Health Care Data Breaches and Information Security
Addressing Threats and Risks to Patient Data

Lucy L. Thomson

HEALTH CARE DATA BREACHES ON THE RISE

Massive data breaches are occurring with alarming frequency. An analysis of data breaches by industry should provide a wake-up call for the health care industry—health care/medical data breaches now account for nearly 40 percent of all data breaches (see Table 15.1). Health care breaches have increased steadily from fourth place in 2007–2009 to second place behind only the business sector in 2010 and 2011. For the first quarter of 2013, there were more data breaches among health care providers than in any other industry sector—58 of 146 total breaches. Further, 562,577 patient records were breached, accounting for 62.9 percent of all reported breaches.

Table 15.1
Percent of Data Breaches by Industry Sector

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Business</td>
<td>33.6</td>
<td>36.9</td>
<td>47.3</td>
<td>42.1</td>
<td>41.2</td>
<td>36.6</td>
<td>29.3</td>
</tr>
<tr>
<td>Health/Medical</td>
<td>39.7</td>
<td>34.5</td>
<td>20.5</td>
<td>24.2</td>
<td>13.7</td>
<td>14.8</td>
<td>14.5</td>
</tr>
<tr>
<td>Educational</td>
<td>9.6</td>
<td>13.6</td>
<td>14.1</td>
<td>9.8</td>
<td>15.7</td>
<td>20.0</td>
<td>24.7</td>
</tr>
<tr>
<td>Government/Military</td>
<td>12.3</td>
<td>11.2</td>
<td>11.5</td>
<td>15.7</td>
<td>18.1</td>
<td>16.8</td>
<td>24.5</td>
</tr>
<tr>
<td>Banking/Credit/Financial</td>
<td>4.8</td>
<td>3.8</td>
<td>6.7</td>
<td>8.2</td>
<td>11.4</td>
<td>11.9</td>
<td>7.0</td>
</tr>
</tbody>
</table>

Failed security has resulted in massive data breaches that led to the loss or compromise of millions of personally identifiable health care records. In order to prevent data breaches, it is essential to analyze and understand the root causes of the security failures and develop a specific plan to address them. Analysis of the types of breaches that have occurred is very illuminating—for the conclusion that most of these breaches did not have to happen. To protect one of the most valuable and vulnerable assets of all organizations—data and information—is not only good business practice, but it will also avoid the high costs associated with responding to data breaches, potential liability, negative press, embarrassment, and ultimately loss of trust of patients and health care providers.

In almost all cases, data breaches that occurred could have been prevented by proper planning and the correct security design and implementation of appropriate security safeguards. Individuals and organizations alike have cause for serious concern. In today’s digital world, threats to information systems are evidenced almost everywhere a computer or laptop, smartphone, thumb drive, or other electronic device is operating. The proliferation of mobile devices and wireless technology that enables mobile health (m-health) and an expanding array of software applications present many vulnerable points in the flow of sensitive data in computer networks.

In just one month in mid-2012, three major data breaches resulted in the potential exposure of more than 1.3 million personal health records with a myriad of medical information, including genome data. A closer look reveals the types of lax security representative of health care breaches generally over the past five years.

- **Lost and stolen computers and mobile devices**—Emory Healthcare, Inc., in Georgia revealed that it lost ten computer disks containing patient social security numbers for about 315,000 surgical patients. Research universities are also involved in these types of breaches.

- **Hacker attacks**—The Utah Department of Technology Services publicized the breach of a server that houses Medicaid claims of 780,000 patients. It was suspected that hackers operating out of Eastern Europe were able to circumvent the security system of the server where the data were stored.

