Patient Privacy: The Evolution of Protecting Health Information

Historical Professional Paper

Steven R. Davies, MS, MBA, CMPE, FACMPE

August 29, 2016

This paper is being submitted in partial fulfillment of the requirements of Fellowship in the American College of Medical Practice Executives.
Patient Privacy: The Evolution of Protecting Health Information

Introduction and Background

The privacy of a patient’s health information is now considered to be a fundamental part of the delivery, operations, and payment of healthcare. It is beyond argument that the delivery of medicine and healthcare in today’s society is infinitely more advanced in every aspect when compared to the earliest forms of healthcare. However, despite centuries of time and change, and monumental advances in medicine, healthcare delivery remains rooted in certain fundamental characteristics such as trust, confidentiality, and privacy (Ferguson, 2012; Higgins, 1989).

The advent of electronic health records (EHR’s) created amazing opportunities for efficiency in the sharing of health information for providers to make better informed clinical decisions, and for improved tracking of health information to manage the health of different populations (“History of HIPAA”, n.d.). However, EHR’s also created a new security threat to maintaining the privacy and confidentiality of patient health information. This security threat exposed vulnerabilities and risks to organizations that maintained electronic patient health information. Health information that was once maintained in a paper chart that was likely accessible only to a few was replaced with information stored on computer servers. Health information on computer servers meant information could be viewed by hundreds of people, and not always those that were authorized to access the information, as computer hackers with malicious intent could potentially access this data as well (Solove, 2013).

As health information became easier to create, maintain, and share electronically due to EHR technology, new laws and rules soon followed to require accountability by those using an EHR. Laws and rules such as the Health Insurance Portability and Accountability (HIPAA) Act, enacted in 1996, and the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted in 2009, offered guidance to healthcare entities regarding safeguarding
health information, defined expectations, and introduced oversight by the government (“HIPAA 101”, n.d.). As more healthcare entities adopted EHR technology, government oversight increased as well, with the focus being on patient privacy and the security of patient health information.

The maintenance of a patient’s privacy has been of importance for ages. It has evolved from a simple commitment by the healthcare provider to keep secret what they know about their patient, to an ideal maintained by professional healthcare providers, to a law enforced by the federal government (Ferguson, 2012). This professional paper, using the American Psychological Association (APA) 7th edition (2010) for formatting and citation of references, will provide a historical evaluation of the roots of privacy in healthcare delivery through an intensive review of the relevant literature available. This paper will begin with an overview of the key concepts of privacy and confidentiality, followed by information related to the importance of privacy. This paper will provide an extensive overview of the evolution of privacy over the years, and will explore what the future may hold for privacy in the delivery of healthcare in a time of major advances in technology information access and sharing. Professionals working in the healthcare sector that have a thorough understanding of how the role of privacy has evolved over time will be better equipped to lead the industry into the future.

**Defining and Understanding Key Concepts of Privacy**

Privacy is an interesting subject with which every individual has a very personal definition and a different expectation. A challenge presented with the subject of privacy is that there is no universally accepted, fundamental definition for it (Institute of Medicine [IOM], 2009). It is generally understood by most that there is a clear connection between the subjects of privacy, confidentiality, and security. However, to fully grasp the role and evolution of privacy in
the area of healthcare, it is essential to first define and better understand the key concepts associated with privacy, including confidentiality, security, and protected health information.

**Privacy**

A fundamental understanding of what privacy is and how it is defined is imperative for better understanding the evolution of privacy and its relevance and role in healthcare. The word privacy is deeply rooted in time and as such has become a challenge to define, adopting different meanings for different people, as it is often viewed from a personal perspective (IOM, 2009). With regard to health information, privacy is used to address which individuals or organizations should have access to a person’s personal health information (PHI) and the conditions under which access is permitted or should be permitted (IOM, 2009). Basically, who has access to protected health information and for what reason do they have access. The National Committee on Vital and Health Statistics defines privacy, with regard to health information, as “an individual’s rights to control the acquisition, uses, or disclosures of his or her identifiable health data” (2006, Definitions section, para. 1). While privacy is not outlined as a basic right within the U.S Constitution, with respect to privacy rights in healthcare the laws are quite clear (Prater, 2014).

**Privacy versus Confidentiality**

The words privacy and confidentiality, while used interchangeably quite often in writing and speaking, are found to have separate and distinct meanings when applied to law and to healthcare. As established above, privacy is used to identify who may access protected health information and for what reasons or under what circumstances. Confidentiality addresses the actual safeguarding of the data that is gathered through the delivery of healthcare (IOM, 2009; Surbhi, 2015). The provision of healthcare, starting with the physician-patient relationship, establishes a legal relationship in the eyes of the law for which data that is shared must be
protected and safeguarded against unauthorized intrusion (IOM, 2009; Prater, 2014; Surbhi, 2015). It is an obligation to the patient to hold private data in confidence (Prater, 2014). So if privacy revolves around the collection of patient data, the storage of patient data, and the use of the patient data, confidentiality revolves around safeguarding the data from unauthorized access or from inadvertent disclosures (IOM, 2009). In simpler terms, privacy is intended to protect the person while confidentiality is intended to protect the data (Prater, 2014; Surbhi, 2015).

Security

Privacy and confidentiality in healthcare practice represents both a legal and a professional obligation to the patient. The technical procedures, measures, methods, and safeguards by which healthcare providers, institutions or entities meet this obligation forms the basis for defining security (IOM, 2009; Weiner, 2002). Security is concerned with the actual protection of private and confidential materials to guard against unauthorized access and use (IOM, 2009; Prater, 2014). If a computer system is hacked, which is most commonly referred to as a breach, this breach represents a breach in security as the hacker managed to successfully bypass security measures intended to prevent unauthorized access and use (IOM, 2009). Once security is bypassed there is the potential then for confidential information stored in the computer system to also be breached, although a breach in security does not automatically mean that confidentiality was breached (IOM, 2009).

Protected Health Information

It is established that privacy, confidentiality, and security, can have numerous definitions that can be applied to a multitude of circumstances depending upon the professional area in which they are applied. Relative to healthcare today, the concepts of privacy, confidentiality, and security, are expressly designed to address something called protected health information (PHI). The United States Department of Health & Human Services (HHS) defines PHI as all
“individually identifiable health information held or transmitted by a covered entity or its business associate” (2003, What Information is Protected section, para. 1). A covered entity refers to health insurance plans, healthcare providers, and healthcare clearinghouses (HHS, 2003). A business associate is viewed as any person or organization that handles protected health information on behalf of a covered entity (HHS, 2003). PHI can be found in any form or format including media, and may include oral, paper, or electronic form (HHS, 2003).

