Chapter 6
EHR, The Laws and Limits of the Laws

Egondu R. Onyejekwe

Abstract Electronic health records are subject to several laws and regulations at the federal and state level in the United States. HIPAA privacy and security rules set the floor when it comes to assuring the privacy and security of health information at the national level. While such regulations provide a good structure for single healthcare entities or covered entities, they lack flexibility or specificity when it comes to health information environments that may not be proprietary-based. As portable health records evolve, the information will be crowdsourced and managed collectively, which brings up new privacy and security concerns and challenges.

Keywords HIPAA · Privacy rule · Security rule · Electronic health records · HITECH Act · Privacy and security · Health information privacy · Health information security

6.1 Introduction

Dealing with proprietary data and the vendor hold of Electronic Health Records, in a fragmented marketplace, is further complicated by the law(s). There are essentially, three laws in the United States that relate to healthcare, and specifically to electronic healthcare. They include the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Wikipedia 2018); The American Reinvestment & Recovery Act (ARRA) that was enacted on February 17, 2009 (HealthIT 2009); and a subset of ARRA—the Health Information Technology for Economic and Clinical Health (HITECH) Act (HealthIT 2009) and others that include many measures to modernize the US infrastructure. The HITECH Act specifically supports the concept of electronic health records—The HITECH Act set meaningful use [EHR-MU], of interoperable EHR adoption in the health care system as a critical national goal (HealthIT 2009). It also incentivized EHR adoption since includes

E. R. Onyejekwe (✉)
Public Health, Health Administration, College of Health Sciences, Walden University, Minneapolis, MN, USA
e-mail: Egondu.onyejekwe@mail.waldenu.edu

E. R. Onyejekwe et al. (eds.), *Portable Health Records in a Mobile Society*, Health Informatics, https://doi.org/10.1007/978-3-030-19937-1_6

both the adoption of EHR as well as the "meaningful use" (HealthIT 2009) of EHR. That is, the use of EHR by providers to achieve significant improvements in care! The effort was led by Centers for Medicare & Medicaid Services (CMS) and the Office of the National Coordinator for Health IT (ONC). This whole idea has been obfuscated by the notion of portable health records which currently are in dispersed and in distributed environments. The implications are discussed later in this chapter.

In any event, this chapter is devoted to the most relevant of the health laws—The landmark piece of legislation in the United States is the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The intent was to "simplify the administration of healthcare, eliminate wastage, prevent healthcare fraud, and ensure that employees could maintain healthcare coverage when between jobs (HIPAA Journal 2018)." The Health Insurance Portability and Accountability Act (HIPAA) of 1996, was enacted by Congress primarily to protect the confidentiality of a person's medical information (Wikipedia 2018). HIPAA therefore, sets boundaries on the use and release of health records as well as, establishes the safeguards to protect the privacy of health information. Despite all its bells and whistles HIPAA addresses the issues required for portable health records (U.S. Department of Health and Human Services 2018).

6.2 HIPAA Overview

"The *Health Insurance Portability and Accountability Act of 1996* (*HIPAA*; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996) was enacted by the United States Congress and signed by President Bill Clinton in 1996. It has been known as the Kennedy–Kassebaum Act or Kassebaum–Kennedy Act after two of its leading sponsors (Wikipedia 2018)." The Act consists of five Titles, each of which covers a different topic.

Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs (Wikipedia 2018). Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers (Wikipedia 2018).

Title III sets guidelines for pre-tax medical spending accounts (Wikipedia 2018). Title IV sets guidelines for group health plans (Wikipedia 2018), and Title V governs company-owned life insurance policies (Wikipedia 2018).

HIPAA covers both individuals and organizations and those who must comply with HIPAA are called HIPAA-Covered entities (U.S. Department of Health and Human Services 2018). Covered Entities, Business Associates, and PHI. In general, the protections of the Privacy Rule apply to information held by covered entities and their business associates (U.S. Department of Health and Human Services 2018). According to HIPAA, covered entities are: health plans; clearing houses; a health

care provider that conducts certain standard administrative and financial transactions in electronic form; and health associates (U.S. Department of Health and Human Services 2018).