- **Malicious insiders**—The South Carolina Department of Health and Human Services revealed a major Medicaid data breach affecting the protected health

---

2. The high costs of responding to data breaches have been well documented. As the notification requirements in the data breach laws become more onerous with increasing numbers of individuals who must be notified, and the liability imposed by courts and administrative agencies for data breaches increases significantly, these costs are likely to rise dramatically. See http://www.ponemon.org/.
4. In January 2012, the Georgia Health Sciences University in Augusta announced a breach in its research medical school when a laptop computer that may have contained some of the patients’ personal information was stolen. Gabriel Perna, Georgia Health Sciences University Reports Data Breach, Healthcare Informatics (March 21, 2012), http://www.healthcare-informatics.com/news-item/georgia-health-sciences-university-reports-data-breach.
information of more than 228,000 Medicaid beneficiaries. The department discovered that an employee, since terminated, transferred spreadsheets with personal information (including contact information, dates of birth, ID numbers, and social security numbers) to a personal e-mail account.\(^6\)

Several months earlier in 2011, Sutter Physicians Services (SPS) and Sutter Medical Foundation (SMF) of Sacramento, California, announced one of the largest health care breaches ever—a password-protected, unencrypted desktop computer containing the health records of 3.3 million patients was stolen from their administrative offices. The computer contained patient contact information, dates of birth, telephone numbers, e-mail addresses, medical record numbers, and health insurance information.\(^7\)

A recent study by the Ponemon Institute confirmed that data breaches among health care providers have increased steadily since 2010.\(^8\) Responses among the 80 health care organizations that participated in the research attributed this situation to a lack of technologies, resources, and trained personnel to deal with privacy and data security risks. The Ponemon Institute concluded that data breaches can have “severe economic consequences,” and it calculated the average cost for the organizations participating in the study to be $2.4 million over a two-year period.\(^9\) Several disturbing findings were provided in the report:

- More health care organizations are having multiple breaches.
- Insider negligence continues to be at the root of many data breaches.
- Confidence in the ability to prevent and detect a data breach is improving but still has far to go.\(^10\)

**CAUSES OF DATA BREACHES**

**Mobile Devices**

Data breaches are pervasive because they are not only the result of hacker attacks, but they are also caused by sloppy security practices. More than one-third of data breaches resulted from the theft or loss of laptops, computers, hard drives, backup tapes, PDAs, or other portable media containing unencrypted personal information. In 2012 through mid-2013, the loss or theft of 132 mobile devices resulted in exposure of 2,681,131 personal records. Some of the largest breaches involving lost and stolen unencrypted mobile devices are identified in Table 15.2.

