Chapter 25
Privacy and Data Security: HIPAA and HITECH

Joan M. Kiel, Frances A. Ciamacco, and Bradley T. Steines

Abstract With the Omnibus Final Health Insurance Portability and Accountability Act (HIPAA) Rule of September 2013, privacy and security of patient health information has been further tightened. Looking back from 2002 when HIPAA was first released, monetary penalties have increased as has the scrutiny surrounding the protection of patient health information. With numerous updates and additions, such as the Health Information Technology for Economic and Clinical Health Act, (HITECH), to the original HIPAA Rule, managers have to be akin to the changes as any day can bring a HIPAA complaint or breach. In this uncertain environment, breach management is a critical part of working with HIPAA. HIPAA and HITECH are laws which are to be operationalized into an organization's standard operating procedures.

Keywords HIPAA • Security • Breaches • Risk analysis • Privacy • Patient health information

As focus and emphasis on the privacy and security of patient protected health information (PHI) continues to grow, so do the sanctions associated with a violation of such tenets. The year 2014 saw the largest monetary settlement to date regarding a data breach involving PHI.

J.M. Kiel, PhD, CHPS MPhil, MPA (✉)
HIPAA & HMS Departments, University HIPAA Compliance, Health Management Systems, Duquesne University, Pittsburgh, PA, USA
e-mail: kiel@duq.edu

F.A. Ciamacco, BS, MS, RHIA
Office of Ethics and Compliance, UPMC, Pittsburgh, PA, USA

B.T. Steines, JD
Corporate Services Division, Office of Ethics and Compliance/Office of Patient and Consumer Privacy, UPMC, Pittsburgh, PA, USA

C.A. Weaver et al. (eds.), *Healthcare Information Management Systems: Cases, Strategies, and Solutions*, Health Informatics,
DOI 10.1007/978-3-319-20765-0_25

In the case in point, New York Presbyterian Hospital (NYP) and Columbia University (CU), operating under a joint arrangement, failed to adequately secure the electronic PHI of nearly 7,000 patients, leading to a breach of sensitive patient information. Upon investigation into the matter, the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) determined that neither NYP nor CU had made "data security central to how they manage their information systems." NYP and CU ultimately settled charges stemming from the breach with the OCR in the amount of $4.8 million [1].

Suits and settlements such as the above are becoming more commonplace.

25.1 The Emergence of HIPAA, HITECH, and the Omnibus Rule

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was created to provide health insurance portability for individuals, to protect the privacy and security of patient health information, and to eradicate fraud and abuse. Also known as the Kennedy-Kassebaum Act or the Administrative Simplification Act, HIPAA was enacted on August 21, 1996 (http://www.ihs.gov/hipaa; accessed October 18, 2014). The law applies to all healthcare providers, clearinghouses, and healthcare plans, known collectively as "HIPAA Covered Entities", who conduct 1 or more of 11 transactions electronically, including billing and receiving payment for healthcare services.

The original impetus for HIPAA emanated from both providers and consumers. Providers wanted standardization and simplification of healthcare claims. Multiple healthcare claim forms, both paper and electronic, had previously existed. This inconsistency necessitated that when transmitting claims data, many times the data would thus first be passed through a clearinghouse, formulating the outgoing data from the provider to the receiving payer organization, and vice versa. This "added step" increased both time and cost to the process. HIPAA standardized claim submissions, such that the sender and the receiver would now have the same formage. Consumers demanded privacy and security of their patient health information, including all oral, paper, and electronic notations. HIPAA thus became integral throughout the delivery of quality healthcare, and if not adhered to, raises wide ranging implications.

The standards set forth in the 1996 passage of HIPAA have since been amended and added to via subsequent legislation, all of which has been consolidated under the HIPAA Omnibus Rule (Omnibus Rule), passed in 2013. The intent of the Omnibus Rule was not only to consolidate the ever evolving obligations and technology associated with the delivery of healthcare, but also to promote objectivity and consistency in the analysis of potential breaches patient privacy.

25.2 The Timeline of HIPAA

In 1996 HIPAA was passed as federal law with the intents to safeguard the privacy of protected health information, to establish national standards for health care transactions, and to secure the information that are the subject of the transactions. To this end, six rules of HIPAA were released for implementation between 2002 and 2007.