Briefly, HIPAA-covered entities thus, include:

- Health plans: Among these are, Health insurance companies, HMOs, or health maintenance organizations, Employer-sponsored health plans, Government programs that pay for health care, like Medicare, Medicaid, and military and veterans' health programs (U.S. Department of Health and Human Services 2018)
- Clearinghouses, and certain health care providers: Clearinghouses include organizations who on behalf of other organizations, process nonstandard health information to conform to standard data content or format, or vice versa (U.S. Department of Health and Human Services 2018)
- Providers are those who electronically submit HIPAA transactions such as claims. Such providers include, but are not limited to: Doctors; Clinics; Psychologists; Dentists; Chiropractors; Nursing homes and Pharmacies (U.S. Department of Health and Human Services 2018)
- Business Associate—this is a person whom a covered entity engages to help carry out its health care activities and functions. The covered entity must formalize the relationship through a written contract with the business associate or have other arrangement with the business associate that: establishes specifically what the business associate is required to do; and requires the business associate to comply with HIPAA. Included in the business associate's lists are: third-party administrator that assists a health plan with claims processing; consultant that performs utilization reviews for a hospital; health care clearinghouse that translates a claim from a nonstandard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer and an independent medical transcriptionist that provides transcription services to a physician (U.S. Department of Health and Human Services 2018)

Also, a covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity (U.S. Department of Health and Human Services 2018).

However, of the five titles, HIPAA Title II is the most relevant to this discourse because it relates to *Privacy* (Wikipedia 2018). The overarching goal of Title II though, is Preventing Healthcare Fraud and Abuse (Wikipedia 2018). Title II contains five rules. The Five Rules of HIPAA Title II include:

1. Privacy Rule
2. Transactions and Code Sets Rule
3. Security Rule
4. Unique Identifiers Rule
5. Enforcement Rule (Wikipedia 2018)

Of these the first—Privacy Rule—and the third—Security Rule—are most relevant for our discussions. The essence of title II of HIPAA which addresses the

Privacy Rule, is to protect most "individually identifiable health information" (U.S. Department of Health and Human Services 2018) that is either held or transmitted by a covered entity or its business associate.

These can be "in any form or medium, whether electronic, on paper, or oral (U.S. Department of Health and Human Services 2018)." Therefore, the Privacy Rule addresses this as Protected Health Information (PHI), which under the US law includes information that can be linked to an individual through any of the following: any information about health status; Information regarding the provision of health care; or information about the payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity) (U.S. Department of Health and Human Services 2018).

So, included in the PHI is demographic information, which relates to:

- The individual's past, present, or future physical or mental health or condition
- The provision of health care to the individual or
- The past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Many of the common identifiers of PHI that can be associated with the information above include name, address, birth date, and Social Security Number (U.S. Department of Health and Human Services 2018)

As a consequence, all these—a medical record, laboratory report, or hospital bill—would be PHI because each document would contain a patient's name and/or other identifying information associated with the health data content. Despite all the provisions of the law, HIPAA violations (both privacy and security) are real and common (U.S. Department of Health and Human Services 2018).

By contrast, aggregated data, albeit, compiled from individual health records would not qualify as a PHI. For example, a health plan report that only noted the average age of health plan members as 45 years would not be PHI. Although such a report could have aggregated individual plan member record, no specific individual can be identified.

It is also important to assess the relationship with health information. PHI does not include simply identifying information, such as personal names, residential addresses, or phone numbers. A good example is a phone book, information that is already reported as part of a publicly accessible data source, would not be PHI since it is not related to heath data. Where however, such information would become a PHI is where it was listed with a health condition, health care provision or payment data, with indication that the individual was treated at a certain clinic.

6.3 De-identification and Its Rationale

There has been a preponderance of the adoption of health information technologies in the United States to combine large, complex data sets from multiple sources in order to facilitate research and or yield beneficial results. The enactment of the process of de-identification, which enables the removal of identifiers from the health

information, mitigates privacy risks to individuals and thereby supports the secondary use of data. These allow for comparative effectiveness studies, policy assessment, life sciences research, and other endeavors!

De-identification of portable health records allows public health professionals and healthcare researchers to conduct epidemiological analysis and clinical investigation with aggregated portable records without compromising the privacy of the participants. The movement to portable records will significantly reduce the size of, or eliminate, consolidated storage of records. These large accumulations of records are used by public health professionals to identify and predict health trends and by researchers to eliminate or control disease. To ensure that these valuable assets are not lost in the march to portable records we must develop standard de-identification processes that can process large numbers of portable records and produce analytical and research databases so that these professionals can continue to work toward improving general health and wellbeing of humankind.