---

9. Id.
10. Id. at pp. 1–3.
Table 15.2
Health Care Breaches Caused by Lost or Stolen Mobile Devices

<table>
<thead>
<tr>
<th>Date</th>
<th>Company</th>
<th>Records Breached</th>
<th>Lost/Stolen Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 2011</td>
<td>TRICARE / SAIC</td>
<td>4,600,000</td>
<td>Backup tapes stolen</td>
</tr>
<tr>
<td>November 2011</td>
<td>Sutter Physicians Service and Foundation, CA</td>
<td>4,200,000</td>
<td>Desktop computer stolen</td>
</tr>
<tr>
<td>March 2011</td>
<td>HealthNet, CA / IBM</td>
<td>2,000,000</td>
<td>Server drives lost</td>
</tr>
<tr>
<td>February 2011</td>
<td>Jacobi Medical Center, Bronx, NY</td>
<td>1,700,000</td>
<td>Backup tapes stolen</td>
</tr>
<tr>
<td>October 2011</td>
<td>Nemours, DE</td>
<td>1,600,000</td>
<td>Three backup tapes missing</td>
</tr>
<tr>
<td>November 2009</td>
<td>HealthNet, CT</td>
<td>1,500,000</td>
<td>Portable hard drives lost</td>
</tr>
<tr>
<td>October 2009</td>
<td>BlueCross BlueShield, TN</td>
<td>1,000,000</td>
<td>Hard drives missing</td>
</tr>
<tr>
<td>September 2009</td>
<td>Oklahoma Dept. of Human Services</td>
<td>1,000,000</td>
<td>Computer stolen</td>
</tr>
<tr>
<td>October 2009</td>
<td>BlueCross BlueShield / Highmark</td>
<td>850,000</td>
<td>Laptop stolen</td>
</tr>
<tr>
<td>March 2012</td>
<td>California Dept. of Child Support</td>
<td>800,000</td>
<td>Computer devices lost</td>
</tr>
<tr>
<td>April 2011</td>
<td>Eisenhower Medical Center, CA</td>
<td>514,000</td>
<td>Computer stolen</td>
</tr>
<tr>
<td>April 2012</td>
<td>Emory University Hospital, GA</td>
<td>315,000</td>
<td>Ten backup tapes stolen</td>
</tr>
<tr>
<td>March 2011</td>
<td>Cord Blood Registry / FTC</td>
<td>300,000</td>
<td>Backup tapes stolen</td>
</tr>
<tr>
<td>April 2011</td>
<td>Oklahoma Dept. of Health</td>
<td>133,000</td>
<td>Laptop stolen</td>
</tr>
<tr>
<td>April 2011</td>
<td>Mid-State Medical Center, CT</td>
<td>93,500</td>
<td>Hard drives lost</td>
</tr>
<tr>
<td>February 2011</td>
<td>St. Francis Hospital, OK</td>
<td>84,000</td>
<td>Computer stolen</td>
</tr>
<tr>
<td>November 2011</td>
<td>Neurological Institute of Savannah</td>
<td>63,000</td>
<td>Laptop stolen</td>
</tr>
<tr>
<td>January 2013</td>
<td>Stanford U Children’s Hospital</td>
<td>57,000</td>
<td>Laptop stolen</td>
</tr>
<tr>
<td>March 2013</td>
<td>NC DHHS / contractor</td>
<td>50,000</td>
<td>Thumb drive lost</td>
</tr>
<tr>
<td>March 2012</td>
<td>Howard University Hospital, DC</td>
<td>34,500</td>
<td>Laptop stolen</td>
</tr>
</tbody>
</table>

These breaches illustrate the sheer magnitude of the exposure of personal records and the potential damage to millions of individuals. In light of available security measures and their widespread acceptance within the information security community, there is no excuse for health care organizations that collect and store ePHI to fail to fulfill their duty to protect personal patient information.

The importance of addressing these types of breaches is illustrated by a recent FTC case involving the operator of a leading cord blood bank. In February 2013, Cbr Systems, Inc., agreed to settle FTC charges that it failed to protect the security of customers’ personal information, and that its inadequate security practices contributed to a breach that exposed the social security numbers and credit and debit card numbers of nearly 300,000 consumers. The FTC charged that Cbr’s failures to provide reasonable and appropriate security for consumers’ personal information contributed to a December 2010 security breach during which unencrypted backup tapes containing consumers’ personal information, a Cbr laptop, a Cbr external hard drive, and a Cbr USB drive were stolen from a Cbr employee’s personal vehicle. According to the complaint, the unencrypted backup tapes included names, gender, social security numbers, dates of birth, driver’s license numbers, credit and debit card numbers, card expiration numbers, checking account numbers, addresses, e-mail addresses, telephone numbers, and adoption type of approximately 298,000 Cbr customers. The unencrypted devices also contained network information, including passwords and protocols, that could have permitted an intruder to access Cbr’s network, where sensitive personal health information (PHI) was stored. The settlement requires Cbr to establish and maintain a comprehensive information security program and submit to independent security audits every other year for 20 years. The Identity Theft Resource Center has analyzed the problem this way: “This is 100% avoidable, either through use of encryption, or other safety measures. Laptops, portable storage devices and briefcases full of files, outside of the workplace, are still ‘breaches waiting to happen.’ With tiered permissions, truncation, redaction and other recording tools, PII can be left where it belongs—behind encrypted walls at the workplace.”

Malicious Insiders
Malicious insider attacks are on the rise and pose a serious threat to the security of sensitive information. These activities accounted for another third of the breaches. Individuals who abused administrative privileges caused a significant number of breaches, and

12. The settlement requires Cbr to establish and maintain a comprehensive information security program and submit to independent security audits every other year for 20 years.
security failures such as not suspending system access for terminated employees caused many breaches.

