February 4, 2012

PATIENT PRIVACY IN THE CLOUD: WHY CONGRESS SHOULD MODEL HIPAA ENFORCEMENT MECHANISMS AFTER THE FCA TO MEET A NEW WAVE OF PRIVACY THREATS FROM THE IMPLEMENTATION OF CLOUD-COMPUTING TECHNOLOGIES

Andrew M Palanzi
INTRODUCTION

The right to privacy has long been considered a staple of modern American jurisprudence.\(^1\) Of the general privacy rights espoused, the right to privacy in one’s medical records is perhaps the most salient.\(^2\) Maintaining the privacy of an individual’s medical records helps prevent not only health related discrimination in fields of employment, finance, insurance, and education, but also protects an individual’s reputation and honor from the potential public dissemination of embarrassing medical records.\(^3\) The necessity for privacy in one’s medical records, however, has been amplified by the recent advent and adoption of Health Information Networks by the healthcare industry.\(^4\) These Health Information Networks largely rely on new cloud-computing technologies which offer the ability to store, transfer, and analyze millions of electronic medical records with ease; however, the use of this new technology has introduced new and additional privacy and security concerns relating to individuals’ electronic medical records.\(^5\)

To address these general privacy concerns and to help promulgate regulations related to the privacy and security of electronic storage and transmission of medical records, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA) in 1996.\(^6\) The original HIPAA legislation, however, only applied to more traditional users of health information referred to as “covered entities”,\(^7\) but because of new technological advances and the growing use of cloud-computing services in the healthcare industry,\(^8\) a new set of privacy and security concerns associated with the storage and transference of electronic medical data on cloud-based Health Information Networks began to emerge.\(^9\) In response to this emerging concern, Congress amended the original HIPAA legislation with the Health Information Technology for Economic and Clinical Health (HITECH) Act,\(^10\) to hold cloud-computing service providers, together with all other “business associates”, to many of the original Privacy and Security Rules that previously only applied to “covered entities”.\(^11\) Cloud-computing services providers that process or store protected electronic medical records,\(^12\) under the HITECH Act, are subject to certain civil and criminal penalties if they fail to comply with HIPAA’s stringent and extensive Privacy and Security Rules.\(^13\)

While this new legislation offers strong privacy and security protections for patients’ electronic medical records that are stored and transmitted using cloud-computing technologies on Health Information Networks, the HITECH Act failed to address the complex problems that have continued to plague HIPAA relating to the actual enforcement of the Privacy and Security Rules. This issue with enforcement stems from the HIPAA’s lack of any private right of action for aggrieved individuals,\(^14\) a financial cap on total amount of fines at only $1,500,000.00 per year,\(^15\) and the continued slow pace of enforcement by the United States Department of Health and Human Services Office for Civil Rights (OCR).\(^16\) Therefore, because the legislation lacks necessary enforcement measures and mechanisms, it creates a concern over whether cloud-computing service providers, as business associates under HITECH, will actually implement any
of the provisions set forth in HIPAA’s Privacy and Security Rules. The lack of enforcement measures in HIPAA ultimately undermines its ability to adequately protect the privacy and security of individual’s electronic medical records that are stored, processed, and analyzed via cloud-computing technologies.

This paper begins by providing some background of the general benefits of implementing cloud computing services, the pressing need for privacy in one’s electronic medical records, and how the recent amendments to HIPAA have altered the legal responsibilities of cloud-computing service providers with how they protect electronic medical records stored on cloud-based Health Information Networks. Next, Part II will discuss how implementing cloud-computing services in the healthcare industry will likely impact the security and privacy of electronic medical records, and how HIPAA attempts to alleviate these legitimate concerns. Finally, Part III will demonstrate how and why HIPAA fails to adequately protect electronic medical records in the cloud because of feeble enforcement of HIPAA’s privacy and security provisions caused by a lack of a private right of action, the perverse incentives caused by too small of a cap on total yearly fines, and the government’s failure to aggressively prosecute HIPAA related infractions. This paper will argue that HIPAA’s enforcement mechanisms should be amended to allow individuals to bring private actions against covered entities and business associates who violate the terms and conditions of HIPAA, in a similar fashion to the qui tam actions allowed under the False Claims Act, to increase HIPAA’s enforcement and thereby alleviate some of the privacy and security concerns regarding electronic medical records, which have been expounded by the implementation of cloud-computing technologies.

I. BACKGROUND

A. The Benefits of Cloud Computing

The term “the cloud” has long been used by data communications professionals to refer to imprecise aggregations of wide-area data telecommunications networks through which peer-to-peer data communications occur between computational devices. A blurring of the distinction between communications and computing functions, particularly through the increased use of software as a service (SaaS), has led to the adoption of “cloud-computing” to refer to wide-area computational resources in addition to communications. Just as the network “cloud” implies arbitrary and imprecise routing data through the network, “cloud-computing” implies a similar imprecision over which or how many computational resources would have access to that data. This introduces many advantages in reduced costs and increased flexibility for both data suppliers and consumers, but it also makes it more difficult to determine and control what privacy safeguards are needed to ensure the privacy of the data that is processed or stored in “the cloud.”

A significant advantage to cloud computing is that it allows companies to lower costs by eliminating the need to acquire their own computing services, network infrastructure, and workforce to maintain the computer networks inside their offices. Traditionally, companies had to purchase enough processing power and storage space to account for periods of peak activity, but during normal operations much of that expensive capacity would be “idle and unproductive.” Cloud services and network infrastructure, however, can now be purchased on a month to month basis from third-party providers rather than purchasing all the network
equipment at an upfront cost, and can better accommodate businesses needs during periods of peak activity. Another benefit of cloud computing is that it allows companies to acquire the capability of utilizing computer functions that otherwise would not be available due to the prohibitive costs involved with owning and running multiple servers. Additionally, service providers can offer helpful services such as tech-support, which will allow companies to no longer be forced to maintain a dedicated IT staff. This in-turn will mean that companies who switch to cloud computing technologies will not only receive immediate financial benefits, but they will also be able to cut down on many long term costs associated with their computer networks.