While the Privacy Rule was designed to protect individually identifiable health information through permitting only certain uses and disclosures of PHI provided by the Rule, or as authorized by the individual subject of the information, exceptions are made. One exception is through de-identification (U.S. Department of Health and Human Services 2015a). In recognition of the potential utility of health information even when it is not individually identifiable, §164.502(d) of the Privacy Rule permits a covered entity or its business associate to create information that is not individually identifiable to apply the de-identification standard and implementation specifications in §164.514(a)–(b) (U.S. Department of Health and Human Services 2015a). These provisions allow the entity to use and disclose information that neither identifies nor provides a reasonable basis to identify any particular individual (U.S. Department of Health and Human Services 2015a).

The Privacy Rule provides two de-identification methods:

1. A formal determination by a qualified expert (U.S. Department of Health and Human Services 2015a); or
2. The removal of specific individual identifiers as well as absence of actual knowledge by the covered entity that the remaining information could be used alone or in combination with other information to uniquely identify individuals (U.S. Department of Health and Human Services 2015a). Both methods, even when properly applied, are not foolproof and may yield de-identified data that retains some risk of identification. While the risk is minimal, it is still not zero, the potential for the linking of de-identified data back to the identity of the patient to which it corresponds exists. In any event, and independent of the method, the Privacy Rule does not restrict the use or disclosure of de-identified health information, it is no longer considered protected health information (U.S. Department of Health and Human Services 2015a).

In conclusion, Privacy Rule, while seemingly complex, can be whittled down to these two basics: consent and disclosure. The use of PHI is restricted to six areas: when disclosed to the individual; for treatment, payment and operations; when permission is given; when used incidentally; in benefit of public interest; and when personally-identifiable information has been removed.

6.4 Security Rule

Security Rule is best understood as it relates to the Privacy Rule. The difference is that, while the Privacy Rule impacts all forms of PHI, the Security Rule specifically pertains to PHI stored electronically (ePHI) (U.S. Department of Health and Human Services 2018).

6.4.1 General Security Rules

The general tenets of the Security Rule require covered entities to apply reasonable and appropriate safeguards for the protection of ePHI. The CMS's Decision tool is useful in determining who the Security Rule covered entities are (U.S. Department of Health and Human Services 2018).

Such entities apply to health plans, health care clearinghouses, and to any health care provider who transmits personally identifiable health information in electronic form. Such transmissions must be in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities") and to their business associates (U.S. Department of Health and Human Services 2018).

The safeguards are administrative, technical, and physical. Thus, entities must:

1. "Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by their workforce (U.S. Department of Health and Human Services 2018)"

According to the Security Rule, "confidentiality" means that ePHI is not available or disclosed to unauthorized persons and confidentiality requirements "support the Privacy Rule's prohibitions against improper uses and disclosures of PHI [4]." Furthermore, "integrity" under the Security Rule, means that ePHI is not altered or destroyed in an unauthorized manner, while "availability" means that ePHI is accessible and usable when an authorized person needs access to it (U.S. Department of Health and Human Services 2018).

Since HHS recognizes that the range of covered entities span the space between the smallest provider to the largest, multi-state health plan, the Security Rule is flexible and scalable enough to allow covered entities to analyze their own needs and implement solutions that are specific to them and that address their needs. For a covered entity the Rule, rather than dictate measures, requires the covered entity to consider (U.S. Department of Health and Human Services 2018):

- 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 (U.S. Department of Health and Human Services 2018).

Because the healthcare field is continuously changing, it behooves covered entities to also continuously review and modify their security measures protecting ePHI.

The Security Rule also, specifies requirements for safeguards where a HIPAA-covered entity uses ePHI. Those safeguards are broken into three part that include: administrative; physical and technical (U.S. Department of Health and Human Services 2018). Detailed steps are provided for entities in each of these areas.