It is PHI that ties privacy, confidentiality and security together in healthcare, as individuals have both a right and a desire to have their health information protected, and a need to trust that those that have their PHI will keep it secure. As would be expected, PHI includes any past, present and/or future health information related to a person’s mental or physical health or condition (HHS, 2003). PHI also includes any information related to a payment for healthcare services by an insurance company or the individual receiving services (HHS, 2003). Perhaps more surprising, PHI also includes any information that could be used to identify an individual or “for which there is a reasonable basis to believe can be used to identify the individual” (HHS, 2003, What Information is Protected section, para. 2). As such, PHI includes any demographic data including name, address, social security number, and date of birth (HHS, 2003).

The Importance of Patient Privacy

There has long been a tradition of healthcare providers keeping their patients information in confidence (IOM, 2009). What started as a simple, unwritten commitment by those providing care has grown into a federal law with governmental oversight (Higgins, 1989). The age old practice of confidentiality in healthcare did not surface and evolve without good reason. Rather, it developed out of a need driven by the patients themselves. Today more than ever patients receiving healthcare services drive the importance of protecting and maintaining privacy. The Institute of Medicine Committee on Health Research and the Privacy of Health Information states
that “American society places a high value on individual rights, personal choice, and a private sphere protected from intrusion” (2009, para. 13). This is because a patient’s health information may contain very intimate details of a person’s health status or condition. Things such as a person’s mental health, physical health, social and family histories, personal relationships, and even the patient’s financial status, all can be potentially found within a patient’s PHI (IOM, 2009). Before exploring the evolution of protecting patient privacy, it is important to better understand several of the primary reasons that patients expect their private health information to be protected.

**Patient Fear**

A basic reason for protecting an individual’s health information is to address the individual’s fears related to inappropriate access to their private lives. This fear that exists is not a simple single thing that people are afraid of, but rather is a host of fears regarding what can happen if their health information is not kept secure and confidential. Patient fears range from fear of discrimination based on their health status to fear of losing their job. These fears result in patients not being truthful with their healthcare providers or even worse, not seeking necessary care for fear of someone discovering something about the individual’s health (IOM, 2009).

In 1999, prior to HIPAA and the emergence of electronic health records (EHR’s), a survey was conducted regarding consumer attitudes as they related to the privacy of health information (IOM, 2009; Weiner, 2002). The results of this study indicated that 75% of respondents classified the concern for the privacy and confidentiality of their health information as significant (IOM, 2009; Weiner, 2002). In fact, respondents ranked a loss of personal privacy as a higher concern to them than terrorism or global warming (Weiner, 2002). A similar survey conducted in 2005, three years after the implementation of HIPAA, though slightly reduced in number, demonstrated a similar consumer sentiment, with 67% of respondents having concern
about the safety and security of their health information (IOM, 2009). The highest level of concern and fear for patient health information privacy and security was found amongst racial minorities and individuals from different ethnic backgrounds (IOM, 2009).

In today’s society, sadly, discrimination still exists in various forms and manners. Individuals have very real fears and concerns that if their health information is not kept private and confidential it could be used to discriminate against them by their employers, banks or lenders, and by health or life insurance companies (IOM, 2009; Peel, 2013). According to Peel (2013), 35% of Fortune 500 companies use health information contained in medical records in determining who to hire and who to promote. Someone with a debilitating disease or with a medical condition deemed expensive or high-risk by an employer could result in a lack of advancement and financial harm to the individual (IOM, 2009; Peel, 2013). The Institute of Medicine Committee on Health Research and the Privacy of Health Information (2009) showed in a 2005 survey that 52% of respondents feared that their health information could be used by their employer to limit the individual’s opportunities within the company. In addition to fears regarding employers, a fear exists with regard to genetic testing and genetic information. The fear is that a health insurance or life insurance company that has access to genetic information might choose to use it in inappropriate ways to the detriment of the individual (IOM, 2009).

Provider-Patient Communication/Relationship

Essential to any productive, satisfying, and effective provider-patient relationship is a bond of trust between the two parties. A patient must be able to trust that their healthcare provider will protect their health information from unauthorized access. Peel (2013) stated that “without trust, people avoid treatment and hide sensitive information about their minds and bodies” (p. 89). If a patient does not trust that a provider will keep their health information confidential and secure they may simply choose to no longer see that provider, or any provider (Peel, 2013). Even if the
patient trusts their provider, the fear of information getting into the hands of those that can use it against them remains. As a result, patients might choose to pay cash for tests ordered by their healthcare provider to avoid insurance companies seeing the information, resulting in additional economic burden on the patient (Peel, 2013). Worse still, patients might choose to avoid having needed testing done at all (Peel, 2013). Patients have even gone so far as to ask providers to alter their diagnosis for fear of the information being used against them by someone (Peel, 2013).

**Quality of Care/Outcomes**

Patient trust in the confidentiality and security of their private health information influences all aspects of the care that they seek out, including where they seek it, when they seek it, who they seek it from, and what kind of care they choose to seek (FairWarning, 2011). Individuals might only seek care from a particular physician if they believe that they can trust their physician to maintain their confidentiality. In a 2011 study 85.2% of respondents stated that if they had a sensitive medical condition the medical provider’s reputation for patient privacy would influence their decision to seek care from that provider (FairWarning, 2011). If there is a lack of trust in the medical community patients might choose to avoid seeking any care at all. Or, a patient might choose to withhold certain information from the medical provider which could negatively impact the care they receive. This is supported by the same 2011 study which showed that 27.1% of respondents would indeed withhold information from their caregiver due to privacy concerns (FairWarning, 2011). In fact, Peel stated that 13-17% of patients actually admit to having withheld information from their healthcare provider, something Peel calls “information-hiding”, because they were concerned about the confidentiality of their condition (2013). This information-hiding includes behaviors such as being dishonest with the provider with regard to their condition or any symptoms they may be experiencing, and also providing inaccurate information as a result of concerns about privacy (IOM, 2009; Peel, 2013). The results of such
The issue of not seeking care over concerns of privacy is no minor issue and is one with the potential to have severe consequences on patient health. The U.S. Department of Health & Human Services (HHS) estimates that 586,000 Americans each year do not seek appropriate early cancer care and treatment due to concerns about the privacy of their health information (Peel, 2013). This problem is magnified greatly when mental health care is involved, with the HHS estimating that 2 million Americans each year do not seek appropriate care for a mental illness due to concerns over the security of their information and confidentiality (Peel, 2013).