A second advantage is that cloud computing service providers are able to offer users access to the “cloud of computers” via the Internet over a user’s personal computer. Therefore essentially, cloud-computing technologies allow the user to access their applications and data that are stored on the cloud “anywhere”. This gives users the ability to store vast amounts of data on remote servers, and have access to powerful computer applications, platforms and other services, all of which can all be delivered over the Internet. This allows businesses and individual users to easily collaborate and share information, even when they are in remote locations. This same technology also allows employees to work from home and have the same access to their work computers. Users also have the capability to update data sets frequently, and to monitor when such updates occur. This can help to ensure accuracy and thoroughness for any data that is stored or collected on the cloud.

Finally, the use of third-party servers to store information on multiple storage sites in remote locations helps protect the integrity of the data and information that is stored on the cloud. For instance, if a server were to malfunction and stop working, than the data could likely be retrieved from an alternate server site instead of being destroyed by the malfunction. Additionally, this lowers the risk that a natural disaster such as a hurricane, earthquake, or flood could cause a catastrophic loss of data. Because cloud-computing services can, and do store data and information in multiple locations, it ultimately protects the integrity of the data by always having a backed up server.

There are many benefits to using cloud-computing technologies to industry and individuals alike, and these benefits also impact the healthcare industry and individuals’ healthcare experiences. The use of cloud computing to store patient’s electronic medical records will provide invaluable benefits to the health profession. Patients will be able to transfer their care between doctors and insurance companies with greater ease and flexibility. Patients may also be able to easily view their medical records, which would allow for corrections and help to further insure the accuracy of a patient’s medical record. Doctors will not have to order wasteful tests that have already been completed; they will also have the ability to collaborate with other physicians and healthcare professionals on patients’ medical records allowing for greater accuracy and thoroughness, and doctors will generally be able to treat patients with increased speed and efficiency. Furthermore, the overall costs of producing and storing literally billions of pages of medical records will become significantly lower because of the cost benefits that cloud computing services offer, and the integrity of medical records will be better protected from natural events that would normally destroy any paper records. All of these benefits of storing private medical data in “the cloud”, however, do come at the potentially steep cost of dangerously exposing patients’ private medical records to unauthorized parties.
B. Privacy Concerns Related to Medical Records

The medical profession and modern American jurisprudence have both recognized the necessity for maintaining patients’ privacy. Physicians, for example, have professional ethics rules that require them to hold their patients’ health information in confidence. One of these professional ethics rules established by the American Medical Association’s Code of Medical Ethics, for instance, provides that, “The physician should not reveal confidential information without the express consent of the patient, subject to certain exceptions which are ethically justified because of overriding considerations.” Furthermore, the modern Hippocratic Oath has also recognized the necessity of maintaining the privacy of a patient’s medical history. As one modern version states, “What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about.”

American courts have gone so far as to cite to the Hippocratic Oath’s concern for patient privacy as the basis for the court to recognize the interest in protecting the confidentiality of the physician-patient relationship. In McCormick v. England, a patient sued her former family physician for disclosing information about her emotional health during her divorce proceedings. The physician moved the court to dismiss the patient’s claim for a failure to state a cause of action. The court in McCormick, however, found that physicians have a duty of confidentiality to their patients, and therefore the patient had a cause of action against her physician for breaching this duty. In coming to this conclusion, the court reasoned that, “The belief that physicians should respect the confidences revealed by their patients in the course of treatment is a concept that has its genesis in the Hippocratic Oath, . . . [and] that the confidentiality of the physician-patient relationship is an interest worth protecting.” The court found that this duty of confidentiality, espoused in the Hippocratic Oath, encourages the uninhibited communications between a physician and his or her patient and is therefore beneficial to the patient who seeks treatment.

In Horne v. Patton, a physician disclosed information to the patient’s employer, contrary to the patient’s express instructions. The patient alleged that the physician-patient relationship constituted a confidential relationship, that the physician therefore had a fiduciary duty to maintain this confidentiality, that the unauthorized release of information breached the fiduciary duty, and further, that it violated the Hippocratic Oath, constituting unprofessional conduct. The Supreme Court of Alabama held that a confidential relationship exists between a physician and patient, and that this relationship imposes a duty upon the physician to not disclose information concerning the patient obtained in the course of treatment. The court reasoned that it is “important that patients seeking medical attention be able to freely divulge information about themselves to their attending physician without fear that the information so revealed will be frivolously disclosed . . . .”

Beyond just relying on the Hippocratic Oath as establishing a right to privacy in one’s medical records, Federal Courts have also taken up the issue of whether the Fourteenth Amendment protects an individual’s private medical records. The United States Court of Appeals for the Third Circuit in Doe v. Delie, building off the Supreme Court’s interpretation that the Constitution protects certain privacy rights, found a constitutional right to private medical records. In Delie, an HIV-positive inmate brought an action against prison officials
alleging violations of his right to medical privacy under the Fourteenth Amendment and State law, after the prison officials failed to keep his HIV-positive status confidential. While the court in Dele ultimately granted the defendants qualified immunity defense, the court did hold “that the Fourteenth Amendment protects an inmate’s right to medical privacy . . . ” Additionally, the court went on to state that, “We have long recognized the right to privacy in one’s medical information: ‘There can be no question that . . . medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection.’”

Additionally, a majority of States have privacy laws established in either statute or common law that protect the privacy of medical records and the physician-patient relationship. The privacy of medical records is held to be sacrosanct largely because of the risks associated with the wrongful disclosure of medical records to unauthorized third parties and the benefits of encouraging an open and complete discourse between a physician and her patient. Encouraging disclosure has the benefit of ensuring proper treatment by allowing the physician to gain a better understanding of the patient’s past medical history. This could help the physician to not only be able to better diagnose the patient, but it will also allow the physician a better opportunity to identify any adverse side effects that may result from any treatment methods. While at the same time, some of the risks of wrongful disclosure include potential discrimination resulting from the misappropriation of private medical records, medical identity theft, and the risk that medical records may be wrongfully altered to represent conditions that a patient may or may not have.