6.4.2 Administrative Safeguards

Administrative safeguards entail a security management process where written privacy procedures are in place to cover authorization, establishment, modification and termination. This implies that a covered entity must not only identify and analyze potential risks to ePHI, but must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level. A covered entity must designate a security official who will be responsible for developing and implementing its security policies and procedures. Consistent with the "minimum necessary," aspect of the Privacy Rule, the Security Rule requires a covered entity to only implement policies and procedures for authorizing access to ePHI, when such access is appropriate, based on the user or recipient's role (role-based access). A covered entity must train all workforce members regarding its security policies and procedures, as well as provide for appropriate authorization and supervision of workforce members who work with ePHI. A covered entity must perform a periodic assessment of how its security policies and procedures meet the requirements of the Security Rule. They must also apply appropriate sanctions against workforce members who violate its policies and procedures (U.S. Department of Health and Human Services 2018).

6.4.3 Physical Safeguards

Physical safeguards emphasize both facility access and control—where a covered entity must simultaneously limit physical access to its facilities while ensuring authorized access to those thus categorized. Physical safeguards apply also to workstation and device security, where policies and procedures specify proper use of and access to both workstations and electronic media. Overall, physical safeguards require access controls, like security plans, maintenance records and visitor escorts. This includes policies and procedures that govern the transfer, removal, disposal, and re-use of electronic media. These will ensure appropriate protection of ePHI (U.S. Department of Health and Human Services 2018).

6.4.4 Technical Safeguards

Technical safeguards focus on access controls that include audit controls; integrity controls; and transmission security. The audit controls include software and or hardware procedures that record and examine access plus other activities in the information systems containing or using ePHI. The integrity controls allow a covered entity to implement policies and procedures that ensure integrity and retention of ePHI. Transmission security safeguards are those controls that guard against unauthorized access to ePHI as it is transmitted over an electronic network. All-in-all, technical safeguards lay out the requirements for use of cryptographic hash functions, data encryption and process documentation. A covered entity must therefore implement technical policies and procedures that would allow only authorized persons access to ePHI (U.S. Department of Health and Human Services 2018).

Time and space do not permit further discussion of other categories of the Security Rule, such as "addressable" and "required" implementation specifications, organizational, policy, procedural, and documentation requirements. Suffice it to state that the essential and pertinent parts of the Security Rule have been addressed. Noteworthy are the key elements of the Security Rule that address who is covered, what information is protected, and what safeguards must ensure appropriate protection and the security of ePHI, including the exporting of such information to other covered entities (U.S. Department of Health and Human Services 2018).

In the piece posted by the 2018 HIPAA Journal, it is hard to not conceive a day without HIPAA violation from either a hospital, health plan, or healthcare professional who is violating HIPAA (HIPAA Journal 2018). There are several and notable updates of HIPAA. They include the HIPAA Privacy Rule, HIPAA Security Rule, HIPAA Omnibus Rule, and the HIPAA Breach Notification Rule (HIPAA Journal 2018). HIPAA is discussed in relation to portable health record and while there are nuances and differences in the updated HIPAA list provided above, they all strive towards the same ends: improving privacy protections for patients and health plan members over the years simply to ensure healthcare data that is safeguarded and the that the privacy of patients is protected. Consequently, a HIPAA violation is a failure to comply with any aspect of HIPAA standards and provisions detailed in 45 CFR Parts 160, 162, and 164 (HIPAA Journal 2018). (These details are not very relevant here, while the violations are relevant.) For those interested in reading more, these are available in the combined text of all HIPAA regulations published by the Department of Health and Human Services Office for Civil Rights, which runs up to 115 pages and contains many provisions.

The concern here is the extraction from the many and hundreds of ways in which HIPAA Rules can be violated. Below is the list of the most common HIPAA violations provided by the 2018 HIPAA Journal (HIPAA Journal 2018):

- Impermissible disclosures of protected health information (PHI)
- Unauthorized accessing of PHI
- Improper disposal of PHI
- Failure to conduct a risk analysis

- Failure to manage risks to the confidentiality, integrity, and availability of PHI
- Failure to implement safeguards to ensure the confidentiality, integrity, and availability of PHI
- Failure to maintain and monitor PHI access logs
- Failure to enter into a HIPAA-compliant business associate agreement with vendors prior to giving access to PHI
- Failure to provide patients with copies of their PHI on request
- Failure to implement access controls to limit who can view PHI
- Failure to terminate access rights to PHI when no longer required
- The disclosure more PHI than is necessary for a particular task to be performed
- Failure to train employees on HIPAA Rules or the failure to provide security awareness training
- Theft of patient records
- Unauthorized release of PHI to individuals not authorized to receive the information
- Sharing of PHI online or via social media without permission
- Mishandling and mismailing PHI
- Texting PHI
- Failure to encrypt PHI or use an alternative, equivalent measure to prevent unauthorized access/disclosure
- Failure to notify an individual (or the Office for Civil Rights) of a security incident involving PHI within 60 days of the discovery of a breach
- Failure to document compliance efforts (HIPAA Journal 2018)