Two other at-risk groups with substantial concerns about their privacy that avoid healthcare are young Americans/adolescents, and American military personnel. Younger Americans do not seek appropriate healthcare for fear that information about health conditions such as reproductive health, sexual activity or sexually-transmitted diseases, and substance abuse, if not adequately kept secure, could lead to family problems or embarrassment in their community (IOM, 2009; Peel, 2013). With regard to military personnel, a study by the Rand Corporation found that each year at least 150,000 soldiers with post-traumatic stress disorder, known as PTSD, do not pursue appropriate medical care for their condition due to privacy concerns (Peel, 2013). Peel goes so far as to suggest that this lack of confidentiality and security is a contributing factor to the suicide rate amongst active military personnel, which is the highest it has been in over 30 years (2013).

Impact on Research

In general, people view medical research as a positive thing for the advancement of healthcare delivery and for finding new ways to treat illness (IOM, 2009). However, the majority of those involved in medical research have concerns about how their health information will be
used, and how it will be kept confidential, and will only consider participation if their consent is given (IOM, 2009). The largest potential negative impact on research, however, relates back to the patient tactic of information-hiding outlined in the previous section of this paper. If a patient deliberately withholds information from their medical provider, the records maintained on that patient are not accurate. If this incomplete or inaccurate data is then used as part of a research project, the outcomes of the research will always be in question (Peel, 2013). In addition to patients hiding information, opting to receive healthcare services in cash-based environments means that the data may not be collected in a useable way at all (Peel, 2013). All of this limits the overall usefulness of medical data collected for research, which stems from patient concerns over privacy and security of their health information.

The History of Patient Privacy

By its nature, medicine and the delivery of healthcare require privacy and confidentiality. An individual must trust their physician or healthcare provider in order to be open and honest about their medical situation or circumstance. This trust and openness from the individual toward the physician places an expectation upon the physician that they will keep what they learn about the patient in confidence. While an individual’s need for health information privacy seems to have been the norm for centuries, an individual’s right to health information privacy is much more recent. According to Ferguson (2012), “historical research into the evolution of approaches to medical confidentiality reveals an enduring ideal that has been interpreted through a variety of theoretical lenses and influences by more pragmatic concerns” (p. 738).

Prior to 1900

Human beings learned centuries ago that they had the power to take another person’s life. It is likely that around that same time humans also learned that they had the ability to cure people (“About Hippocrates”, n.d.). Individuals that adopted the “profession” of healing people that were
sick or injured came to be known as sorcerers, witch doctors, and shamans ("About Hippocrates", n.d.). They had the ability to use things in their environment to make the sick healthy again, though their understanding of how the human body functioned was very limited and often incorrect. As early humans developed in knowledge so did their understanding of how to heal the human body and how the human body functioned.

**Hippocrates.**

One of the earliest Greek physicians, and perhaps the best known, was a physician named Hippocrates ("About Hippocrates", n.d.; Tyson, 2001). Hippocrates lived and practiced medicine during the time of famous teachers and philosophers Plato and Socrates, and he started a school of medicine around 400 B.C. ("About Hippocrates", n.d.). Hippocrates organized the art of healing and medicine into a professional code of conduct that outlined a specific set of duties, codes, and ethics. Roughly a century after the death of Hippocrates, his professional philosophy on practicing medicine as an art of healing was written into what is known as the Hippocratic Oath ("About Hippocrates", n.d.; Tyson, 2001). It is in this oath, considered “one of the oldest binding documents in history” (Tyson, 2001, para. 1), that the importance of maintaining a patient’s privacy found its way into writing (IOM, 2009).

A physician was expected to enter into a “trust-based relationship” ("About Hippocrates", n.d.) with their patient, a relationship in which the secrecy of the patient’s condition was a professional and ethical expectation of the physician (Higgins, 2009). Every physician initiate was expected to swear to the Hippocratic Oath, which included the following with regard to the importance of maintaining patient privacy:

> And whatsoever I shall see or hear in the course of my profession, as well as outside of my profession in my intercourse with men, if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets. (Higgins, 1989, para. 8)
It is interesting to note that the wording in this oath required that a physician not only maintain the privacy of the patient's health information, but that the physician consider any information they attain related to their patient be kept as a secret (Higgins, 1989). What is noticeably missing in this pledge to privacy, however, is a definition of, or examples of, what is meant by that which “should not be published abroad” (Higgins, 1989). The result of this lack of clarity with regard to what specifically should be kept secret and in confidence was that it was left to the discretion of each individual physician to decide (Higgins, 1989). Despite a lack of clarity in the oath, patients had their desire and need for privacy and confidentiality acknowledged.

**The oath of Asaph.**

The oldest of Hebrew manuscripts related to medicine and healing is a group of works said to have been written by a physician named Asaph Judaeus, also known as Asaph ben Berachiah (Rosner & Muntner, 1995). Asaph was believed to have been a Jewish physician that lived between 600-400 B.C. (Rosner & Muntner, 1995). There is very little written or known about Asaph as a person (Rosner & Muntner, 1995). The texts attributed to him provide great detail about the various types of medicine and healing practices used throughout that period of time.

Of particular interest to the area of patient privacy, the works of Asaph contained an oath said to have been expected of all Hebrew physicians, now referred to as the Oath of Asaph (“Oath of Asaph”, 1994; Rosner & Muntner, 1995). In this oath, Asaph outlined expectations of physicians, putting in writing a code of ethics for Hebrew physicians to uphold (Rosner & Muntner, 1995). The oath is believed to have perhaps been influenced by Hippocrates, as Hippocrates and other Greek physicians are mentioned in Asaph’s writings (Rosner & Muntner, 1995). In this oath, the physician is told, “do not disclose secrets confided in you” (“Oath of Asaph, 1994). The oath is a total of seven paragraphs, out of which only those seven words
address patient privacy. However, these words instruct the physician to keep information that they learn from their patients confidential, which in turn allowed patients to trust their physicians.

**The Middle Ages.**

The rise of Christianity brought about a period referred to as the Middle Ages, which lasted from around 500 A.D. until the mid-1500’s A.D. (“Medical Ethics”, 2004). Medicine continued to grow as a profession during this time. The various religious belief systems, including Christianity, Islam, and Judaism, all embraced the role of the physician as each believed it aligned well with their tenets (Koios, Veloyanni, & Alvanos, 2012). Each saw caring for the sick as a pillar of their belief system. The different religious systems beliefs were generally in agreement with the ethical standards outlined in the Hippocratic Oath (Koios et. al., 2012; “Medical Ethics”, 2004). According to Higgins (1989), “in the middle ages, the Hippocratic Oath was held in high esteem” (p. 922).