Together, both the risks and benefits of maintaining the privacy of medical records are well worth the effort and expense due to the damage that can potentially come from an illicit or accidental disclosure. For instance, the risks associated with medical identity theft include free-riding off of other’s medical insurance coverage, hackers searching for financial data located within one’s medical records, and even malicious alterations to one’s medical record. The potential risk for discrimination is so high because an individual’s health information can be used by employers to help determine future productivity, by financial firms and lenders with a stake in the individual’s financial future which can reasonably be assumed to be directly affected by the individual’s overall health, by drug companies that may wish to directly market to individuals based on their health status, by blackmailed who wish to extort money to not publicize or otherwise disseminate damaging medical facts, and even by charlatans who may wish to financially prey on those they find to be vulnerable.

Furthermore, the risks associated with the wrongful alteration of one’s medical file are potentially devastating. Healthcare providers often rely on medical records in diagnosing and treating patients. When errors in a patient’s medical record are introduced as a probable consequence of relaxed security or compromised privacy, a patient can be seriously injured or die from an incorrect treatment or misdiagnosis that could have otherwise been prevented. Therefore, if privacy concerns relating to medical records are not adequately met there could be not only financial burdens, but also more importantly people could potentially die. These risks make it imperative that sensitive health information remains private and secure. The many risks associated with any erosion of security and privacy for medical records
are not purely financial; they also include risks to human life. Therefore, the maintenance of the privacy and security of medical records is not a luxury; it is a necessity.

C. How HITECH Amended HIPAA to Include Business Associates in the Privacy and Security Rules

Congress originally passed HIPAA with a goal to protect the privacy of patients’ electronic medical records, and HIPAA still operates as the primary federal regulation for maintaining the privacy and security of private health information. When Congress initially passed the HIPAA legislation in 1996, Congress originally declined to create specific privacy or security rules within the act. Rather, Congress delegated this authority to the Secretary of the United States Department of Health and Human Services (HHS), who then created the regulations relating to the privacy and security standards for electronically stored medical records known the Privacy and Security Rules. These new regulations created by the Secretary of HHS originally only regulated how “covered entities” could use and disclose private medical information, and the level of security that electronic medical records must receive.

Cloud computing service providers, however, constitute “business associates” under HIPAA because they operate under contract and in conjunction with covered entities to provide services relating only to the storage and transmission of electronic medical records. Therefore, this originally meant that because cloud computing service providers are not covered entities they were not subject to the Privacy and Security Rules, despite the fact that, as business associates, cloud computing service providers often have similar access to the same private electronic medical records as covered entities.

Realizing this gap in privacy protections, Congress addressed the potential privacy and security concerns of not holding business associates to the same Privacy and Security Rules as covered entities through certain provisions in HITECH Act. Under the new law, business associates now have many of the same privacy and security responsibilities to protect patients’ private medical records that traditionally were imposed solely on covered entities under the Privacy and Security Rules. Furthermore, business associates now face similar threats of criminal and civil penalties for violating these responsibilities as covered entities.

Under the Privacy Rule, a covered entity may only disclose protected health information to a business associate if they obtain satisfactory assurances that the business associate will appropriately safeguard the privacy of the protected health information. Furthermore, covered entities must form contracts with business associates, and these contracts must enforce certain privacy specifications that strictly determine the circumstances in which a business associate may disclose private health information. Before the HITECH Act, however, only covered entities were subject to fines from OCR for any failure by a business associate to follow the mandated privacy provisions in their contracts with the covered entity. Under the HITECH Act, however, Congress mandated that OCR apply these same fines for privacy violations to these business associates as well. Therefore, HIPAA now subjects business associates to civil and criminal penalties if they fail to follow proper disclosure requirements stipulated in their contracts with covered entities.
Under the newly amended Security Rule, business associates now face similar requirements and restrictions as covered entities had under the original HIPAA legislation. Specifically, business associates must now implement and maintain certain “policies and procedures to prevent, detect, contain, and correct security violations,” and they must closely monitor access to patients’ medical records. They must limit physical and electronic access to the electronic information systems and the facilities in which they are housed, while guarding against all unauthorized access. Additionally, business associates must implement internal policies to ensure the confidentiality, integrity, and availability of all electronic protected health information that they receive, maintain, or transfer. Finally, they must now protect against any reasonably anticipated threats or hazards to the security or integrity of protected health information. Conclusively, under the HITECH Act business associates are now required to assume a much larger responsibility in protecting the security and integrity of protected electronic medical.

The new HITECH Act also adds new provisions to the Security Rule, which mandates, in part, that business associates and covered entities notify individuals when a breach in security or privacy is suspected. Under the HITECH, a business associate must now notify the covered entity of each individual whose medical records have been or are reasonably believed to have been wrongfully accessed, acquired, or disclosed as a result of a breach. A covered entity, upon receiving information of a security breach from the business associate, is required to provide any individuals affected by the potential security breach complete notice of the nature of the breach and what protected medical records were potentially exposed. These notices to individuals must provide a brief description of the breach, the material that became unsecured, the steps that an individual can take to protect themselves, and a description of the investigatory efforts of the covered entity. Covered entities must also submit notice of each breach to the Secretary of HHS, who is then to submit an annual report to Congress regarding all notices of breaches in security and privacy received from covered entities.

There are also new restrictions on business associates regarding the sale of electronic medical records to third parties. Under the HITECH Act, business associates cannot receive payment in exchange for an individual’s protected health information unless the covered entity receives valid consent from the individual. Business associates are allowed, however, to reveal private health records in exchange for compensation, but only for the purposes of public health activities, research, treatment of an individual, certain business management and administrative activities, and providing individuals with copies of their protected health information. Therefore, activities like marketing individuals’ private health information to private companies are now strictly prohibited under HIPAA, unless the covered entity has obtained express consent from the individual.

Perhaps the most significant changes to the original HIPAA legislation, however, come in the ways in which the statute can now be enforced. Importantly, business associates are now subject to the same fines as covered entities for violating the Privacy and Security Rules. Under the HITECH Act, OCR can now enforce the privacy and security provisions of a business associate’s contract with a covered entity through the use of these statutory fines. Under HIPAA, the statutory fines for each separate violation of any privacy provision in a business associate’s contract with a covered entity ranges from $100.00 to $50,000.00, with a yearly maximum fine of $1,500,000.00 for any given business associate. Effectively, the HITECH
Act forces business associates to maintain the administrative policies required under the Privacy and Security Rules to help insure that medical records remain private. Furthermore, State Attorney Generals are now also allowed to file HIPAA enforcement actions, along with OCR, for any violations of the Privacy or Security Rules that are not properly reported to the corresponding State’s Attorney General’s office.