During the first quarter of 2013, approximately 26 to 28 insider breaches were reported by organizations tracking data breaches. In 2012, 88 insider breaches were reported. In 2007, 12,372 data breaches caused by insiders were reported. About one-quarter of the reported insider breaches were perpetrated by employees who had some type of job change—they were fired, they resigned, they were newly hired, or they changed roles within the organization.

Defending an organization’s perimeter from external attack does not protect against valuable information seeping out because of insider malfeasance, whether that behavior is characterized as malicious, mischievous, or ignorant/accidental. Carnegie Mellon University has published a list of best practices to minimize the risk of insider attacks. Recent incidents and law enforcement activity against malicious insiders include the following:

- A federal grand jury indicted a surgical instrument technician at UPMC Shadyside in Pennsylvania for selling patients’ names, birth dates, and social security numbers; he pled guilty.

- In March 2013, a husband and wife in Chester Springs, Pennsylvania, were charged in a $257,710 tax fraud scam that involved the stolen identities of patients at Crozer-Chester Medical Center and Chester Community Hospital. The couple allegedly filed fraudulent tax returns seeking more than $1.7 million in refunds. They obtained the names, dates of birth, and social security numbers of 144 patients by paying employees of the hospitals to steal confidential medical forms.

- In February 2013, a senior clerk at the Palm Beach Health Department in Florida was arrested and charged with using her job to steal identity information from more than 2,800 patients.

- In April 2012, a former manager of the Head Injury Association in Long Island, New York, was indicted for stealing the identities of patients. A 48-count indictment alleged that he used the names and social security numbers of patients to e-file fraudulent tax returns and obtained over $200,000 in federal and state tax refunds.

---


Causes of Data Breaches

• In January 2012, United Healthcare (UHC), based in Minnesota, discovered employee access to information in a database that UHC learned was unauthorized. The information that may have been accessed included patients’ names, social security numbers, telephone numbers, dates of birth, addresses, and Medicare Healthcare insurance numbers.  

• In March 2013, Anthem BlueCross-BlueShield of Ohio informed patients that an employee at Connexions, a vendor that supplies call center services to Anthem BlueCross, took social security numbers and may have conveyed some information to third parties who are the subject of an ongoing criminal investigation.

• River Falls Medical Clinic in Wisconsin notified about 2,400 clients of a breach that was tied to a subcontractor, an outside cleaning service employee who stole patient records during the summer of 2012.

• In November 2011, several employees of the Berkeley Heart Lab in California were found to have accessed patient information without authorization and to have taken the data to a competitor.

Databases are vulnerable to attacks from both insiders and hackers. These vulnerabilities are well-documented and include the use of default and weak passwords, failure to patch known vulnerabilities, misconfigurations, and excessive privileges granted to users. Specific security measures must be taken to protect personal data in biometrics, bioinformatics, and other health care databases.

Inadvertent Postings at Websites and Other Disclosures

Through careless handling, personal data, particularly social security numbers, are often exposed in postal mailings. In addition, data may also be posted on websites where it is accessible to individuals who are not intended to have access to it.

For example, in January 2013, MedAmerica of Florida found that long-term care insurance enrollment forms placed on what was believed to be a secure server had become publicly accessible through the Internet for a six-month period in 2012. The forms included applicants’ names, addresses, dates of birth, and social security numbers. To the extent that health information or the names of other insurance companies were provided on the enrollment forms, that information may have been included as well.


23. Josh Shaul, Stop Attackers in Their Tracks: Addressing the Insider Threat, http://www.us-cert.gov/GFIRST/presentations/2011/Combating_Database_Insider_Threat.pdf. Specific security measures that must be taken to protect personal data include: (1) Inventory your databases; (2) Classify systems with sensitive data; (3) Scan for vulnerabilities and misconfigurations, keep up-to-date with security patches, enforce strong passwords, and audit configurations and settings; (4) Identify privileged users (DBAs); (5) Validate access to sensitive data; assign restricted permissions on tables with sensitive information; (6) Prioritize and fix what you can; (7) Monitor database activity; and (8) Encrypt data in transit and at rest using network-level encryption and column-level encryption.