1. Transactions and Code Sets: Has established standard formats and coding of electronic claims and related transactions. Implemented October 16, 2002.
2. Privacy Rule: Has established guidelines for the use and disclosure of patient health information. Implemented April 14, 2003
3. National Employer Identifier Rule: Has established the federal tax identification number as an employer's national identifier. Implemented July 30, 2004.
4. Data Security Rule: Has established technical and administrative protocols for the security and integrity of electronic health data. Implemented April 20, 2005.
5. Enforcement Rule: Has established rules on how the Government enforces HIPAA. Implemented February 16, 2006
6. National Provider Identifier Rule: Has established a national identifier for each provider and the mechanisms for disseminating, storing, and updating the identifier. Implemented May 23, 2007 [2].

In 2009, the Health Information Technology for Economic and Clinical Health Act (HITECH) was passed as a subset of the American Recovery and reinvestment Act (ARRA). Although it focused on the utilization of electronic health records and meaningful use, it also expanded the Privacy and Security Rules of HIPAA. In 2013, HIPAA was further modified and the Final Rule of HIPAA known as the Omnibus Rule was implemented. Some of the highlights include obligations to business associates, increased rights for patients to access and restrict disclosure of their PHI, rules for use and disclosure of PHI, and clarification of the Enforcement Rule [3] (New Privacy and Security Omnibus Rule Released, Robert Tennant and Amy Nordeng, MGMA Connexion, April 2013, page 18 of 18–21).

25.3 Security

The HIPAA Security Rule was enacted to prevent patient health information from being accessed by those without a "need to know". It is paramount that the security and integrity of electronic health data must be protected from unauthorized users. Although electronic exchanges and storage of medical information is prevalent, HIPAA security encompasses physical and administrative security in addition to technical security.

The Security Rule challenges that all electronic transmissions maintain a balance between being accessible, but also being secure and confidential. Information technology systems will follow the ANSI (American National Standards Institute) Standards for interfacing with, including storing, accessing, and transmitting data, all systems. In addition, the Security Rule encompasses various technical and operational policies and procedures such as password maintenance and management, incident reporting, periodic reminders to ensure a secure environment, virus protection, and monitoring of log in and user access.

Data intrusion and breaches of privacy and security protocols are not concerns unique to the health care industry. Long gone are the days where customer records exist on a single piece of physical paper locked away neatly in a filing cabinet. Today's world is filled with the ability to immediately access and transmit mass amounts of information of all kinds. Customer information is not only used to facilitate direct transactions, but it is also warehoused and data-mined for downstream use.

As large amounts of information are utilized by the commercial sector such ways, the information is in turn exposed to the risk of intrusion. Further, as the number of individuals whose information an entity utilizes continues to climb, and the detail associated with that information becomes increasingly more detailed, the likelihood that a breach of that information would be a major issue affecting a large population grows exponentially in turn.

An entity's data security measures must be robust enough to combat current threats, while remaining nimble enough to adjust to an ever changing world of risk. Unfortunately, it is tempting to become complacent in times of minimal breach activity, relying on outdated or insufficient security processes. When a technologically savvy criminal element is added to this mix, the setting is ripe for compromise. It was exactly this climate of risk that yielded an epidemic of large-scale data breaches in 2013 and 2014.

Target (2013) – Approximately 110 million people affected
JP Morgan Chase (2014) – Approximately 75 million people affected
Home Depot (2014) – Approximately 56 million people affected
Evernote (2013) – Approximately 50 million people affected
Living Social (2013) – Approximately 50 million people affected
Adobe (2013) – Approximately 40 million people affected [4]

A breach is the acquisition, access, use, or disclosure of protected health information in a manner which compromises the security or privacy of the protected health information (45CFR164.402) [5]. A disclosure to unintended recipients is reportable under HIPAA to the affected individuals and the Department of Health and Human Services. In addition, if the affected number is 500+, the breach must be reported publically and to the media. Breaches must be investigated according to four factors:

(a) The nature, extent, and level of detail of the patient health information involved: In investigating this factor, one would examine if the information was publically

available. Was only demographic information sent and does this escalate the risk of identity theft. Are there any embarrassing elements to the patient health information? Lastly, even if a patient name was not used, does the patient health information lead one to have the ability to identify the patient.