Essentially, the HITECH Act has significantly altered the responsibilities and duties that cloud computing service providers, as business associates, have in protecting individual’s medical records and data. By amending HIPAA to hold business associates to the same privacy and security standards that previously only applied to covered entities under the threat of steep fines, the HITECH Act has increased the costs and burdens on cloud computing services providers to enter into the healthcare field. While not enough time has passed to determine exactly whether these increased burdens imposed upon cloud computing service providers will ultimately lead to increased security and privacy for medical records that are stored or traversing in the cloud, the new HIPAA legislation will have real implications on cloud computing service providers. The actual enforcement of these new provisions, however, remains an ever-real concern.

II. MAINTAINING THE PRIVACY OF ELECTRONIC MEDICAL RECORDS ON THE CLOUD

A. Why Cloud-Computing Places the Privacy of Electronic Medical Records in a Precarious Position

With the advent of cloud computing, companies and governmental agencies have begun taking advantage of the cheap, relatively secure, off-site, electronic storage options provided by the technology. The healthcare industry has also taken off with this trend and is rushing to implement cloud-computing services in an attempt to lower overall costs and to give patients more autonomy and control over their personal health records. Despite the significant benefits cloud computing services offer the healthcare industry, there are many important privacy concerns that face all data stored on cloud-networks that have yet to be overcome. While cloud computing service providers have the technology and capability to store a plethora of information on remote servers that can be accessed anywhere in the world, a breach could be potentially devastating. Despite the fact that data stored on cloud-servers is relatively secure, if a breach in private data occurs through either an accidental exposure or an intentional breach, the data can no longer be considered private because of the ease of transferring large amounts of data in electronic form. Furthermore, locating the culprit or cause of the breach can be difficult, as evidenced through many of the leaks that have already occurred. Therefore, by moving towards implementing cloud-computing technologies, the healthcare industry is placing the privacy of millions of electronic medical records at risk of improper disclosure and dissemination.

Ironically, the very benefit of being able to have access to vast amounts of data with a simple Internet connection also opens the door to those who want to intentionally breach the private cloud-networks for various reasons. This is a new, yet blossoming issue, as there have been a growing number of intentional breaches in the healthcare industry over the past two years. These breaches highlight the risk of cyber-attacks and hacking that electronic medical records face when stored in electronic form on cloud-base Health Information Networks.
For example, the Virginia Department of Health Professions experienced a cyber-attack in late April 2009, which resulted in the theft and possible exposure of more than eight million electronic medical records and thirty-five million electronic prescription records from their internal Health Information Network. The hacker who committed the attack demanded that the State pay him $10,000,000.00 for the return of the information, after he allegedly stole all the data and deleted the State’s electronic backups of the data stored on the its network. Furthermore, the State took over a month to issue any breach notices for the 500,000 individuals who had their social security numbers exposed, and the State never bothered to notify any additional individuals whose private health information may have been released.

Cyber-attacks have also occurred in other industries outside of healthcare, which still works to show some of the insecurities of cloud-based networks. In December 2009, Google, Inc. discovered that a significant and sophisticated cyber-attack had occurred against some of its cloud-networks. This wide-scale cyber-attack only resulted in the theft of certain intellectual property from Google and a failed attempt to obtain unauthorized access to e-mail accounts of Chinese human rights activists. The attack, however, demonstrated the vulnerabilities of cloud-networks even when they are run and protected by powerful and technologically advanced firms such as Google. For Google had not only failed to immediately recognize that an attack had occurred, but they were also unable to discover with certainty the culprit of the attack, or the exact weakness in their cloud-network that allowed the breach to occur, which leaves one to ponder whether Google can prevent a similar attack in the future.

Another example of a cyber-attack is the one that occurred against the Sony PlayStation network in April of 2011. The attack targeted Sony’s data center in San Diego, California, and resulted in the breach of millions of customers’ personal information. The personal data exposed by the attack included customers’ names, addresses, birthdates, passwords, login names, purchase and billing history, and even credit card information leaving millions exposed to the potential of identity theft. Additionally, the attack forced Sony to temporarily close down their cloud-network for a period of days before they were able to locate the source and cause of the breach. Sony, however, never found or located the actual culprits of the breach, so there is no way of telling what information was actually gathered by the attack or who had been harmed by the breach.

While these cyber-attacks where conducted over the Internet, there is also a risk those who have legal access to the data stored on a cloud-network can wrongfully disseminate data stored on cloud-networks. Within the healthcare industry the threat of wrongful dissemination by healthcare professionals has long been an issue. In Yath v. Fairview Clinics, an employee wrongfully accessed the private electronic medical records of a patient whom the employee personally recognized. Discovering that the patient had contracted a sexually transmitted disease from a new sexual partner who was not the patient’s husband, the employee informed the patient’s husband of her sexually transmitted disease and created a website to disseminate the patient’s entire medical record to the public at large.

Another issue with wrongful disclosures involves nosey employees who wish gain access to the private lives of celebrities. In March 2009, fifteen employees of Kaiser Permanent were
fired and another eight were reprimanded for wrongfully viewing the medical records of Nadya Suleman, who had recently become a tabloid sensation after giving birth to octuplets.157 There have even been reports of other celebrities, such as George Clooney and Britney Spears, who have had their medical records wrongfully accessed and viewed by curious employees of covered entities and business associates alike.158

In addition to the risks of cyber-attack and wrongful dissemination, another potential issue in using cloud-networks to store private health information is the actual physical security of the hardware devices used by the service provider.159 These hardware devices have the ability to store millions of data sets and records, all of which have the potential of exposure if there are not certain physical security measures taken. Giving credence to this threat of physical exposure, in early 2006 an employee with Aetna Inc.160 had his laptop stolen from his car in a public parking lot.161 Because the laptop contained electronic medical records stored on its hard drive, this physical breach alone exposed the electronic medical records of over 38,000 people,162 which included the private medical and financial data of roughly 35,253 employees of the Department of Defense.163

What makes the idea of a physical breach to a cloud-network storage site even more unsavory is the potential for a much larger set of data to be reached. Unlike a personal laptop that has relative limits to how much data can be stored on it, a cloud-network server station can hold almost infinitely more information. Therefore, a physical breach of network security at a cloud-network storage facility has the potential of exposing far more medical records than were exposed by the Aetna employee.