24. ITRC Data, supra note 21.
In February 2012, the St. Joseph Health System alerted more than 31,000 patients in California that their PHI records may have been searchable on the Internet.  

In April 2013, it was reported that stacks of paperwork containing personal information—including social security numbers—of patients were carelessly dumped on the sidewalk when Landmark Medical Supplies, a Brooklyn, New York, medical supply store, was shuttered.  

In March 2013, the FBI investigated an unlocked dumpster full of medical documents from Family Intervention Services in Georgia that television news reporter Ross Cavitt found outside an office complex. Cavitt called authorities after finding the documents full of people’s sensitive identification and medical information.  

Peer-to-peer (P2P) file-sharing technology creates a significant risk of a breach when it is installed on the same computer as PHI. When the P2P file-sharing software is not configured properly, sensitive records not intended for sharing may be accessible to anyone on the P2P network. In several cases, personal health records were breached this way.

Cloud Computing Risks

Because of the increased flexibility and efficiency afforded by computing resources available on demand, cloud environments may be ideally suited to processing genomic data. Large amounts of computing power are needed for research within short time periods. However, cloud computing introduces information technology (IT) security and privacy risks related to outsourcing the administration and physical control of sensitive data to a third-party vendor and to maintenance of the data on shared computing platforms, risks that will need to be carefully evaluated and addressed by entities that intend to put genomic data of patients in the cloud.

THE NEED FOR RISK ASSESSMENT

Ensuring the confidentiality, integrity, availability, and privacy of data in health care information is fundamental to protecting the personal information of patients. Information security is not a mystery—it is based on a systematic assessment of threats and risks that are present in a particular information system.

Federal laws governing the privacy and security of patient health records require that government and private-sector organizations conduct a risk assessment as part of their security management processes. Based on a risk assessment, appropriate security measures can be implemented to protect sensitive data.

---

26. FTC Data, supra note 21.
27. The FTC has notified almost 100 organizations that personal information, including sensitive data about customers and/or employees, has been shared from the organizations’ computer networks and is available on peer-to-peer (P2P) file-sharing networks to any users of those networks, who could use it to commit identity theft or fraud. Widespread Data Breaches Uncovered by FTC Probe, FTC Warns of Improper Release of Sensitive Consumer Data on P2P File-Sharing Networks, http://www.ftc.gov/opa/2010/02/p2palert.shtm.
controls can be selected, implemented, and continuously monitored, so that risks and vulnerabilities are reduced to a reasonable and appropriate level.\textsuperscript{30}

The principal goal of an organization’s risk management process should be to protect the organization and its ability to perform its mission, not just its IT assets. A risk analysis process\textsuperscript{31} includes, but is not limited to, the following activities:

1. Evaluate the likelihood and impact of potential risks to ePHI;
2. Implement appropriate security measures to address the risks identified in the risk analysis;
3. Document the chosen security measures and, where required, the rationale for adopting those measures; and
4. Maintain continuous, reasonable, and appropriate security protections.

Risk analysis should be an ongoing process, in which an organization regularly reviews its records to track access to ePHI and detect security incidents; periodically evaluates the effectiveness of security measures put in place; and regularly reevaluates potential risks to ePHI.

**ACHIEVING OPTIMAL NETWORK SECURITY THROUGH CONTINUOUS MONITORING**

To protect against massive data breaches, it is clear that the health care industry, as well as companies in the retail, education, and financial sectors, and government agencies, must take immediate action to strengthen their security posture. Government officials and private-sector executives have reached a consensus that a prioritized approach to information security is required. Continuous monitoring of systems and networks is essential to protect against the broad range of serious threats to information systems.\textsuperscript{32}

At the direction of the U.S. Congress, NIST is developing a common information security framework for the federal government and its contractors.\textsuperscript{33} Robust continuous monitoring will provide senior executives with the information necessary to make cost-effective, risk-based decisions.\textsuperscript{34} While NIST guidance has been developed for

\textsuperscript{30} HIPAA requires Administrative, Physical, and Technical Safeguards. See 45 C.F.R. § 164.306.