(b) Identity of the recipient: Is the recipient a HIPAA covered entity and thus employing privacy and security standards? Would the recipient know what to do with the patient health information in regards to the sender?

(c) Whether the patient health information was actually acquired or viewed: Was the patient health information encrypted? Who saw what and was their further disclosure? How did the covered entity become aware of the situation?

(d) What mitigation steps were taken: If the patient health information was in paper format, was the original copy returned or destroyed; were further copies made? If electronic, was there remote scrubbing of devices and drives. Did law enforcement need to be contacted? [6]

In looking at the four factors, breaches are to be evaluated based on the unique facts and situation. If an allegation or suspicion is substantiated, but a low probability of compromise is legitimately determined, the matter may still be a breach or violation of a standard, but it is not reportable. In contrast, if a risk assessment is not performed, the breach determination reverts to the presumption of the event being reportable.

In 2012, Massachusetts Eye and Ear Infirmary and Eye and Ear Associates (MEEI) settled with the Office for Civil Rights for $1.5 million. It was found that there was theft of an unsecured and unencrypted laptop containing PHI. In addition, MEEI failed to take the necessary steps to comply with the Security Rule [7]. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement.html.

In 2012, the Alaska Department of Health and Human Services (DHHS) settled with the Office for Civil Rights for $1.5 million. It was found that a USB hard drive was stolen out of an employee's vehicle. The portable device was unsecured and unencrypted and thus patient health information could be accessed. In addition, the covered entity did not have HIPAA policies and procedures in place concerning security encryption of devices or appropriate risk analysis for breaches [8]. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/alaska-agreement.html.

In 2014, New York Presbyterian Hospital (NYP) and Columbia University (CU) had a violation while sharing a network and firewall. A physician was able to pull protected health information onto another server without HIPAA compliant technical safeguards. This resulted in the public being able to view patient health information via an internet search engine. Six thousand, eight hundred patients were involved and the resultant fine to the Office for Civil Rights was $4.8 million [9].

HIPAA covered entities must appoint a person to direct their HIPAA security efforts. A major responsibility of the security person is to conduct an information technology security audit. The audit examines how compliant the software and hardware are with the HIPAA mandated ANSI standards and how compliant the organization is in following the standards. The HIPAA Security Rule involves technical, administrative, and physical security and all three are under the auspices of the secu-

rity person. Technical security involves the information technology security such as passwords. Administrative security involves having the policies and procedures for the HIPAA security Rule. Physical security involves ensuring that patient health information is secure in the physical environment such as having locked cabinets for storage of patient health information. The security person will also determine the employees who have a "need to know" and have role based access to patient health information; they must then undergo training and adhere to HIPAA policies. The Security Rule also mandates about developing a disaster recovery plan and routine back-ups for all electronic information. Facilities must identify a contingency plan to restore any loss of data and to identify safe storage locations such as an off-site mine. Disaster plan testing and recovery are to be performed.

The HIPAA Security Rule is more than information technology, but also how the employees interact and utilize PHI. To this end, a Computer Usage Policy, again based on the "need to know" principle, specifies how the information technology system is to be used in an organization. Computer workstations must be safeguarded such that unauthorized users cannot gain access. In addition the transfer of data must be protected. Employees also agree to certain restrictions such as not accessing information for personal gain, preventing others from using your system, and cooperating with audits and monitoring of technology usage.

Moreso, the Security Rule must become a part of daily operations through policies, procedures, and standard operating practices of all PHI, oral, written, and electronic, including social media. A covered entity's policies and procedures for electronic information systems that hold ePHI are to allow access only to those persons or software programs that have a role based need to know. A covered entity can meet the requirements by doing the following:

1. Require unique user identifications whereby the covered entity assign a unique name and/or number for identifying and tracking user identity.
2. Have emergency access procedures whereby a covered can obtain necessary ePHI during an emergency.
3. Consider using an automatic log-off such that the covered entity can terminate an electronic session after a predetermined time of inactivity.
4. Use encryption and decryption for ePHI [10]. (http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_049463.hcsp?dDocName=bok1_049463; Accessed October 18, 2014)