While the vast majority of the Hippocratic Oath was suitable to the religious sects of the time, modifications were made to it by each group to ensure it harmonized with their ideology and practices (Koios et al., 2012). All groups changed language in the oath by removing the references to the Greek deities noted in the oath, and added their own statements referencing the god that they worshipped (Higgins, 1989; Koios et. al., 2012). Other changes included language about caring for the poor and the needy (“Medical Ethics”, 2004). What remained and was never changed was the commitment in the Hippocratic Oath that the physician keep secret the information they gain from their patient (Higgins, 1989).

Throughout the Middle Ages the importance of privacy in the delivery of healthcare remained a pillar that stood the test of time, as communities valued the physician-patient relationship (Koios et. al., 2012). An example of this can be seen in the words of the well-respected physician at the time, Constantine the African, who around 1050 A.D. said that a
Physician “ought to keep to himself confidential information concerning the ailment, for at times the patient makes known to the physician things he would blush to tell his parent” (Higgins, 1989, p. 922). Physicians came to understand that by keeping their patient’s health information secret, the patient gained confidence in them as a physician and their communities trusted them more to treat them or their families (Higgins, 1989). The respected surgeon John Aderne in 1370 wrote about patient confidentiality and trust in his treatise, writing “for if a man sees that you hold secret another’s information, he will better trust you” (Higgins, 1989, p. 922).

**Modern history.**

Throughout the age of enlightenment and the industrial revolution, mankind enjoyed significant advances in technology, education, quality and quantity of life, and in medicine. Two notable physicians of the time, John Gregory and Thomas Percival, both emphasized in practice and in writing the critical importance of a code of medical ethics in the practice of medicine, including a focus on patient privacy and confidentiality (Ferguson, 2012; Higgins, 1989). As a practicing physician, Gregory recognized that due to the nature of the work of a physician, patients were likely to share with the physician very private things about them and their life (Ferguson, 2012). Gregory opined “how much the characters of individuals, and the credit of families, may sometimes depend on the discretion, secrecy, and honor of a physician” (Ferguson, 2012, para. 5).

Thomas Percival echoed the thoughts of John Gregory in regard to patient privacy in his book *Medical Ethics* (Higgins, 1989). Percival is credited by many as having written “the first modern ethical code of medical ethics” (Higgins, 1989, p. 923), and his book formed the foundation of the American Medical Association’s very first code of ethics which was adopted in the year 1846 (Higgins, 1989; IOM, 2009). In this book Percival twice notes the value and importance of patient privacy (Higgins, 1989). In one such passage, Percival states that:
Secrecy and delicacy when required by peculiar circumstances should be strictly observed. And the familiar and confidential intercourse, to which the faculty are admitted in their professional visits, should be used with discretion, and with the most scrupulous regard to fidelity and honor. (Higgins, 1989, para. 19)

What is noted in the writings of Gregory and Percival is that the physician’s obligation to keep confidential that information that they learn from their patients is as much about building trust and rapport with the patient as it is about maintaining the honor of being a physician (Ferguson, 2012). The reasoning behind this was that physicians wanted to look honorable to earn the favor and trust of wealthy clients (Ferguson, 2012). Regardless of their rationale, patient privacy continued to be emphasized by physicians.

Patient privacy and confidentiality met its first real challenge in the late 1800’s with the emergence of local governments focusing on public health (Ferguson, 2012). The desire of the individual to have privacy was confronted with a need to protect the welfare of the community as a whole (Ferguson, 2012). Physicians were indeed routinely asked to balance the obligation to the patient to keep their information confidential and the need for the health and greater good of the public (Ferguson, 2012; Higgins, 1989). This conflict was inevitable as the medical community recognized the legitimate need for the sharing of health information in preventing the spread of disease.

1900-1990

As the medical professions evolved, so did the role of privacy and confidentiality in healthcare. What was once simply a commitment by a physician to their patient to keep their health information private blossomed into an obligation for physicians that became part of their professional ethical obligations (Higgins, 1989). The desire for this privacy obligation to be
absolute was forced to adapt to an evolving society, advances in medical education, and the introduction of modern technology.

**The rise of medical specialties.**

Along with advances in medicine, physicians started specializing their training to prepare them to treat specific body systems and the diseases and ailments associated with them (Ferguson, 2012). As a result, there was no longer simply one physician involved in a patient’s care, but often several physicians of varying training backgrounds. This increased specialization by physicians meant that patients would get more expertise for a specific disease, resulting in better health outcomes. However, this now meant that there were multiple physicians that had private information about the patient, and there was a need for all physician’s involved in the patient’s care to communicate and exchange information (Ferguson, 2012). This caused many to begin to question the ongoing relevance of the physician-patient relationship and the general expectation of confidentiality and privacy that accompanied it (Ferguson, 2012).

**The Privacy Act of 1974.**

In 1973 a report titled Records, Computers, and the Rights of Citizens was provided to the U.S. Department of Health, Education and Welfare (HEW) by an advisory committee that articulated an individual’s right to health information privacy stating individuals had a “meaningful right to control the collection, use, and disclosure of their information” (IOM, 2009). The report also added that those that collect health data had a responsibility to safeguard the data (IOM, 2009). The federal government recognized that the use of computerized databases to house patient data was becoming the norm and that this data needed safeguarded (“Electronic Privacy Information Center [EPIC], n.d.). This report formed the foundation and framework for what would become the first federal regulatory and statutory protections for protecting an individual’s right to the privacy of their health information (IOM, 2009). This foundation was built around
regulating and limiting the collection of health data, data quality, and obligating those collecting data to have purposeful reasons for data collection (IOM, 2009). In addition, the report called for limitations on the use of collected health data, security safeguards, openness, participation by the individual in the use of their data, and accountability (IOM, 2009). This would be the first time the federal government was prepared to regulate health information, and while there were laws to protect an individual’s privacy, most were with regard to financial information and not health information (Weiner, 2002).