\textsuperscript{31} Excellent resources for conducting a risk assessment and assessing compliance with the HIPAA Privacy and Security Rules are available at http://www.nist.gov/itl/csd/20111122_hipaa_tools.cfm.

\textsuperscript{32} The SANS Consensus Audit Guidelines (CAG) provide guidance to maximize the impact of government and private-sector security efforts and identify 20 critical priority controls, most of which can be continuously monitored. Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines, v. 4.1, http://www.sans.org/critical-security-controls/ (the website provides a wealth of valuable information about the leading information security methodologies and how they relate to each other).


government agencies, it is equally appropriate for private-sector organizations. Significantly, NIST has issued guidance tailored for health care organizations.\(^\text{35}\)

Information security continuous monitoring is a critical part of organization-wide risk management. To properly support an organization’s risk management framework, security must be incorporated into the architecture and design of the organization’s information systems and supporting IT assets. Continuous monitoring provides an understanding of threats and threat activities by evaluating the security impact of actual and proposed changes to the system; assessing all security controls; collecting, correlating, and analyzing security-related information; providing actionable communication of security status across all levels of the organization; and establishing active management of risk by organizational officials.

Continuous monitoring is designed to provide meaningful, actionable intelligence and reporting—instead of merely collecting data. Cybersecurity situational awareness will inform executives about the threat, vulnerability, and compliance posture of the system, as well as provide information about incidents that will need to be investigated. Potential threats must be investigated, and targeted attacks can be detected in advance or addressed as they occur, enabling a highly proactive security posture. The result of continuous monitoring will ensure that all the information necessary to address security incidents and potential attacks is readily available for analysis and review. The objective is to address the multitude of security threats and risks in a timely, disciplined, and structured fashion. The tenets of continuous monitoring apply to bioinformatics databases.

**ACTION PLAN TO ADDRESS HEALTH CARE DATA BREACHES**

Data breaches can and must be prevented. Organizations that collect, use, store, and share patient information must accept responsibility for protecting personal health care information and ensuring that it is not compromised by hackers or malicious insiders or inadvertently accessed, lost, or stolen.

The intense focus on response after a data breach has occurred is very costly to organizations and does little to remediate the losses of the individuals for whom the breach of their personal information has exposed them to identity theft or fraud. Business owners and data custodians and their attorneys in the private sector and in government around the globe, particularly those involved in health care, must redouble their efforts to understand the risks of collecting, storing, and sharing sensitive and personal information, the many ways data can be breached, and the tools available to protect the data. They must develop the expertise to avoid these breaches and to address them appropriately if and when they occur. This includes an appreciation of the fact that no single solution is appropriate for every organization. Information security must be tailored based on the type(s) and sensitivity of data to be protected, the potential risks to the data, and the nature of the information system of the organization, including the hardware.

software, applications, and interconnections. As well, business owners and data custodians must understand that implementation and periodic auditing are as important as the initial security controls that are put in place.

Privacy and security must be considered when system design requirements are being developed and decisions are being made about the data and information that will be collected, and how it will be used in the system and shared. Adoption of best practices, including continuous monitoring and adherence to the tenets of the HIPAA Privacy Rule and Security Rule, will ensure that health care organizations can maintain information security and avoid data breaches—and the massive invasions of privacy that result.

**PROTECTING THE PRIVACY AND SECURITY OF PERSONAL HEALTH RECORDS**

It is not necessary or appropriate to assume that electronic medical records cannot be protected from data breaches. Health care providers, researchers, and other health care entities have a legal responsibility to protect medical records from unauthorized access, whether malicious or unintentional, by both insiders and hackers. To do this, organizations must have appropriate privacy and security policies in place to protect the data, as well as risk-based management, administrative, and technical controls necessary to ensure information security. Securing personal patient information in large health care databases must be approached systematically. The majority of privacy and security risks can be addressed by conducting a risk assessment and prioritizing steps to secure an information system. As the amount of genomic information collected in electronic form continues to grow, the imperative of information security will only grow stronger.