6.5 How HIPAA Violations Are Uncovered

Many of these HIPAA violations are discovered though internal audits by HIPAA-covered entities. These can come through supervisors who may have identified employees who have violated HIPAA Rules or directly from employees who often self-report HIPAA violations and potential violations by co-workers. The main enforcer of HIPAA Rules is the HHS' Office for Civil Rights (OCR). Also, it is the OCR that investigates complaints of HIPAA violations reported by healthcare employees, patients, and health plan members as well as investigates all covered entities who report breaches of more than 500 records and conducts investigations into certain smaller breaches. Additionally, OCR intermittently conducts audits of HIPAA covered entities and business associates. Also involved with the investigation of breaches and other HIPAA violations are the State attorneys general especially when reports of breaches of patient records are received (U.S. Department of Health and Human Services 2003; U.S. Department of Health and Human Services 2016; U.S. Department of Health and Human Services 2015b; Andrulis 2010; U.S. Department of Health and Human Services 2007).

6.5.1 *The Penalties for Violations of HIPAA Rules*

The penalties for violations of HIPAA Rules vary—from where State attorneys general can issue high fines and fines that range up to a maximum of $25,000 per violation category, per calendar year; to where OCR can issue fines of up to $1.5 million per violation category, per year. Also, Multi-million-dollar fines can be—as well as have been—issued.

For individuals, there are also potential fines for violating HIPAA Rules and sometimes criminal penalties have been appropriate. Individuals may earn jail terms for violating HIPAA, with some violations carrying a penalty of up to 10 years in jail! Furthermore, healthcare providers, health plans, and business associates of covered entities can also be fined. While more about the penalties for HIPAA violations on this page are available, the 2018 HIPAA Journal (HIPAA Journal 2018) presented the infographics in Figs. 6.1, 6.2, and 6.3 below for a more detailed depiction of recent HIPAA violation penalties and the HIPAA penalty structure.

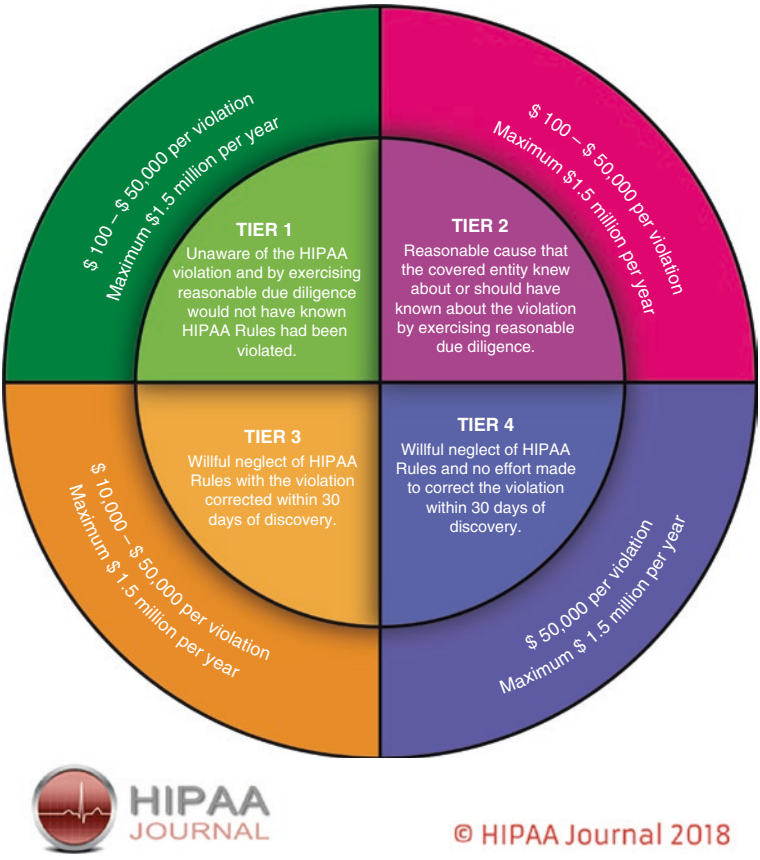

Fig. 6.1 HIPAA violation penalties. Reproduced from HIPAA Journal (2018)