Partially because of the sheer difficulty of protecting sensitive data stored on cloud-networks, service providers, such as Google, decline to offer warranties that information stored and processed on their cloud-network infrastructure will be safe from cyber-attacks, wrongful dissemination or disclosure, or from physical breaches.164 Despite these vulnerabilities, however, cloud-computing service providers still encourage users to store their sensitive information on cloud computing networks, and these service providers often make representations that their services and networks are secure, despite known privacy risks and threats of future cyber-attacks.165 This particular claim of cloud-based network security by Google has become the subject of a Federal Trade Commission complaint filed by the Electronic Privacy Information Center that, among other things, asserts Google has misrepresented their privacy controls for individuals’ sensitive information.166

While cloud-networks are generally a very secure method of storing and processing electronic data, the breaches discussed above support the proposition that securing and ensuring the privacy of any data stored on cloud-networks is nearly impossible. If companies such as Google and Sony and State governments are unable to protect individuals’ private health data, how can other cloud-networks be expected to properly secure electronic medical records without stringent regulations and actual enforcement of these regulations? The use of Health Information Networks will place large quantities of data into one location in cyberspace, which can be accessed by those with either the skill to break into the network or those who are improperly trusted to view the information. This will subsequently place at risk the privacy of millions of electronic medical records. Electronic medical records stores not only the intimate
details of peoples’ lives, it also stores billing information and personal identification information that can expose people to the potential for identity theft if the records are not properly protected.\textsuperscript{167}

Storing medical records in an electronic format on cloud-networks expounds many traditional privacy concerns surrounding traditional paper medical records because the electronic format of the record allows it to be transmitted, viewed, dissected, and interpreted with ease. Interestingly, many of the benefits to cloud computing—speed, accuracy, efficiency—also make cloud computing extremely risky in regards to privacy. All the information stored on the cloud can be accessed electronically, and is therefore exposed to cyber attacks,\textsuperscript{168} wrongful disclosure and dissemination, and even traditional breaches in physical security.\textsuperscript{169} If a database that is stored on a cloud-based network is breached, all the electronically stored private medical information could be stolen and disseminated with vastly less effort and cost than traditional paper medical records.

Another compelling concern with placing private medical records onto cloud-networks in an electronic format is the threat of what is known as data mining. Data mining is a complicated “process of identifying valid, novel, potentially useful, and ultimately understandable patterns of data,”\textsuperscript{170} that uses complex algorithms and supercomputers to scan vast amounts of electronic data.\textsuperscript{171} Data mining is popular amongst both the private commercial sector to develop targeted marketing tools\textsuperscript{172} and the federal government to gather intelligence.\textsuperscript{173} While data mining can be a useful tool for companies and the government when used ethically, its use can become malevolent when the data set includes wrongfully obtained or unauthorized access to private electronic medical records.\textsuperscript{174} For example, if a cyber attack occurred on a cloud-based, Health Information Network that allowed someone to gain at least temporary access to the material, they could then quickly mine the data for useful information such as social security numbers, permanent health ailments, insurance premiums, and other factors that relate to one’s financial or medical history. Malevolent data mining of cloud-networks that store private electronic medical records would allow for the most sensitive, valuable information to simply be plucked out of the database and used for any purpose. Essentially, once a cyber-attack, wrongful access, or physical breach occurs that exposes individuals’ electronic medical records to data mining, the privacy of these electronic records will be effectively eliminated.

One significant security advantage to using cloud-networks to store medical records, however, is that electronic medical records may be more easily monitored than traditional paper records.\textsuperscript{175} Unlike traditional paper records, when a copy is made of an electronic record the storage system may be able to track the copy or notify the user that a copy has been made, whereas it is nearly impossible to detect when a copy of a paper medical record has been made.\textsuperscript{176} This gives the service provider the ability to warn anyone whose privacy may have been jeopardized, and allows the both to take corrective measures to prevent further harm. This privacy benefit alone, however, does not offset all the other privacy concerns associated with storing electronic medical records on cloud-networks.

Despite the privacy concerns associated with the use of cloud computing technologies, many healthcare providers have decided that the cost cutting benefits of cloud computing outweigh the threats to privacy and are beginning to make the switch to using cloud computing
networks to electronically store patient’s medical records. Microsoft and Google have both created cloud-based data storage services for healthcare entities, and healthcare entities such as the Cleveland Clinic and Kaiser Permanente have begun implementing these services. With all of the risks associated with private medical records stored and processed in the cloud and the implementation of cloud computing technologies by healthcare entities, it becomes essential that the Privacy and Security Rules of the HIPAA regulation be adequately enforced to ensure compliance and to ensure the privacy of sensitive medical records.

B. How New HIPAA Regulations Fail to Adequately Protect the Privacy of Electronic Medical Records that are Stored in Cloud-Networks

The HITECH Act significantly alters the privacy and security responsibilities that all cloud-computing service providers who operate in conjunction with covered entities to store, process, analyze, and transfer private electronic medical records. Congress, perhaps realizing the privacy concerns relating to use of cloud-networks, made an assertive effort to protect the privacy of electronic medical records by regulating Health Information Networks under HIPAA’s Privacy and Security Rules. Under these new regulations, Health Information Networks now must keep stringent privacy and security protocols to protect the electronic health data, as discussed above in Part I.C., and they must also notify the covered entity of any potential breach along with intimate details of the breach and all data that may have been exposed. Furthermore, many of these security and privacy measures, if fully observed, would provide fairly adequate privacy protection for electronic medical records stored on any cloud-network. Thereby, the HITECH Act appears to reconcile many of the privacy and security concerns that exist with storing sensitive electronic medical records onto cloud-networks, which in turn allows the healthcare industry to move forward and reap the financial and practical benefits of cloud-computing technology.