**LEGAL REQUIREMENTS AND IMPLICATIONS**

**HIPAA Privacy Rule and Security Rule**

The HIPAA Privacy Rule (Privacy Rule)\(^{36}\) establishes a category of health information, defined as “protected health information” or PHI,\(^{37}\) that a covered entity\(^{38}\) may use or disclose to others only in certain circumstances and under various conditions. PHI is a subset of “personally identifiable information.”\(^{39}\) The Privacy Rule applies to individually identifiable health information created or maintained by a covered entity.\(^{40}\)

In addition to the Privacy Rule, other regulations may apply as well. For instance, individual records held by covered entities that are also alcohol and substance abuse

---


\(^{37}\) 45 C.F.R. § 160.103.

\(^{38}\) Id. A covered entity is a health care provider, a health care plan, or a health care clearinghouse, including entities that process nonstandard health information they receive from another entity into a standard format (i.e., standard electronic format or data content), or vice versa.


\(^{40}\) 45 C.F.R. § 106.103.
treatment providers are protected by the Confidentiality of Alcohol and Substance Abuse Patient Records regulation.\textsuperscript{41} Also, the HHS and U.S. Food and Drug Administration (FDA) Protection of Human Subjects regulations may apply to health services research.\textsuperscript{42} In addition, if health-related research involves ePHI, covered entities must also consider the requirements of the HIPAA Security Rule.\textsuperscript{43}

The national goal of developing an electronic health record, consisting of a broad array of the most sensitive types of information about individuals, for all Americans by 2014 has stimulated the creation of ePHI that can be transmitted to other entities and stored in information repositories around the world. These electronic medical records contain detailed information such as patient contact information, social security numbers, dates of birth, height, weight, sex, and race; medical, psychological, and dental information; laboratory and diagnostic test results; registries; social, economic, and demographic data; health services utilization; insurance and hospital cost data; employer, conditions of work environment, and exposure to hazardous substances and compounds; information pertaining to stored biologic specimens (including blood, urine, tissue, and genetic materials); genetic information; characteristics and activities of health care providers and educators and trainers; and associated correspondence.

Individuals and organizations involved in the health care and research environments who collect sensitive personal and medical information and store, use, and share it electronically are required under HIPAA to protect and safeguard those records.

The HIPAA Security Rule sets national standards for the security of ePHI.\textsuperscript{44} It requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting ePHI. Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

The Security Rule is designed to be flexible and scalable so a covered entity can implement policies, procedures, and technologies that are appropriate for the entity's particular size, organizational structure, and risks to consumers' ePHI. Therefore, when a covered entity is deciding which security measures to use, the rule does not dictate those measures but requires the covered entity to consider:

- Its size, complexity, and capabilities;
- Its technical, hardware, and software infrastructure;

The costs of security measures; and
• The likelihood and possible impact of potential risks to ePHI.

Finally, the Security Rule does not mandate the use of any specific technology, such as encryption. However, HHS guidance issued following the passage of the federal data breach notification requirement provides a safe harbor for PHI that either is encrypted or has been destroyed. If a data breach occurs involving encrypted PHI, there is no violation of the statute.45

The most significant risks to privacy or of a data breach appear to be at physicians’ offices where PHI is collected routinely, as well as in organizations such as hospitals and health plans that maintain large databases containing health records of millions of patients.46 At the physician level, sensitive data are being entered into electronic medical records, and with the growth of health information exchanges, these data are being transferred from one medical doctor or health care entity to another. In these circumstances, it is clear that HIPAA applies—PHI is being transmitted electronically. It appears that physicians and hospitals (including affiliated and independent laboratories) are gathering health care information, including PHI.