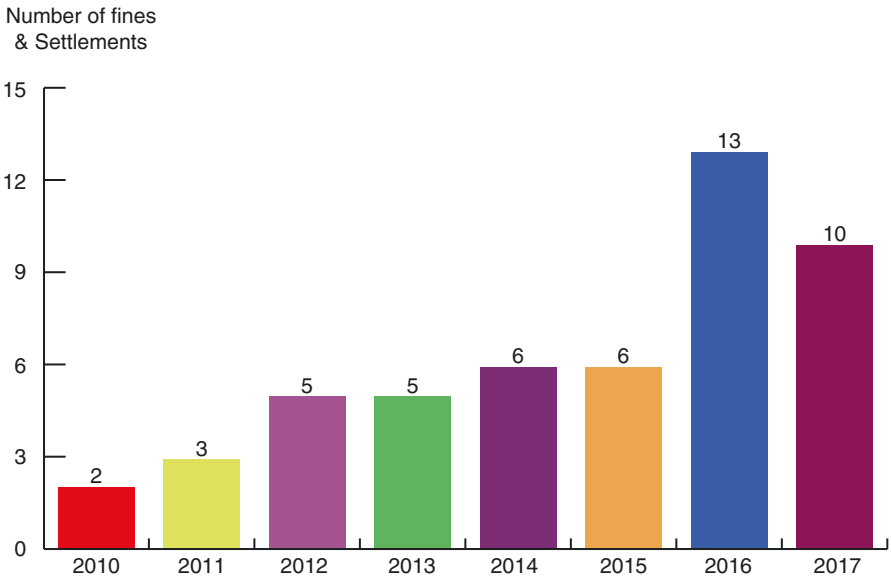

Fig. 6.2 HIPAA fines and settlements (2010–2017). Reproduced from HIPAA Journal (2018)

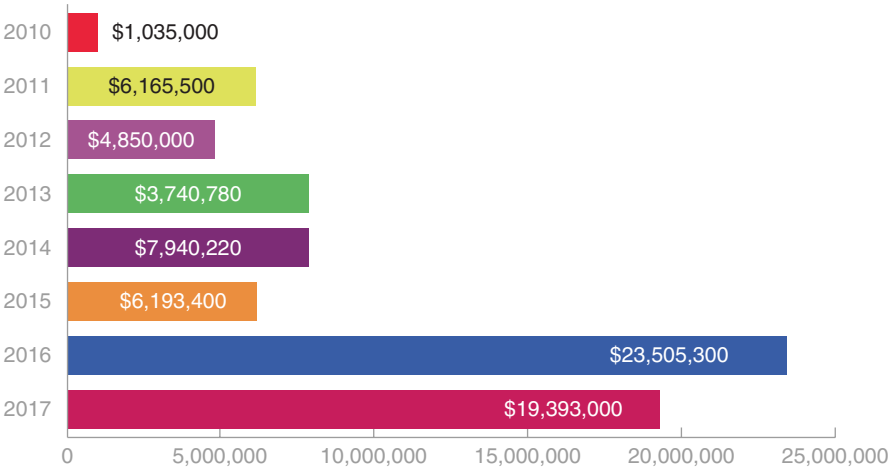

Fig. 6.3 Healthcare organizations made to pay for HIPAA violations. Reproduced from HIPAA Journal (2018)

6.6 HITECH ACT: Subtitle D—Privacy

6.6.1 Part 1: Improved Privacy Provisions and Security Provisions

On November 30, 2009, the regulations provided by Subtitle D, and associated with the enhancements to HIPAA enforcement took effect. These enhancements, although related to privacy, embellished HIPAA.

When data breaches affect 500 or more people, the HITECH Act Subtitle D, requires entities covered by HIPAA to report such breaches to the United States Department of Health and Human Services (HHS), to the news media, and to the people affected by the data breaches. This Subtitle D also extends the liability for the complete Privacy and Security Provisions of HIPAA to the business associates of covered entities, thereby including the extension of updated civil and criminal penalties to business associates. Covered entities are also, required to include these in any business-associate agreements among them (U.S. Department of Health and Human Services 2007).