While HIPAA, after HITECH, now provides stringent security and privacy protections for electronic medical records stored on cloud-networks, the legislation still fails to adequately protect patients’ privacy in the cloud for three primary reasons. First, HIPAA does not allow for any type of private right of action for individuals whose privacy is affected by HIPAA violations. Second, OCR has traditionally failed to adequately enforce HIPAA by only rarely punishing companies that fail to comply with the legislation, and it is too early to tell what effect State enforcement of HIPAA’s Privacy and Security Rules will have. Finally the present cap on individual yearly fines severely hinders the deterrent effects intended by the fines, and thus does not create the proper incentives to motivate cloud-computing service providers to implement the requirements of the Privacy and Security Rules.

To begin, perhaps the greatest flaw with HIPAA is that the statute does not expressly provide for a private right of action for any violations of the act, and courts have unanimously refused to find a private right of action for individuals when there are violations. Under HIPAA, the only form of legal redress an individual has when their privacy has been violated is to file a complaint with the Office for Civil Rights (OCR) within HHS, who then is in charge of processing the complaint and following through on any potential prosecution. Additionally, after the HITECH Act, State Attorney Generals may now also prosecute HIPAA violations; however, it is too early to tell what impact, if any, this enforcement mechanism will have.
Even after the HITECH Act, HIPAA still does not grant individuals any financial incentive to report any violation, it does not grant individuals any private right of action and it does not ensure that an individual’s grievance will even be prosecuted to the full extent of the law. Therefore, when an individual’s privacy rights have been violated because of a HIPAA infraction by either a covered entity or business associate, that individual must rely on an outdated patchwork of State statutes and common law to achieve legal redress. Furthermore, because Health Information Networks are not physicians or even healthcare providers, courts are likely to find that no common law duty even exists to maintain the privacy or security of the medical records stored on the cloud. While there are many risks and potential harms that could occur from a loss of privacy in one’s medical records, it can often be difficult to determine the exact extent of damages that occur from any single breach.

While the lack of any private right of action for HIPAA violations reduces legal costs, thereby making it easier for service providers to offer cloud-networks to the healthcare industry, it fails to create the proper incentives for implementation of the Privacy and Security Rules. This is important because the problem with HIPAA is not that it fails to create adequate security and privacy standards for protected health information stored on cloud-networks; the problem is that these standards can be ignored because there are few actual consequences for the large corporations that choose to ignore them. If service providers were faced with the threat of higher fines based off the number of records exposed due to a violation, they would almost be forced to ensure their complicity with HIPAA or risk financial disaster.

Critics to the idea of creating a private right of action under HIPAA argue that it will “open a flood of litigation.” While there would likely be an increase in litigation, the litigation would serve the legitimate purpose of protecting patients’ privacy rights. Collectively, all the potential harms and risks of discrimination associated with a lack of medical privacy justify an increase in judicial cost, and the utility of protecting medical privacy in Health Information Networks outweighs any fundamental concerns over judicial economy. Furthermore, the exact impact of a private right of action under HIPAA on the healthcare industry at large is unclear, but there are clear implications of under enforcement by not having any sort of private right of action. Therefore, because one can understand the severe harms that do occur from a lack of privacy in one’s medical records, Congress should take major strides to protect that privacy even if this means a risk of increased costs or decreased judicial efficiency.

Arguably, allowing for a private right of action would help increase the actual implementation of the Privacy and Security Rules; however, Congress has decided to leave HIPAA’s enforcement solely in the hands of OCR and State Attorney Generals. This decision has proven to be a major mistake if Congress was indeed serious about protecting patients’ privacy in their electronic medical records. For while OCR has been able to handle consumer complaints and claims to correct problems ad hoc, they have not aggressively sought to press criminal or civil charges against companies for their violations, and it is too early to be able to determine the effectiveness of State prosecution.

Highlighting this lack of aggressive prosecution is the statistic that OCR has only ever placed a handful of major sanctions against companies for violating HIPAA. The first ever major sanction came on July 16, 2008, after OCR entered into a resolution agreement with Providence Health & Services (Providence) in which Providence agreed to pay $100,000.00 in fines and implement a strong corrective action plan to correct multiple HIPAA violations which
resulted in the compromising of 386,000 patients protected health information.\textsuperscript{191} The second major sanction took place on January 19, 2009, when OCR was able to reach a settlement agreement with CVS Pharmacy, Inc. to settle multiple complaints that involved the privacy of millions of medical records.\textsuperscript{192} \textit{Per} the agreement CVS agreed to pay $2,250,000.00 in fines and to implement a strong corrective action plan to correct their multiple HIPAA violations.\textsuperscript{193} Another recent major sanction, was revealed in a July 27, 2010 press release from OCR, in which it was released that Rite Aid Corporation and its 40 affiliated entities agreed to pay $1,000,000.00 and to implement a strong corrective action plan to correct their multiple HIPAA violations from employees throwing away personal health information into public trashcans.\textsuperscript{194}

The largest HIPAA fine ever administered came in February 2011, when OCR issued a $4,300,000.00 total fine against Cignet Health Care of Temple Hills (Cignet) for a litany of HIPAA violations that occurred over a period of years.\textsuperscript{195} In a Notice of Proposed Determination issued by OCR on October 20, 2010, OCR found that Cignet violated 41 patients’ rights by denying them access to their medical records when requested between September 2008 and October 2009.\textsuperscript{196} These patients individually filed complaints with OCR, initiating investigations of each complaint and resulting in fines of $1,300,000.00 for this violation alone.\textsuperscript{197} OCR also found that Cignet failed to cooperate with OCR’s investigations on a continuing daily basis from March 17, 2009, to April 7, 2010, and that the failure to cooperate was due to Cignet’s willful neglect to comply with the Privacy Rule.\textsuperscript{198} This violation of failing to comply with HIPAA’s Privacy Rule led a maximum fine of $3,000,000.00 for the 13 months of non-compliance.\textsuperscript{199} Importantly, however, one must note that this has been by far the largest fine ever administered by OCR, and there is no indication how regularly these types of fines will be administered against violators in the future.\textsuperscript{200}