**HITECH—The Federal Data Breach Notification Law**

Congress enacted the first federal data breach notification law as part of the Health Information Technology for Economic and Clinical Health Act, known as the HITECH Act,47 a law whose primary purpose is to promote health information technology, including electronic health records. HITECH and HIPAA48 are designed to protect PHI from unauthorized access and use. Pursuant to the statutory scheme, covered entities must protect this individually identifiable health information by encrypting such information or utilizing another means to protect the information. And if unauthorized access occurs, they must notify individuals of the breach in a timely manner. With the collection of significant personal information about individuals, both identified and de-identified, all those involved with bioinformatics need to be prepared to address the requirements of the recently enacted federal data breach notification statute.

In enacting HITECH, Congress has endeavored to respond to the need to protect electronic health records and address widespread invasions of privacy caused by breaches of medical and other individually identifiable health information. HITECH requires entities covered by the statute to notify individuals whose PHI has been breached. Generally, PHI means all medical records, including electronic medical records, and other information reflecting individually identifiable health information maintained by an entity or its business associates. Both HHS and the Federal Trade Commission (FTC) have issued final rules or regulations designed to implement HITECH requirements.49

46. See infra the discussion of data breaches.
49. 42 C.F.R. pts. 412, 413, 422, and 495 (HHS); 16 C.F.R. § 318.4 (FTC).
HHS has issued an Omnibus Final Rule\(^{50}\) that defines “breach” as the acquisition, access, use, or disclosure of protected health information in a manner not permitted under the HIPAA Privacy Rule and that compromises the security or privacy of the protected health information. The rule provides a safe harbor under which covered entities that encrypt PHI consistent with standards promulgated by NIST or that destroy the information are not required to comply with the notification requirement in the event of a data breach. The means of notification required vary depending on the extent of the breach, meaning the number of individuals whose PHI has been breached. In some cases, only individuals must be notified; in larger breaches, the media and the Secretary of HHS must also be notified.

NIST publications present a broad array of guidance that a covered entity may utilize or follow to protect individually identifiable health information, including encryption. No single standard will ensure the security of an information system. While HHS focuses on the need for encryption, no information system can be secure absent an appropriate security design, selection and implementation of security controls based on a risk assessment, and timely maintenance and periodic monitoring of the system.

The FTC has also issued regulations pursuant to HITECH that cover vendors; its jurisdiction is limited to non–HIPAA-covered entities. As such, the FTC regulations do not cover electronic health records made and utilized in a physician’s office. The primary focus of the regulations is the security of personal health records maintained by individuals on vendor websites.

**State Data Breach Notification Laws**

Forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of individuals whose personal information may have been affected by a security breach.\(^{51}\) California was the first state to enact a data breach notification law, and other states have followed its lead. Generally, the laws require that any business in possession of sensitive personal information about a covered individual must disclose a breach of that information. Many health care providers, researchers, and other entities that maintain databases with personal health records are covered by these state laws. Each state law defines the type of personal information covered by the law, who must be notified, when notice must be provided, and the content and form of the notice.

The definition of a breach varies from state to state. Generally, the statutes require notice to affected individuals following the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information about individuals. However, notice is not required in several states unless there is a reasonable basis to believe the breach will result in substantial harm or inconvenience to the affected individuals. In most cases, businesses may avoid the notification requirements if the breach involved information that has been encrypted, provided the encryption key has not been compromised.


Some states have responded to the massive data breaches by expanding their laws to provide some type of information security to protect sensitive personal information—not merely to report when data have been hacked or stolen. Nevada and Massachusetts have enacted statutes requiring substantial security measures. Massachusetts requires any firm conducting business with state residents to develop a comprehensive information security program. They must employ encryption, adopt a risk-based approach to ensuring security, and protect against data leakage. Nevada has taken the additional step of requiring holders of credit card and other personal information in computerized information systems to comply with the professional standards promulgated by the Payment Card Industry Council. In addition, businesses are required to encrypt all transmissions of personal information.

Data custodians in California must implement reasonable security procedures and practices. New Jersey law limits disclosure and transmission of social security numbers over the Internet. Maryland requires organizations to employ reasonable security procedures.

In recent years, many states have expanded the scope of their data breach laws, set additional requirements related to notification, and changed the penalties for those responsible for breaches.