The 1973 advisory committee report noted above resulted in the passage of the Federal Privacy Act of 1974, which went into effect on September 27, 1975 (EPIC, n.d.; IOM, 2009; Weiner, 2002). This was a big step for advancing individual health privacy, however, this act was only applicable to federal government agencies, and while it did encompass federal government run hospitals, research institutions, and some government contractors, private healthcare providers were not subject to the act (IOM, 2009). This act had four distinct procedural rights embedded into it on behalf of an individual’s health information. The first was that it obligated government agencies to show individuals what records it was keeping on people (EPIC, n.d.; IOM, 2009). Next, the act required government agencies to follow what it called “fair information practices” with regard to the use of personal health information (EPIC, n.d.; IOM, 2009). Third, the Privacy Act implemented certain restrictions upon government agencies with regard to how individual health data could be shared and with whom it could be shared (EPIC, n.d.; IOM, 2009). The fourth and final individual right embedded in the Privacy Act was that it permitted individual’s to sue the federal government if there was a violation of any part of the act, or if an individual’s data was misused (EPIC, n.d.). There were some exceptions to the Privacy Act; however, one of which being that any government agency whose purpose was for law enforcement did not have to abide by the rules set forth in the Act (EPIC, n.d.).
The Privacy Act of 1974 did a great deal to define health information privacy and create accountability, though it still had its shortcomings. In addition to only being applicable to certain government agencies, and not the private sector, it also only allowed U.S. citizens or permanent residents to sue the government if it was misusing an individual’s health information (EPIC, n.d.). As would be expected, those agencies accountable to the Act often found ways to work around the provisions of the Act. An example of this can be found in a provision of the Act that allowed for the disclosure of health information if it was part of “routine use” (EPIC, n.d.). This exception was able to be manipulated in such a way that data often “creeped” from one set of records to another, when it really should not have (EPIC, n.d.).

1990-Present

Advancements in computer technology skyrocketed after 1990. Computers and the technology that supported them made its way into all professions and all aspects of business, as well as into the individual’s home for personal use. The healthcare delivery sector, however, heavily resisted the integration of this advanced technology into the delivery of patient care (Stark, 2010). Despite the fact that there was evidence that medical errors could be reduced through increased technology such as electronic health records (EHR’s), healthcare systems and physician practices were not swayed (Stark, 2010). Factors such as the cost of the technology, changes in work flows, interruptions in the interactions with patients, and strong concerns about protecting patient privacy and confidentiality were all routinely cited as reasons against implementing an EHR (Stark, 2010). As a result of such resistance the U.S. government recognized it needed to give the healthcare sector a push towards technology use. With the establishment of the Office of the National Coordinator for Health Information Technology (ONC) in 2004, the federal government stood ready to press the healthcare sector to embrace technology (Stark, 2010). However, the challenge of protecting the privacy and confidentiality of
health information in a digital environment was a very real concern, and one that needed addressed.

The Health Insurance Portability and Accountability Act of 1996.

On August 21st, 1996, the 104th Congress of the United States and President Bill Clinton enacted the Health Insurance Portability and Accountability Act (HIPAA) (“HIPAA 101”, n.d.; “History and background of HIPAA”, n.d.). A lesser known name for HIPAA is the Kennedy-Kassebaum Act, as the original bill was introduced by the late Democratic Senator Edward Kennedy and Republican Senator Nancy Kassebaum (“HIPAA 101”, n.d.). HIPAA represented a series of governing regulations that were outlined into two titles, I and II (“History and background of HIPAA”, n.d.). Title I of HIPAA was not intended to address privacy or confidentiality concerns. Rather, Title I, known as Health Care Access, Portability, and Renewability, was specific to health care plans such as insurance companies, and addressed coverage limitations, exclusions, and waiting periods (“HIPAA 101”, n.d.; “History and background of HIPAA”, n.d.). Title II of HIPAA, which was called Preventing Health Care Fraud and Abuse, contained five separate and distinct rules of which two were directly intended to address privacy and confidentiality (“HIPAA 101”, n.d.; “History and background of HIPAA”, n.d.). The two rules regarding privacy and confidentiality were the Privacy Rule and the Security Rule (“History and background of HIPAA”, n.d.).

With the official enactment of HIPAA in April of 2003, individuals now were granted defined rights under the law with respect to the use of their protected health information (PHI). The Privacy Rule of HIPAA now made it the legal responsibility of a covered entity to engage the patient in controlling the “movement” of their health information. The Privacy Rule under HIPAA mandated that covered entities such as hospitals, physicians, and health clinics, get signed permission from an individual before disclosing any PHI to another individual, entity, or
organization (“HIPAA 101”, n.d.). The original rule, as written, was determined to be too stringent as it required covered entities to get a signed authorization from a patient for absolutely any use of their PHI (Peel, 2013). In 2002 the U.S. Department of Health & Human Services (HHS) amended the Privacy Rule to provide for some exceptions to the rules (Peel, 2013). The amended exceptions were designed to ensure that patients had continuity of care between different providers, that covered entities could conduct business operations, and so that insurance companies could receive and process payments for services provided by covered entities (“HIPAA 101”, n.d.) Other exceptions in which a patient’s signed authorization was not required to disclose their PHI included certain law enforcement needs and health information that was needed for a greater public health interest (“HIPAA 101”, n.d.). Despite these exceptions, an individual’s PHI was now to some degree able to be controlled by the patient, and any unauthorized releases or disclosures of an individual’s PHI in which a patient’s consent was not received or that did not meet an exception were strictly forbidden.

In addition to the Privacy Rule, Title II of HIPAA also called for the creation of the Security Rule. This rule was seen as complimentary to the Privacy Rule as it required covered entities to protect the health information that they had possession of on behalf of their patients. Covered entities were now expected to implement and maintain security standards, protective measures, and safeguards to assure the confidentiality, integrity and accessibility of PHI stored in their systems (“HIPAA 101”, n.d.). Massive amounts of patient data was being stored on electronic computer servers, data bases, and on computer systems, and with each of these systems there was the potential that the PHI could be accessed by unauthorized users, or breached.

The Department of Health and Human Services Office of Civil Rights (OCR) was assigned responsibility by HIPAA for enforcing and overseeing the Privacy and Security Rules (“HIPAA 101”, n.d.). However, the OCR was crippled in addressing infractions of the rules, as there was no system of penalties or punishment for violations by covered entities. At long last all
patients had rights under the law for the protection, privacy and security of their PHI, but there was no real mechanism with which to enforce and police the rules or by which to hold covered entities accountable to the rules (“HIPAA 101”, n.d.). In fact, during the first two years that HIPAA was in place, there were over 13,000 complaints submitted to the OCR by individuals regarding violations of their privacy, with absolutely no enforcement actions taken by the OCR (Solove, 2013). Over several years of audits and investigations of patient complaints, indeed the OCR discovered that many covered entities were often knowingly and willfully neglecting the Privacy and Security Rule and that breaches of PHI were quite common (“HIPAA 101, n.d.).

**The Health Information Technology for Economic and Clinical Health Act of 2009.**

On February 17, 2009 the Health Information Technology for Economic and Clinical Health Act (HITECH) was signed into law and enacted as part of the economic stimulus bill known as the American Recovery and Reinvestment Act (“Overview of HIPAA/HITECH”, 2013). HITECH was enacted to improve upon areas of weakness and vulnerability found in the Privacy Rule and Security Rule. In addition, HITECH was enacted to create and enforce penalties for covered entities that did not comply with HIPAA regulations (Solove, 2013). These new penalties were substantial, and included large monetary fines. HIPAA finally had the “teeth” that patients desired.