The overall slow pace of sanctions that OCR has been able to deliver belies the lack of enforcement issues that face proper HIPAA enforcement and implementation of the Privacy and Security Rules. To put the point in relief; from the time compliance with HIPAA became mandatory in April of 2003 through January of 2011, OCR has received over 56,119 Privacy complaints under HIPAA’s Privacy Rule, of which only three resulted in major fines,\textsuperscript{201} and they have received 207 security complaints under HIPAA’s Security Rule with no indication of whether any fines have been given for any violations under the Security Rule.\textsuperscript{202} While OCR claims that it has been able to “resolve” ninety-one percent of all complaints, it has only officially issued large fines to three companies.\textsuperscript{203} Of the 56,119 Privacy complaints that have been reviewed,\textsuperscript{204} 12,161 resulted in an investigation and ended with “enforcement.”\textsuperscript{205} The “enforcement” that OCR refers to, however, includes the recommendation of corrective actions to the violating party, and does not necessarily include any civil or criminal penalties.\textsuperscript{206}

Recommending corrective actions, however, does not even reach the condemnation of a slap on the wrist. As evidenced by the large number of complaints, OCR’s actions have not been effective in enforcing HIPAA’s Privacy and Security Rules, which is placing the privacy of protected electronic medical records at risk. OCR must take real actions to enforce HIPAA’s Privacy and Security Rules, or they risk allowing companies to ignore mandatory rules and regulations regarding the security and privacy of electronic medical records. Additionally, it is too early to be able to predict how well State Attorney Generals will be able to enforce HIPAA mandates; however, the current results look somewhat promising.
In early 2010, Connecticut’s Attorney General, Richard Blumenthal filed the first (and at this time only) lawsuit utilizing HIPAA’s new state enforcement power against Health Net, Inc. The lawsuit stemmed from a theft of a portable computer disk drive from one of Health Net’s offices. The disk drive contained the electronic medical records, social security numbers, bank account numbers, and other identifying information of roughly half a million people. Health Net violated the notice provisions in the Privacy Rule by waiting to notify individuals of the breach until six months after it occurred. Health Net ended up settling the lawsuit with the State in June 2010. In the settlement, Health Net agreed to pay $250,000 in fines to the State, implement a detailed corrective action plan, provide identity theft insurance for the individuals’ whose identities were stolen because of the data breach, and run free credit reports on all those effected for the next two years.

While this is a good start for State enforcement of HIPAA, this is only one case and only time will tell if there are continued regular enforcement efforts by the States. Furthermore, State enforcement cannot be solely relied upon because of the inequities involved. Certain individuals who happen to live in states where their Attorney Generals are more active will be better protected than those individuals who live in states where the Attorney Generals are more apathetic towards prosecuting HIPAA violators. All in all there needs to be an adequate federal regulation to ensure that all Americans, not just those lucky few with an active Attorney General, are afforded the foundational right to privacy in their medical records.

Finally, one of the most significant changes to the original HIPAA legislation is that cloud computing service providers who constitute business associates are now subject to the same fines for violating the Privacy and Security Rules that covered entities have faced since the rules’ inception. Under the HITECH Act, OCR can now enforce the privacy and security provisions of a business associate’s contract with a covered entity through the use of statutory fines. This is an instrumental change to the law because before the HITECH Act, business associates simply were not subject to any statutory or regulatory fines for violating the privacy and security terms of their contracts with covered entities, or for negligently exposing patients’ medical records to unnecessary privacy risks. Therefore, by granting the power to OCR to fine business associates under the HITECH Act, Congress has finally given HIPAA some “teeth” to help protect the privacy and security of electronic medical records that are stored and processed by cloud computing service providers.

There is, however, still lack of deterrence effect even with the implementation of the fines because the cap on dollar amount of fines collected in a year is too low for the massive corporations that offer cloud-computing services such as Microsoft, Amazon, and Google. Generally, only large companies will likely even have the capital-structure and capacity to create the infrastructure that is needed to offer the large-scale cloud computing services required for cloud-based Health Information Networks. While the maximum limits for fines is pragmatic for smaller healthcare entities such as local hospitals and health clinics, which cannot easily absorb a $1,500,000.00 fine and likely view this as a huge financial incentive to comply, the law does not take into account the new corporate giants that are entering into the health record storage-field who will not be as financially incentivized by the size of the fine.

By placing a cap at $1,500,000.00 regardless of the egregiousness of the violation or the size of the corporation, Congress has not created a real incentive for cloud computing service providers to implement the provisions as mandated by the Privacy and Security Rules. The
transaction costs alone for these service providers to implement all the necessary provisions under HIPAA could be in excess of the statutory cap. Now, not only must a cloud-computing service provider implement all the privacy and security standards required under HIPAA if they wish to store protected electronic medical records, but for each separate violation of any privacy provision in a business associate’s contract with a covered entity carries with it a fine ranging from $100.00 to $50,000.00,\textsuperscript{215} with a yearly maximum fine of $1,500,000.00 for any given business associate.\textsuperscript{216} Furthermore, business associates are now forced to maintain administrative policies to help insure the privacy of medical records, which potentially could further raise transaction costs.\textsuperscript{217} Also, each suspected breach requires immediate notice to the covered entity of a myriad of details as explained above in Section I.C.

To give an example, if a breach were to occur and millions of medical record were suspected of possibly being exposed, under HIPAA, the business associate would have to give detailed information about each record that was exposed within 60 days.\textsuperscript{218} The costs of a large-scale breach could make it economically prudent to just ignore the breach and take the risk of getting a fine. Because of the grave concerns over the privacy of medical records, it seems important that there should be harsher penalties for those who ignore federally mandated law that is intended to protect this sensitive topic.

Together, the application of the Privacy and Security Rule to business associates gives a new level of privacy protection to individuals whose health information is stored and processed using cloud computing technologies. Certainly these new standards improve upon Congress’ ultimate goal to protect patients’ privacy interest; however, they must first be completely implemented by cloud computing service providers if they are to have any real affect. This implementation will only occur if enforcement of the Rules becomes more prevalent, and the deterrence of the fines and legal costs are significant enough to incentivize cloud-computing service providers to work under HIPAA and not just ignore it. If the Privacy and Security Rules are not implemented by cloud-computing service providers who handle protected electronic medical records, than millions of patients’ personal medical records could be placed at risk. Therefore, there must be an adequate enforcement of Privacy and Security Rules under HIPAA and adequate fines to ensure implementation, otherwise the privacy concerns espoused in the HIPAA legislation risks becoming essentially ignored across the cloud-computing industry.

