Regional medical center August 2006	28,400	A laptop containing personal data, including SSN, on home healthcare patients was lost when a vehicle containing the laptop was stolen.
Multispecialty health clinic September 2006	1,100	Two cousins, one a clinic employee, apparently colluded to steal electronic personal information and use that data to file \$2.8 million worth of fraudulent Medicare claims; both were later indicted.
Several Indianapolis pharmacies September 2006	Unknown	The state investigated 30 pharmacies for violations of state law when a local reporter found customer information in unsecured garbage containers.
Regional Hospital System October 2006	266,200	CDs with unencrypted personal data were temporarily misplaced by a third-party billing service, exposing names and SSN of patients, employees, physicians and hospital board members.
Children's hospital October 2006	235,903	Hospital computers with personal data, including SSN and billing and banking information, were breached by overseas hackers.
Publicly traded health insurers/HMOs December 2006	200,000+	Personal data from health insurance records on computer backup tapes was stolen when a lockbox containing the tapes was taken from a vendor holding the data for an insurance company.
Data processing company December 2006	63,000+	Patient information dating back as far as 30 years, including SSN, name, date of birth and medical data, was on computers stolen from a provider of data processing services to large hospitals.



Type of Organization/ Month Made Public	# of Records	Incident Description
Veterans medical center February 2007	535,000 veterans, 1.3 million doctors	Despite uncertainty about the contents of a stolen portable hard drive, the VA has spent \$20 million to respond to 250 incidents leading to 46 investigations that may have involved exposed data on veterans and doctors.
State community health department April 2007	2,900,000	A private vendor handling state healthcare claims reported a missing data storage device that included SSN, addresses, date of birth, names and more.
Pharmacy chain April 2007	Hundreds	A pharmacy chain was accused of exposing personal information including credit and debit card numbers, names and addresses by illegally disposing of the information in a dumpster behind a store that was closing.
State public health department May 2007	140,000	SSN (without names or addresses) were exposed when a state health department failed to shred data on the parents of infants born over the course of a nearly a year.
Multinational drug maker June 2007	17,000	Current and former employee data, including names, SSN and addresses, was exposed by file sharing software installed on a company laptop. Some of the data files were found to have been copied.

Risk Management and Insurance Solutions

Effective risk management for data privacy exposures goes beyond traditional solutions. New processes are required. Healthcare organizations should start by identifying the stakeholders involved in the collection, processing, management and utilization of data. Often this includes individuals from IT security, audit/compliance, physical security, finance, human resources, risk management, legal and other departments.

Another key step is identifying relevant electronic assets, which include data, programs and processes, and evaluating their importance to the organization. This allows the measurement of the danger posed by various security threats. With the risks

quantified, an organization can then undertake an analysis of existing insurance policies with an emphasis on identification of coverage gaps.

The following are common findings of a gap analysis.

- **Property Coverage** – Often requires physical damage to tangible assets to trigger coverage, and data is not typically considered tangible property.
- **General Liability Coverage** – Similarly requires physical damage or bodily injury and would not be triggered by network security breach. Personal injury coverage may apply only to published matter, but not to theft of private



information. In addition, no coverage applies for electronic data, intentional acts or copyright exposures.

- **Professional Liability Coverage** – Bodily injury triggers may be required in malpractice policies. Coverage may be excluded by the narrow definitions of professional services in other policies. Some policies may cover disclosure of protected medical information, but not personal, financial or employee information.
- **Crime** – Theft of money and securities is covered, but not theft of information.
- **Directors and Officers Coverage** – Public company forms do not provide entity coverage except on securities claims. For both private companies and nonprofits, D&O policies typically contain personal injury, intellectual property or professional liability exclusions and do not provide coverage for first-party losses.



- **Cyber Liability Policies** – Network security policies purchased before 2005, and some more recent ones, likely provide cover for losses related to hackers, viruses and security breaches, but need to be broadened to respond to breaches of data where there is no failure of network security, as in breaches caused by administrative errors, or lost or stolen computers.