While HITECH was mainly developed to add an enforcement piece to HIPAA, it also included some new expectations of covered entities. Specifically, HITECH required covered entities to provide information to individuals regarding the potential for breaches and how the covered entity would handle any breaches (Solove, 2013). This change meant that covered entities had a legal obligation to alert patients when and if their protected health information was misused or handled in an unauthorized manner. However, not only did covered entities now have to report to the patient with any breach, they were now required to report any breaches to the
federal government. Lastly, HITECH contained language requiring the U.S. Department of Health & Human Services (HHS) to conduct audits of covered entities and business associates to analyze their compliance with privacy and security laws and regulations (Solove, 2013).

**Patient Privacy in the Modern Age – The Omnibus Rule**

Today an individual’s health information is protected by federal laws known as HIPAA and HITECH. These two federal regulations modernized patient privacy and security by addressing electronic health technology and storage, requiring covered entities and business associates to comply with regulations, and allowing enforcement of these regulations for organizations that failed to comply. In addition, they mandated government agencies to audit relevant agencies and organizations to ensure compliance. Prior to 1996 when HIPAA was signed into law, there was no federal law protecting and regulating the privacy and security of all patient’s health information. While HIPAA and HITECH are now the law of the land, and they both highlight in significant detail the importance of protecting a patient’s privacy, recent updates to these regulations added more complexity to these laws in what is referred to as the Omnibus Rule.

On January 25, 2013 HIPAA and HITECH had major updates and revisions added as a final rule in a publication titled Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA rules (“Overview of HIPAA/HITECH”, 2013). This lengthy title was fortunately shortened to simply the Omnibus Rule. The effective date for the Omnibus Rule was March 26, 2013, with effected parties having 180 days to come into compliance from that date, making the full compliance date September 23, 2013 (“Overview of HIPAA/HITECH”, 2013). While it had several purposes, the general purpose of the Omnibus Rule was simple, to strengthen protections
found within HIPAA regarding both security and privacy as it relates to electronic PHI (Modifications to the HIPAA Privacy, 2013). The Omnibus Rule consists of four separate rules (Modifications to the HIPAA Privacy, 2013).

**Final Modifications to the HIPAA Privacy, Security, and Enforcement Rules**

The first section in the Omnibus Rule consists of final modifications to HIPAA and HITECH (Modifications to the HIPAA Privacy, 2013). One of the most substantial changes from this rule impacted business associates (BA) by expanding the definition of a BA and by increasing the liability and obligations of a BA (Gilleskie & Sullivan, 2013). The expanded definition of a BA now includes any business or individual that handles PHI on behalf of a covered entity, even if the relationship is an indirect one, such as a subcontractor of a BA (Gilleskie & Sullivan, 2013; Solove, 2013). Prior to this section found in the Omnibus Rule, a BA would not be held liable in the event of a breach of PHI, with all of the risk of liability falling to the covered entity (Solove, 2013). Now a BA or any of their subcontractors can be held directly liable for any compliance issues related to PHI, including sanctions and monetary fines (Gilleskie & Sullivan, 2013). Solove (2013) believes this change came from findings that greater than 20% of breaches reported to the federal government were actually due to BA’s and not covered entities.

This section of the Omnibus Rule provides several final instructions regarding PHI for use in fundraising, marketing, and the sale of PHI (Modifications to the HIPAA Privacy, 2013). It first increases limitations for the use of PHI when used for marketing purposes by requiring that an individual be notified by a covered entity if they are paid by a third party to send out marketing materials on behalf of the company (Gilleskie & Sullivan, 2013; Modifications to the HIPAA Privacy, 2013;). This change allows for more transparency between a covered entity and their patient. Another change in this rule addresses the use of PHI for fundraising purposes
PATIENT PRIVACY

(Gilleskie & Sullivan, 2013; Modifications to the HIPAA Privacy, 2013). Within HIPAA there are very limited means by which a covered entity can use a patient’s PHI for fundraising purposes without needing to get the consent of the patient (Gilleskie & Sullivan, 2013). This section of the Omnibus Rule adds additional language which directs covered entities to ensure that patients are given very clear opportunities with which to opt out of receiving fundraising materials or communications (Gamble, 2013; Gilleskie & Sullivan, 2013). Lastly, with regard to the sale of PHI, this section of the Omnibus Rule clearly articulates that the sale of PHI is prohibited unless the sale is authorized by the patient, and any sale in which a covered entity will be receiving remuneration must be communicated to the patient prior to requesting authorization (Gamble, 2013; Gilleskie & Sullivan, 2013).

Also contained within this section of the new Omnibus Rule is an expansion of a patient’s rights with regard to receiving copies of their PHI, and an increased ability for the patient to restrict disclosures of their PHI (Gamble, 2013; Gilleskie & Sullivan, 2013; Modifications to the HIPAA Privacy, 2013). A patient may now request an electronic copy of their PHI and a covered entity must comply with this request by providing the PHI in an electronic form (Gamble, 2013). A patient may now also request that a covered entity restrict their PHI from being disclosed to health insurance plans if the patient chooses to pay for the services with cash and requests such a restriction (Gamble, 2013; Gilleskie & Sullivan, 2013). This new ability for a patient to restrict PHI applies to all insurance plans, including governmental payers like Medicare (Gamble, 2013). This new regulation should provide relief to patients that are afraid of being discriminated against based on their health status by adding an extra layer of protection of their PHI.

There are a few other notable changes found within this section of the Omnibus Rule. The first is recognition of the need for public health and data sharing in the school systems (Modifications to the HIPAA Privacy, 2013). Since most states prohibit students from starting
school without first having verified the child’s immunizations, covered entities may now release relevant childhood vaccination records to appropriate school systems by simply documenting a verbal authorization from a parent or guardian of the child (Modifications to the HIPAA Privacy, 2013; “Overview of HIPAA/HITECH”, 2013). The removal of the requirement for a written authorization is intended to increase the speed and efficiency with which information can flow to the school systems. Lastly, as a result of the numerous changes to HIPAA, HITECH, and a patients right’s, this section of the Omnibus Rule requires all covered entities to update their Notice of Privacy Practices, which is a public document made available to all patient’s that summarizes privacy regulations and the patient’s privacy rights under the law (Modifications to the HIPAA Privacy, 2013).