Thus far, the security topic has focused on protecting patient health information. But what happens when a facility no longer has to save the health information either as mandated by law or organizational policies and procedures? The answer lies in the destruction and disposal mandates for health information. When disposing of health information, one must ensure that the data is destroyed and cannot be resurrected. Simply removing it from the property or deleting computer files is not adequate. What are needed are strict mandates on the internal and external destruction of health information, and disposal of physical computers and health information. Keep in mind, because healthcare organizations may contract this task to an outside vendor, this vendor must also abide by HIPAA regulations. Here the outside vendor cannot use or disclose the patient health information. In addition, the vendor will use safeguards to

ensure that the patient health information is not disclosed during the destruction process, but if a disclosure does occur, the vendor will notify the facility immediately. If the vendor subcontracts to another agent, that agent must be known to this facility and must abide by the HIPAA regulations. Patient health information shall be permanently destroyed such that there is no possibility of reconstruction of the data. Paper records can be destroyed by burning, cross shredding, pulping, and pulverizing. Microfilm and microfiche can be destroyed by recycling and pulverizing. Magnetic data can be destroyed by degaussing [11]. A Certificate of Destruction must then be completed and retained by the organization.

As with the external destruction of health information, all patient health information that is to be internally discarded is to follow a procedure of destruction that will comply with the HIPAA regulation and ensure privacy, security, and confidentiality of all patient health information. Because patient health information is a component of normal business operations, the internal destruction policy mandates that the organization destroy patient health information that no longer has a business function and can rightfully be destroyed under law. Facilities can utilize shredders at the end of each shift or as the information to be destroyed has completed its business function.

The last measure of health information destruction is computer disposal, the actually physical hardware being rendered clear of all health information. Also included here is when a computer is moved and used by another person who does not have the same "need to know" privileges for health information as the former computer terminal user. When information is saved on a computer hard disk, the magnetic characteristics of that disk change in two ways. The first way is for the information that is stored on it (ie. the written file). The second way is for the address or the location of the file being stored on the magnetic disk; thus, the disk holds two identifying elements for each file stored. When a file is "deleted", the only part that is erased on the magnetic disk is the address or location. The information remains even though the disk is used over or formatted, the magnetic characteristics of the disk still hold the information and therefore it is accessible with certain technology tools. The only way to ensure that both the information and address are removed (i.e. change the magnetic characteristics back to their original format) is to overwrite the disk with specific technology tools. Previously DoD 5220.22-M was the standard to follow for data overwrite. But in 2006 and updated in 2012, this standard was replaced with SP800-88 for data erasure compliance for hard drives and other electronic media [12]. After the overwriting is completed, the computer will be dated and initialed as to when and who did the overwrite procedure. The information technology department is to also log the information.

25.4 Privacy

The HIPAA Privacy Rule is quite extensive and concerns itself with the use and disclosure of identifiable patient health information and seeks to maintain its confidentiality. The Privacy Rule encompasses protecting the privacy with business associates and users allowing patients to request to amend their medical records, and

receiving consent and authorization prior to sharing information. Providers must also publicize their information practices in a "Notice". All personnel who have access to patient health information must be trained on the requirements.

Similar to the Security Rule, the Privacy Rule goes beyond medical records per se as it also includes policies and procedures which impact one's standard operating procedures. Healthcare providers must designate a privacy officer. This person will be responsible for implementing the safeguards to maintain the confidentiality of the information. In addition, they will be the person who performs routine audits and investigates any breaches of privacy and ultimately disciplines those who have committed the breech. The breaches can surface in multiple manners such as through an anonymous complaint line, direct patient or family member complaints, or through the audits. It is the HIPAA Privacy personnel working in concert with the security personnel to protect the covered entity from breaches. Risks must constantly be assessed and measures in place to respond. What is the impact of the risk and what is the probability of occurrence? Although with PHI, all occurrences are problematic, although it is mitigated as all are not a critical risk.