Next steps in the process include:

- Review of vendor/partner contracts and procurement procedures for appropriate risk transfer and limitation of liability elements
- Evaluation of physical and technical controls, including corporate policies and training
- Evaluation of insurance options to address gaps in coverage

Healthcare organizations should start by identifying the stakeholders involved in the collection, processing, management and utilization of data.

The solution to managing data privacy risks requires an approach that combines technology and security investments, procedures and training, legal planning and regulatory compliance, risk mitigation, contractual transfer, and an insurance program that proactively addresses the full scope of data privacy risks faced by an organization.

Frank Castro is a Senior Vice President with the Willis Healthcare Practice and the Managed Care Practice Leader. Also contributing to the article were Thomas Srail, Vice President, Willis Executive Risks Practice; and Gordon J. Calhoun, Esq., Chair of the Insurance Regulatory and Reinsurance Practice, Group Chair of Information Management and Privacy Practice Group and Vice Chair of the Life, Health, Disability and ERISA Practice Group at Lewis Brisbois Bisgaard & Smith LLP. Tom can be reached at 216 357 5997 or tom.srail@willis.com. Gordon can be reached at 213 250 1800 or calhoun@lbbslaw.com.



Footnotes

- 1 J. Gold Associates, "The Mobile Data Loss Epidemic," Technology Brief (6/5/2006); Sybase iAnywhere White Paper, "The Top 4 IT Considerations for Secure Wireless Email"
- 2 Ibid.
- 3 Ibid.
- 4 Sections 261-264 of HIPAA require the Secretary of Health and Human Services to publicize standards for the electronic exchange, privacy and security of protected health information. These provisions are known as the Administrative Simplification Provisions.
- 5 Ibid., § 164.302, *et seq.*
- 6 Ibid., §§ 160.103, 164.501 and 164.514(a), (b) and (e).
- 7 45 C.F.R. (Code of Federal Regulations) § 164.520.
- 8 *Id.*, §§ 160.102-.103.
- 9 *Id.*, §§ 164.501-.502.
- 10 *Id.*, §§ 160.103, 164.502(e), 164.504(e) and 164.524.
- 11 *Id.*, §§ 164.504(g), 164.510(b) and 164.522.
- 12 Social Security Act, 42 U.S.C. § 1320d-5(a).
- 13 Social Security Act, 42 U.S.C. § 1320d-6.
- 14 45 C.F.R. §§ 160.201-.205.
- 15 45 C.F.R. §§ 160.201-.205.
- 16 California Civil Code §§ 1798.80, *et seq.*
- 17 ChoicePoint Settles Data Security Breach Charges; to Pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress, January 26, 2006, available at www.ftc.gov/opa/2006/01/choicepoint.htm
- 18 Ibid.
- 19 Lawsuit Accuses Tri-West Healthcare of Negligence, Arizona Republic, Jan 30, 2003.
- 20 Fiercehealthit.com/story/more-hospital-data-security-breaches/2006-11-06



Contacts

For further information, please contact any of the following:

Kevin J. Downs
Executive Vice President and
Practice Leader
Chicago IL
Tel: 312-621-4812
kevin.downs@willis.com

Robert Marshall
Senior Vice President
New York NY
Tel: 212-837-0670
robert.marshall@willis.com

Paul A. Greve, Jr.
Executive Vice President/
Senior Consultant
Nashville TN
Tel: 615-872-3320
paul.greve@willis.com

Patrick Hickey
Senior Vice President
New York NY
Tel: 212-804-0598
patrick.hickey@willis.com

Jacqueline Bezaire RN, JD
Senior Vice President/Senior
Consultant
Los Angeles CA
Tel: 213-607-6343
jacqueline.bezaire@willis.com

Keith P. Becker
Senior Vice President
Atlanta GA
Tel: 404-224-5117
keith.becker@willis.com

David C. Wynstra
Executive Vice President
San Francisco CA
Tel: 415-955-0233
dave.wynstra@willis.com

Frank Castro
Senior Vice President
Los Angeles CA
Tel: 213-607-6304
frank.castro@willis.com

Brad Gabbard
Senior Vice President
Columbus OH
Tel: 614-766-8905
brad.gabbard@willis.com