**Final Rule Adopting Changes to the HIPAA Enforcement Rule**

This section of the Omnibus Rule adopted changes specific to the enforcement of HIPAA’s Privacy Rule. The first was the addition of a structured penalty system for covered entities and business associates that are found negligent in their compliance of privacy rules and regulations (Modifications to the HIPAA Privacy, 2013). The structure created is a tiered system of increased civil monetary penalties up to $1.5 million per violation (Gilleskie & Sullivan, 2013). This section also expanded the enforcement of these penalties and sanctions to business associates. Lastly, this section made it a requirement for the U.S. Department of Health & Human Services (HHS) to conduct an investigation of any party for which they have received a complaint or have a reason to believe are in violation of any privacy regulations if the potential violation is believed to be due to what is called willful neglect (Gilleskie & Sullivan, 2013; Modifications to the HIPAA Privacy, 2013). Prior to this change HHS had the discretion to consider whether or not to investigate such a situation (Gilleskie & Sullivan, 2013). HHS views willful neglect by a party to be a conscious intent to violate a privacy law or regulation (“Overview of HIPAA/HITECH”, 2013).
Final Rule on Breach Notification for Unsecured Protected Health Information

Fundamental to protecting a patient’s privacy is keeping PHI from being viewed or obtained by a person that is not authorized to view or have the PHI, in other words, avoiding a breach of the PHI. In this section of the Omnibus Rule, HHS added language to state that any impermissible use of PHI should be presumed by a covered entity or business associate to be a breach unless the party can demonstrate through a formal risk assessment “that there is a low probability that the PHI has been compromised” (“Overview of HIPAA/HITECH”, 2013). In addition, HHS changed the language previously being used in which a party was to determine any “risk of harm” from a potential breach of PHI, to state that a party must determine any “risk of compromise” in any potential breach (Gamble, 2013). These changes are intended to remove any subjectivity of a party evaluating a potential breach and to insert objective and uniform decision making criteria (“Overview of HIPAA/HITECH”, 2013). This is a substantial change and means that a covered entity must notify a patient that a breach has occurred in all situations unless through a risk assessment it has been determined that there is a “low probability that the PHI has been compromised” (Gamble, 2013).

The risk assessment called for by this section of the Omnibus Rule outlines four factors that should be part of any organization’s risk assessment when investigating a potential breach of PHI (“Overview of HIPAA/HITECH”, 2013). The four factors that must be part of the risk assessment include:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
(4) The extent to which the risk to the PHI has been mitigated (Gamble, 2013; “Overview of HIPAA/HITECH”, 2013).

These four components represent the minimum requirements of the risk assessment, though other factors identified as needed or relevant are certainly permissible to be added (“Overview of HIPAA/HITECH”, 2013). After conducting a risk assessment on any potential breach, the covered entity or business associate is then expected to identify whether there is a risk of compromise of the PHI. If there is a risk of compromise the patient or patients impacted are to be notified.

**Final Rule Modifying the HIPAA Privacy Rule**

The final section of the Omnibus Rule prohibits health plans and insurance companies from disclosing and/or using genetic testing information for the purposes of determining healthcare coverage or for underwriting life insurance policies (Gilleskie & Sullivan, 2013; Modifications to the HIPAA Privacy, 2013). This rule is designed to ensure compliance with the requirements of the Genetic Information Non-discrimination Act (GINA) that was passed in 2008 (Gilleskie & Sullivan, 2013; “Overview of HIPAA/HITECH”, 2013). This section of the Omnibus Rule also amended the definition of health information enforced by HIPAA to include genetic information, allowing genetic information to be considered protected health information (“Overview of HIPAA/HITECH”, 2013). This rule also clearly outlines what is to be considered genetic information. Any information regarding a disease condition or manifestation of a disease in a family member is considered genetic information and is not able to be used by health plans and insurers (“Overview of HIPAA/HITECH”, 2013). However, information about a patient’s individual disease or the manifestation of the disease in the individual seeking insurance coverage is not considered genetic information and can be used for the purpose of underwriting by an insurer (“Overview of HIPAA/HITECH”, 2013).
Protecting Patient Privacy in the Future

The use of technology in the healthcare sector has and will continue to create incredible advances in the delivery of care and the creation and value of information and data. “However, the ability to successfully leverage the potential of health IT depends to a large degree on the public trusting that their information will be kept private and secure” (Peel, 2013, p. 11). Each year new applications and new platforms for measuring and capturing health data are introduced into the marketplace. With each new idea the potential for data to be misused or accessed by unauthorized people or institutions also increases. Some of the growing trends in the healthcare arena that should be of focus to healthcare professionals include patient-generated data, personal health records, Health Information Exchanges, Health Record Banks, and the continued use and popularity of social media.

Patient-Generated Data and Personal Health Records

The Office of Civil Rights (OCR) states that a personal health record (PHR) is “an emerging health information technology that individuals can use to engage in their own health care to improve the quality and efficiency of that care” (n.d., para. 1). Individuals are using new technologies including devices and cellular phone applications in which the individual can create, store, and control their own health data (OCR, n.d.). Devices purchased and worn by individuals to track things such as heart rate, blood pressure, activity levels, sleep patterns, and other health parameters are becoming quite commonly used, and they have the potential to transform healthcare as we know it (DeAngelis, 2014). The medical community, however, is slower to embrace some of this new technology due to concerns about its reliability, and as such are cautious about making any clinical decisions based on patient-generated data (DeAngelis, 2014). In addition to concerns about reliability, there are challenges with integrating patient-generated data and data kept in personal health records into EHR’s used by medical providers and systems
A larger looming challenge with the use of this type of new technology is the security and privacy of this health information (DeAngelis, 2014).

Health systems often invest substantial infrastructure into protections and security safeguards on their electronic systems to protect patient data stored on their devices and to be in compliance with HIPAA. This level of attention to security is not being applied to mobile applications and portable devices used by individuals to track their own health information (DeAngelis, 2014). Further, unless a device or mobile application is provided by a covered entity to an individual to track personal health information, HIPAA and the Privacy Rule do not apply (OCR, n.d.). What this means is that devices and applications not provided by a covered entity are not held to the same security expectations and standards, and that information stored in these environments is likely at high risk to be breached and viewed. Also, if this data is indeed compromised or breached the providers of these devices and applications have no legal accountability to inform the individuals affected.