Risks impact the patient, but they do not see it upfront. Other areas of the Privacy Rule have direct impact on patients. For example, patients are able to request to amend their medical records on information that they feel does not represent their health encounter. The key here is that they can make a request which will then be considered, but it does not guarantee that the change will take place. The patient would contact the author of the medical note and request that a change be made and also submit what the wording for the change should be. The provider or a committee will consider the request and make a ruling. With HIPAA as specified in the HIPAA Notice of Privacy Practices is that it is a patient right to be able to request an amendment as the data belongs to the patient. One of the most heralded parts of the HIPAA Privacy Rule is the Right to Request to Inspect, Copy, and Amend Medical Records section. In fact, one of the main purposes of HIPAA from a consumer's perspective is the right to view and possibly amend their record. The physical medical record belongs to the provider, but what is not known by many, is that the information contained within belongs to the individual; therefore under State Privacy Laws, patients have had the right to examine their medical records. HIPAA corroborates that an individual has a right to **request** to inspect, copy, and amend their medical record in most circumstance. Exceptions to this are psychotherapy notes, information to be used in legal proceedings or for forensic matters, information that could cause harm to oneself or another especially when inmates are involved, research information when a patient is in the sample, and if the requestor is judged that they may be further harmed by having seen the information [13].

The facility has the requesting party complete a request form and validate their identification. The request form will ask the patient what needs to be amended, why, and what the new wording should be. The healthcare facility must rule on the matter in a timely manner. If the request is denied, the patient can appeal whereby the facility will have an additional 30 days to further review the case. If the request to amend the record is granted, the healthcare facility will inform the requestor that the amendment was granted, then insert the amended language next to the changed

language. The amendment must then be shared with all those who have a "right to know" about the changed language. If the healthcare provider denies the request to amend the record, a written statement in laymen's term of the reason for denial is given to the requestor. The requestor can then counter in writing a statement of disagreement. If it is again denied, the facility must alert the requestor that they can further appeal to the Secretary of Health and Human Services and the facility's complaint line. Also, the facility must make known in the medical record the denied request with any future disclosures of the patient health information.

As introduced above with the request to amend a record, organizations are to issue the Notice of Health Information Practices (Notice). The notice describes how health information about an individual may be used and disclosed and how one can get access to this health information. Many people are already knowledgeable of the fact that health information is shared with insurers and other health care facilities/providers for treatment decisions and payment. The Notice though covers many other areas related to those that have an interest, for business purposes, in one's health information. Facility departments, such as risk management and quality assurance receive information to analyze the care, treatment, and outcomes of procedures and tests. This health information is used to continually improve the care by analyzing best practices. Information can be extrapolated by physician, procedure, or demographic characteristic. Health care facilities also maintain a directory used by visiting predominantly by clergy. Patients can opt out of being in the directory by stating such prior to signing the notice. Business associates such as pharmacies, medical equipment vendors, and medical laboratories receive patient health information. Business associates must follow HIPAA standards and certify that in writing to the healthcare facility. In the Omnibus Final Rule issued September 23, 2013, business associates needed HIPAA training and must follow the HIPAA policies just as a covered entity does. In teaching hospitals and academic medical centers, health information may be disclosed to researchers if they have appropriate consent forms and the research has been approved by an institutional review board. The researchers will be held to the facility's health information privacy standards and verify that the data being requested is truly needed to accomplish the research objectives. Funeral directors will receive health information in accordance with State laws and for professional purposes only. Consistent with applicable laws, health information may be disclosed to organ procurement organizations or organizations involved in the transplantation of and related services for organs, tissue donation, and transplant [14]. Patient health information being used for marketing has been an area of controversy. Health information can be disclosed to remind patients about treatments and services that may benefit them given their medical condition, but patient data cannot be used for marketing purposes without patient consent. Federal Government agencies, such as the Food and Drug Administration, may be required to disclose health information related to a food recall or outbreak of a food related condition. State Government agencies such as workman's compensation will share health information as it becomes necessary by law and to render a decision on a compensation case. The Federal and State Governments may require health information to be disclosed for public health purposes such as for communicable disease

tracking and injury prevention. The Notice specifies, in general, to whom health information can be disclosed to and for what purpose.

An ever increasing challenge for HIPAA is the mobility of data both with portable devices and personnel working from remote locations. It is reported that one-third of healthcare personnel work outside of the healthcare entity at least once per week. In concert with this, 78 % of records breached in security incidents were attributed to stolen or lost mobile devices and 39 % of healthcare security incidents are caused by a stolen and/or lost device [15].