An additional significant change heralded by Subtitle D of the HITECH Act are new breach notification requirements, that impose new notification requirements on covered entities, business associates, vendors of personal health records (PHR) and related entities if a breach of unsecured protected health information (PHI) occurs. The HITECH Act required both the HHS and the Federal Trade Commission (FTC) to issue regulations associated with the new breach notification requirements. The HHS, on April 27, 2009, issued guidance on how to secure protected health information appropriately. On August 24, 2009, the HHS rule was published in the Federal Register and on August 25, 2009, the FTC rule was published there as well (HealthIT 2009).

A final and significant change made to HIPAA in Subtitle D of the HITECH Act is noteworthy, as it implements new rules for the accounting of disclosures of a patient's health information. The current accounting for disclosure requirements for information used to carry out treatment, payment and health care operations when an organization is using an electronic health record (EHR) became extended. This simultaneously limited the timeframe for the accounting to 3 years instead of its previous 6 years. These changes took effect differentially depending on when organizations were implementing their EHRs (HIPAA/HITECH 2012):

- January 1, 2011, for organizations implementing EHRs between January 1, 2009 and January 1, 2011, and
- January 1, 2013, for organizations who had implemented an EHR prior to January 1, 2009 (HIPAA/HITECH 2012)

HHS, on July 14, 2010, issued a rule that listed categories that included 701,325 entities and 1.5 million business associates who would have access to patient information without patient consent after the patient had given general consent to their medical practitioner's HIPAA release (HIPAA/HITECH 2012).

6.7 HIPAA/HITECH Implications for Portability

HIPAA regulations, is the first in the Healthcare industry to provide accepted set of security standards or general requirements for protecting health information. However, and simultaneously, new technologies were evolving, and the healthcare industry began to discontinue processes and rely more heavily on the use of electronic information systems for services such as the payment of claims, answer eligibility questions, provide health information a variety of other administrative and clinically based functions. As indicated earlier, HITECH proposed the *meaningful use of interoperable electronic health records* throughout the United States healthcare delivery system as a critical national goal (Centers for Medicare & Medicaid Services 2010). Meaningful Use itself is defined by the use of certified EHR technology in a meaningful manner (HealthIT 2015). (An example of meaningful manner includes electronic prescribing). Meaningful use also is defined to ensure that the certified EHR technology is connected in a manner that provides for the electronic exchange of health information (HealthIT 2015). Such an exchange should improve the quality of care. Finally, the provider who uses the certified EHR technology must submit to the Secretary of Health & Human Services (HHS) some pertinent information on quality of care and other measures. In summary, the concept of meaningful use rested on the "5 pillars" of health outcomes policy priorities that include (Centers for Disease Control and Prevention 2017):

1. Improving quality, safety, efficiency, and reducing health disparities
2. Engage patients and families in their health
3. Improve care coordination
4. Improve population and public health
5. *Ensure adequate privacy and security protection for personal health information* (Centers for Disease Control and Prevention 2017)

Current Healthcare industry providers, for example, use electronic information systems for clinical applications such as computerized physician order entry (CPOE) systems, electronic health records (EHR), and radiology, pharmacy, and laboratory systems. Health plans provide access to claims and care management, among other applications.

So, portable health records would imply, on the surface, that the medical workforce would be more mobile and more efficient. For example, physicians can check patient records and test results from their location(s). However, a byproduct of the rise in the adoption rate of these technologies is the risk of compromising patient's privacy as well as the potential increases in security risks. A current portable health record does not ensure the adequate privacy and security protection for a person's health record or information because it lies in a distributed environment. This is compromised also because systems so distributed do not allow interoperability of the health records.

This offsets the Security Rule that was designed to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies

towards improving the quality and efficiency of patient care. Additionally, the healthcare marketplace is diverse, and has great implications for mitigating against both the Security Rule whose design intent allowed for flexibility and scalability. The intent was to allow a covered entity "to implement policies, procedures, and technologies that are appropriate for the entity's particular size, organizational structure, and risks to consumers' e-PHI." Therein lies another problem, as each organization would pursue a route that serves its particular purpose.