**Health Information Exchanges and Health Record Banks**

The use of electronic health records (EHR’s) is now widespread in healthcare delivery, and the use of this technology allows for increased opportunities to share data between healthcare providers. However, there are hundreds of EHR vendors and platforms in use throughout the U.S. and the world, and many of them do not interface with each other to allow for easy sharing of patient data. To overcome this obstacle to sharing patient data, there has been a rise in Health Information Exchanges (HIE’s). An HIE, sometimes referred to as a Health Information Organization (HIO), is an organization or vendor that provides an electronic, on-line forum of a single platform with which numerous healthcare organizations can share and exchange relevant and appropriate patient health information, regardless of the EHR being used by the system (Privacy Rights Clearinghouse, 2012). Medical providers or health systems that participate in an
HIE electronically can share things such as lab reports, radiology and imaging results, medications and medication allergies, referrals, and patient care summaries (Privacy Rights Clearinghouse, 2012). Why an HIE seems to make sense is that by sharing this patient health information, this should “help reduce any errors, reduce unneeded duplication of tests and procedures, and consequently, could reduce medical bills” (Privacy Rights Clearinghouse, 2012, para. 2). While an HIE seems to offer a great deal of benefits to patients, the use of an HIE brings with it a host of new privacy challenges and security concerns.

The use of an HIE means that PHI that is maintained by a single health system will now be available universally to any other provider participating in the same HIE (Privacy Rights Clearinghouse, 2012). Health systems that agree to share PHI through an HIE must ensure that the HIE has appropriate safeguards in place to adequately protect PHI, a task that was once simply the responsibility of the health system creating the PHI (Privacy Rights Clearinghouse; 2012; Sullivan, 2012). Survey data presented by Sullivan (2012) indicates that this will be no small undertaking, as 66% of healthcare organizations surveyed had little to no confidence in the security and privacy of patient data kept in an HIE. HIE’s must adhere to the regulations found in HIPAA, and for now an added layer of protection of PHI from a breach in an HIE is that a patient must give consent for an organization to share their PHI in an HIE (“Privacy Rights Clearinghouse, 2012). The federal government is funding the development of HIE’s in each state of the U.S., so this means of sharing health data does not look to be going away any time soon (Privacy Rights Clearinghouse, 2012). However, both medical providers and patients will need to gain confidence in the privacy and security of these systems before this system of sharing data can be widely adopted and of greater use and value (Sullivan, 2012).
Social Media

In addition to the advent of electronic health records, the rise of the digital age also brought about a new means for people to share and communicate on the world-wide web through social networking. Social media sites such as Facebook, Twitter, Snapchat, and YouTube, have all made information about people readily accessible to the world with simply the click of a button. As a consequence of an individual’s data being so easily accessible, the ability to maintain privacy is heavily challenged. Within the realm of healthcare social media is now being widely accepted, so an individual’s personal and private health information can be at risk and privacy must be carefully considered (Chauhan, 2015; Solove, 2013). The challenges that social media presents with regard to privacy and health information comes from the use of social media by healthcare workers (Health Information and Management Systems Society, 2013; Rebecca, 2013; Solove, 2013).

Healthcare employees may misuse social media by intentionally or unintentionally posting items on social media sites that contain patient information, patient photos or videos, or patient comments, which can possibly be used to identify an individual (Mosley, 2016; Ventola, 2014). Examples of this type of unauthorized use of PHI are on the rise due to the ease of posting to social media. Healthcare organizations, in an effort to stay current and in touch with the modern consumer, are turning to social media platforms as a way to engage with their patients and their communities. Physicians are finding social media to be a valuable way to expand upon the physician-patient relationship and to be an easy way to network with and problem solve with other physicians (Chauhan, 2015). However, without being cautious, mindful of what is being posted or shared, or focusing on their professional obligations and commitments to privacy and medical ethics, a physician with even the best of intentions can end up breaching a patients privacy by sharing their health information (Chauhan, 2015). According to Ventola (2014), an internet study of blogs that were written by healthcare professionals found there was individual
patient information contained in 42% of the blogs. 17% of time there was enough information by which a patient could identify themselves (Ventola, 2014). Without careful controls, policies and procedures, and appropriate staff training around social media use, healthcare providers and institutions have the potential to place a great deal of patient health data at risk (Solove, 2013).

**Conclusions**

Since the beginning of the delivery of what we now call healthcare, mankind has articulated a desire and need for privacy and confidentiality with regard to what they share with their caregiver (IOM, 2009). There was a need to trust the caregiver in order to be honest about their condition, and to in turn receive appropriate and adequate care. The same holds true today. Individuals have routinely expressed a legitimate fear and concern that their most personal and intimate health information might be used against them to do harm, or that it might be accessed by individuals that are unauthorized to view such information (FairWarning, 2011; Weiner, 2002).

An evaluation of the history and evolution of privacy and medicine has demonstrated that physicians practicing in medicine first found it important to develop their own personal commitment to maintain the confidentiality and privacy of a patient (Higgins, 1989). This personal commitment then evolved into a professional ideal, and from that into a code of conduct (Higgins, 1989). Now, with the passage of HIPAA, at long last a patient’s right to the privacy and security of their protected health information is clearly outlined and protected by law in the U.S (HHS, 2003). What has remained constant over the centuries is that the privacy and confidentiality of an individual’s personal and private health information is fundamental to every aspect of healthcare. Further, for healthcare delivery to be meaningful, effective and appropriate, the privacy, security and confidentiality of an individual’s health information needs to be of the highest priority.
The delivery of healthcare, and all of the facets that surround it, has evolved into a profession of enormous proportions, and technology has taken it to places never before thought possible. Despite some early resistance, the healthcare community has come to embrace the role and importance of technology in the delivery, operations, and communications of all aspects of the healthcare sector (Stark, 2010). This rise of technology in healthcare has been accompanied by a host of new security and privacy concerns that did not previously exist (IOM, 2009). Despite the best efforts and intentions by all involved, the risk for a loss or breach of protected health information cannot be completely mitigated (Peel, 2013). However, covered entities and business associates must continually evaluate the safeguards that they have in place and ensure that all identifiable risks are reasonably addressed. New technologies will continue to push the boundaries of healthcare delivery, and protecting the privacy and security of PHI will meet new and unexpected threats. In addition, the healthcare sector will forever be challenged with the inevitable conflict that arises between a legal obligation to protect a patient’s private health information and the often competing interest of the greater good of society (Higgins, 1989).

History has clearly shown that privacy in healthcare has and will forever be of the utmost importance to those receiving care. Healthcare professionals must be constantly reminded of the role of privacy and of the needs and expectations of the patients that they serve. It is evident that the ability for healthcare to serve its purpose in society rests firmly on its ability to protect and secure the privacy of the communities it serves. Healthcare professionals that have a thorough understanding of the base privacy needs of their patients, and that understand the history and rationale behind these needs, will be best equipped to implement policies and procedures that create and embrace an environment that values and enforces the highest security standards for protecting patient privacy and confidentiality.
References


Modifications to the HIPAA privacy, security, enforcement, and breach notification rules under the Health Information Technology for Economic and Clinical Health Act and the