To mitigate issues with mobile devices, organizations can employ several strategies. First, in your information systems strategic plan and disaster plan, know the risks of these devices and plan how they will be used with patient health information. If they are being used to transmit data to external networks, consider that in your information technology risk assessment and HIPAA technical security policies. Develop and manage policies regarding mobile devices. For example, can one use a personal mobile device within the organization. Are there any restrictions on using a mobile device issued by the organization? Ensure that the policies are enforced and make this a routine part of a HIPAA audit [16].

The authors of the Health Insurance Portability and Accountability Act wanted to ensure that providers would not simply put HIPAA in place and then forget about it. Rather, the authors wanted HIPAA to be operationalized into a provider's daily operations. To do such, they required that an organization institute operational audits, a reporting mechanism, and discipline procedures. Operational audits are an evaluation mechanism to measure compliance with the stated policies and regulations of HIPAA. The Compliance Officer and staff will conduct monthly (or more frequent) audits on various measures such as computer logins, medical record documentation, coding and billing, adherence to confidentiality policies, adherence to security policies, HIPAA training for employees, and a review of personnel access to patient health information. These, among others, will be conducted to assess system weaknesses such that corrective action can be taken to ensure that HIPAA is being adhered to. Audits can be announced or unannounced, but predominantly they will become a part of the facility's operations such that employees will see them as a part of routine business. If the audits detect problems, then an action plan must be specified on how to reeducate the affected employee(s) and/or department(s). Second, the employee(s) and/or department(s) must be re-audited. Even if on the next audit, there is not a problem, one must continue to routinely re-audit them such that a problem does not reoccur. All of this must be documented on the audit forms. If the facility fails to reeducate and re-audit, or fails to document it, they can be held liable for not correcting a situation that they were aware of [17].

Another way to detect non-adherence to HIPAA is via a reporting mechanism system. Here, employees and other constituents can confidentially report violations or suspected violations of HIPAA without retaliation. The facility must publicly advertise its reporting mechanism system in all of its locations. The reporting mechanism system can include a hotline telephone number, paper reporting system, or electronic reporting system. The most important criteria is that the reporting system must be conducive for all levels of employees to use. The employee and/or

constituent can only report violations or credible, suspected violations of criminal conduct in relation to HIPAA; thus, this is not a general complaint line. Employees must also know that HIPAA is a Federal mandate and false reporting can lead to a criminal penalty. The reporting system must maintain the confidentiality of the reporting individual and no retribution can be taken against the reporting individual. If the reporting individual tells of any retribution, the facility must document it and have a follow-up investigation immediately. When an employee or constituent files a complaint, the reporting mechanism call log is to be completed immediately. The complaint has a statute of limitations of 180 days. An initial investigation must begin immediately on the complaint with the action and response being documented. After the investigation is complete, follow-up must ensure that credible violations are not repeated. In addition, the facility must cooperate with any outside investigation including sharing records in a timely manner and allowing access to pertinent records [18]. As shown in Table 25.1, complaints and follow-up have increased exponentially since HIPAA began, but it is this due diligence that is required to protect patient health information.

When operationalizing HIPAA, a covered entity is to develop and implement a disciplinary system for HIPAA violations. With this, all breaches must be fully investigated and if warranted disciplinary measures taken, including termination from and non-rehire to the organization. Disciplinary measures are taken on those who violate the HIPAA mandate and those who are responsible to monitor, detect, and report an offenses, but fail to do so; therefore covering acts of commission and omission.

All breaches and sanctions in violation of HIPAA must be clearly documented and substantiated. During the investigation, as warranted by the compliance person, the employee(s) under investigation can be moved to another position whereby access to patient health information is not warranted. If the investigation reveals a

Table 25.1 Enforcement results by year

Year	No violation		Resolved after intake and review		Corrective action obtained		Total resolutions
Partial year 2003	79	5 %	1,177	78 %	260	17 %	1,516
2004	360	7 %	3,406	71 %	1,033	22 %	4,799
2005	642	11 %	3,888	68 %	1,162	21 %	5,692
2006	897	14 %	4,128	62 %	1,574	24 %	6,599
2007	727	10 %	5,017	69 %	1,494	21 %	7,238
2008	1,180	13 %	5,940	63 %	2,221	24 %	9,341
2009	1,211	15 %	4,749	59 %	2,146	26 %	8,106
2010	1,529	17 %	4,951	54 %	2,709	29 %	9,189
2011	1,302	16 %	4,466	53 %	2595	31 %	8,363
2012	979	10 %	5,068	54 %	3,361	36 %	9,408
2013	993	7 %	9,837	69 %	3,470	24 %	14,300