6.8 Conclusion

True that both HIPAA and HITECH did establish privacy practices for organizations. The nagging questions remain: Can regulations (HIPAA/HITECH) be supported in electronic health record systems that are no longer proprietary-based? In the era of portable health records, the information will be crowdsourced and will (should be) managed collectively. So, it will no longer be managed by entities and or individual organizations. As these individual organizations grow to meet their needs, so grows the problem of privacy and security of electronic health records. Because, the portable health records will, by definition, be crowdsourced, no single custodian (organization) can be held responsible for the security and privacy of the patient record! This means that the (portable) record itself must be inherently secure! Otherwise, access to the records will then be controlled by people who would lack the knowledge and skill needed to maintain the privacy previously required of entities, who were also held accountable to breaches of privacy and security. For health records to be portable, therefore, the implication is that new regulations will have to evolve simultaneously with suitable technologies like Blockchain (distributed ledger). The distributed ledger will support processes like prescriptions to be added to a personal secure health record by any authorized prescribing authority while at the same time maintaining the integrity and the security of the independent and portable health record. At the core remains the management of individual privacy and the security of their health information. Several pertinent questions remain. Who would be responsible for these—privacy and security of patient's portable electronic health record/s? The US Federal government? The state and local governments? Selected and independent organizations? The patient? A patient's agent? Or a mandated electronic health record broker?

References

Andrulis D. Patient protection and Affordable Care Act of 2010: advancing health equity for racially and ethnically diverse populations. 2010. http://www.jointcenter.org/research/patient-protection-and-affordable-care-act-of-2010-advancing-health-equity-for-racially-and. Accessed 27 Jan 2018.

Centers for Disease Control and Prevention. Meaningful use. 2017. https://www.cdc.gov/ehrmeaningfuluse/introduction.html. Accessed 27 Jan 2018.

Centers for Medicare & Medicaid Services. Secretary Sebelius announces final rules to support meaningful use of electronic health records. 2010. https://www.cms.gov/Newsroom/MediaReleaseDatabase/Press-releases/2010-Press-releases-items/2010-07-13.html. Accessed 27 Jan 2018.

Centers for Medicare & Medicaid Services. Are you a covered entity? 2016. https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html. Accessed 27 Jan 2018.

HealthIT. Index for excerpts from the American Recovery and Reinvestment Act (ARRA) of 2009. 2009. https://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra_with_index.pdf. Accessed 27 Jan 2018.

HealthIT. Meaningful use definitions and objectives. 2015. https://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives. Accessed 27 Jan 2018.

HealthIT Security. Why HIPAA privacy and HIPAA security rules are needed. 2018. https://healthitsecurity.com/news/why-hipaa-privacy-and-hipaa-security-rules-are-needed. Accessed 27 Jan 2018.

HIPAA Journal. 2018. https://www.hipaajournal.com/. Accessed 27 Jan 2018.

HIPAA/HITECH enforcement action alert. 2012. https://www.morganlewis.com/pubs/eb_lf_hipaaenforcementactionalert_21mar12. Accessed 27 Jan 2018.

U.S. Department of Health and Human Services. Unequal treatment: what healthcare providers need to know about racial and ethnic disparities in healthcare. 2003. http://www.nationalacademies.org/hmd/~/media/Files/Report%20Files/2003/Unequal-Treatment-Confronting-Racial-and-Ethnic-Disparities-in-Health-Care/Disparitieshcproviders8pgFINAL.pdf. Accessed 27 Jan 2018.

U.S. Department of Health and Human Services. The power to reduce health disparities: voices from reach communities. 2007. https://stacks.cdc.gov/view/cdc/12109/. Accessed 27 Jan 2018.

U.S. Department of Health and Human Services. 2015a. https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html Accessed 27 Jan 2018.

U.S. Department of Health and Human Services. HHS action plan to reduce racial and ethnic disparities: implementation progress report 2011–2014. 2015b. http://minorityhealth.hhs.gov/assets/pdf/FINAL_HHS_Action_Plan_Progress_Report_11_2_2015.pdf. Accessed 27 Jan 2018.

U.S. Department of Health and Human Services. National partnership for action to health disparities. 2016. http://www.minorityhealth.hhs.gov/npa/templates/browse.aspx?lvl=1&lvlid=5. Accessed 27 Jan 2018.

U.S. Department of Health and Human Services. Summary of the HIPAA security rule. 2018. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html. Accessed 27 Jan 2018.

Wikipedia. Health insurance portability and accountability act. 2018. https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act. Accessed 27 Jan 2018.