Source: Department of Health and Human Services. Office for Civil Rights. Enforcement Results by Year. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/historicalnumbers.html

violation of civil or criminal, federal or state law, the violation must be reported to Government authorities immediately. If the investigation reveals an overpayment to a facility, the overpayment must be returned immediately. Organizations must then discipline the individual according to their chain of discipline. For example, individuals who use health information for malice, personal gain, and or intimidation can be terminated. Breaches which involve accessing patient health information not related to one's job responsibilities can be suspended without pay for 3 weeks, be put on a 90 working day probationary period, and undergo HIPAA training. A second offense can result in immediate termination. Organizations will need to determine if their present discipline procedures are stringent enough for the violation of health information privacy.

HIPAA violations need not occur if the organization develops a "culture" to adhere to HIPAA by all employees. This can occur through orientation sessions, email reminders, staff meetings, payroll reminders, and diligence among all employees.

25.5 Summary

The keys for compliance to the Health Insurance Portability and Accountability Act is to operationalize it into the organization's daily functions and to be very current on changes. In fact, know of proposed changes and enter into the public comment foray. HIPAA must be integrated to not only protect information, but also to deliver quality health care when data are needed. With so much in healthcare depending on accurate data and information, the protection of those data and information are paramount.

References

1. Department of Health and Human Services. News release. http://www.hhs.gov/news/press/2014pres/05/20140507b.html. Accessed 7 May 2014.
2. Department of Health and Human Services. HIPAA security series. Volume 2, paper 1, March 2007. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf.
3. Robert Tennant and Amy Nordeng. New privacy and security omnibus rule released. MGMA connexion, Apr 2013, page 18 of 18–21.
4. The Wall Street Journal. Home depot's 56 million card breach bigger than target's.http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571. Accessed 18 Sept 2014.
5. Department of Health and Human Services. HIPAA final rule, 45CFR164.402. 25 Jan 2013.
6. Downing K. Navigating a compliant breach management process. J AHIMA. 2014;85(6): 56–8.
7. US Department of Health and Human Services. Massachusetts provider settles HIPAA case for $1.5 million. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement.html. Accessed 20 Apr 2015.

8. US Department of Health and Human Services. Alaska DHSS settles HIPAA security case for $1,700,000. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/alaska-agreement.html. Accessed 20 Apr 2015.
9. US Department of Health and Human Services. Data breach results in $4.8 million HIPAA settlements. 2014, May 7. http://www.hhs.gov/news/press/2014pres/05/20140507b.html. Accessed 21 Apr 2015.
10. AHIMA. Mobile device security (updated). J AHIMA. 2012;83(4):50–5. http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_049463.hcsp?dDocName=bok1_049463. Accessed 20 Apr 2015.
11. Office for Civil Rights. The HIPAA privacy and security rules. Frequently asked questions about the disposal of protected health information. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdf
12. Department of Defense Media Sanitization Guidelines 5220.22 M. http://www.destructdata.com/dod-standard/
13. Department of Health and Human Services. Standards for privacy of individually identifiable Health Information. 45CFR164.508.
14. Office for Civil Rights. Understanding the HIPAA notice. http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/understanding-hipaa-notice.pdf
15. Sherman C, Shey H, with Balaouras S, Duong, J. Brief: stolen and lost devices are putting personal healthcare information at risk. Forrester Res. 2014:3.
16. Department of Health and Human Services. Managing mobile devices in your health care organization. http://www.healthit.gov/sites/default/files/fact-sheet-managing-mobile-devices-in-your-health-care-organization.pdf
17. HIPAA Privacy, Security, and breach notification audit program. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/
18. Department of Health and Human Services, Office of the Secretary. Standards for privacy of individually identifiable health information. 45 CFR 160.306(b)(3).