III. WHY HIPAA ULTIMATELY FALLS SHORT OF ITS GOAL TO PROTECT PATIENT’S PRIVACY INTEREST IN THE CLOUD

While HIPAA’s Privacy and Security Rules both offer strong protections for electronic medical records that are stored on the cloud, the traditional enforcement of these provisions is inadequate to ensure full implementation by cloud-computing service providers. HIPAA’s lack of a private right of action gives individuals little hope of protecting their personal medical privacy once their medical records are stored in the cloud, and the myriad of state common law actions to protect an individual’s privacy in their electronic medical records are largely ineffective and unjust.\textsuperscript{219} Furthermore, OCR’s enforcement of HIPAA’s Privacy and Security Rules has thus far been insufficient given the level of complaints and the egregious nature of
some of the violations mentioned above in Part II.B, and this problem will only be amplified by
the use of cloud computing due to the risks of significantly larger breaches of easily transferable
records. Finally, the current fines for violations under HIPAA are too small to provide a
sufficient deterrent for the large corporations who offer cloud-computing services.\(^{220}\) Therefore,
the current state of the enforcement of HIPAA threatens to undermine the very purpose of its
implementation: to protect the privacy of electronic medical records.\(^{221}\) Only if Congress
amends HIPAA to provide more “teeth” to the legislation will the integrity of private electronic
medical records be adequately protected.

In order to solve this enforcement problem, Congress should look to successful
enforcement mechanisms that exist in other legislation. Particularly, Congress should implement
some of the enforcement provisions of the False Claims Act (FCA) to strengthen the
enforcement capabilities of HIPAA. By modeling HIPAA enforcement after the successful
enforcement measures in the FCA, implementation of the Privacy and Security Rules may finally
occur and patients’ privacy in their electronic medical records may finally be adequately secured.
Specifically, Congress can achieve this goal by amending HIPAA to add a private right of action
measure similar to the FCA’s *qui tam* actions and by increasing and modifying the fine structure
for services that store large number of electronic medical records on cloud-networks.

The FCA prohibits a person from “knowingly” submitting claims or making a false
record or statement in order to secure payment of a false or fraudulent claim by the federal
government.\(^{222}\) Under the FCA, if a person is found to have violated the statute, than they are
liable for a civil penalty for each such claim not less than $5,500 and not more than $11,000,
plus three times the amount of damages sustained by the federal government.\(^{223}\) What is unique
about FCA enforcement, however, is that the government is not the sole actor who can enforce
the provisions of the Act. The FCA also authorizes what are known as *qui tam* actions to be
brought on behalf of the federal government by a private party who has knowledge of any
fraud.\(^{224}\) These private parties, or relators, can share in the monetary recovery paid as part of the
eventual settlement or resolution of the case by filing a complaint against a defendant under seal
with the Department of Justice.\(^{225}\) The amount of monetary recovery that a private party stands
to make is based off of whether the Department of Justice decides to intervene in the case, and
how much the relator’s information leads to a successful outcome in any litigation or settlement,
which can lead to an award anywhere from fifteen to thirty percent of the final settlement or
resolution.\(^{226}\)

What this enforcement mechanism allows for is two fold. First, the fine structure and
legal damages a violator may face are based off the amount of all the false claims, and the actual
number of false claims made. This helps to ensure that the deterrence of filing a claim correctly
matches egregiousness of the claim itself. If a small company erroneously makes a false claim
under the statute, they will face a penalty only in the amount of the fine and treble the damages
caused by the claim. They cannot be subject to tremendously high fines for a simple oversight or
omission, but rather will be punished accordingly for their error. Similarly, if a company makes
many egregious claims repeatedly, they will face stiff fines and penalties with no overall cap on
the amount of fines or damages. This helps to ensure correct deterrence effects of the statute by
making sure the specific punishment fits the specific fine.

Second, the FCA gives individuals a financial incentive to help with the enforcement of
the statue. By allowing individuals to collect a percentage of the final settlement or resolution
for helping the government to prosecute the violators, Congress has given individuals an incentive to act as investigators and whistleblowers for the government. This gives the federal government more information with which to prosecute and punish violators, and helps to further ensure that the FCA is being enforced efficiently. Essentially, individual relators act as an additional enforcement arm along with the DOJ, at no upfront cost to the government.

The large-scale success in the enforcement of the FCA can be seen in the monetary outcomes in favor of the government. For instance, between 1987 and 2010, the U.S. government was able to recover nearly $28 billion. This success has been attributed to the success of many relators and the use of financial encouragement for whistleblowing. Furthermore, enforcement of the FCA has been particularly successful in the healthcare industry where the U.S. government is recovering roughly $15 back for every $1 invested in FCA prosecutions. Again, this is largely attributable to Congress’ decision to allow individuals to file qui tam actions, which help the government to adequately prosecute and enforce the provisions of the FCA.

Many ideas behind the successful enforcement measures in the FCA can be utilized by Congress to strengthen HIPAA’s enforcement measures, albeit in a slightly different fashion. First and foremost, Congress should look to add a qui tam-like private right of action to HIPAA to allow for individual enforcement of the Privacy and Security Rules. Under the FCA, a relator in a qui tam action cannot file a claim on the basis of public information alone, although they do not need to necessarily have personal knowledge of the fraud that occurred in order to file suit. The relator also does not have to suffer any real damages themselves in order to move forward with a complaint, so long as the information relating to the fraud has not been gathered through public information and the government has been injured by the fraudulent action. This requirement, in part, is intended to prevent individuals who only have public knowledge of a fraud from being able to financially benefit from any qui tam action. Qui tam actions under the FCA are meant to encourage individuals with personal information of a fraud to come forward and file what is essentially a whistleblowing complaint to aid the government in enforcement of the FCA.

With HIPAA violations, however, individuals are the ones being damaged by the exposure of their electronic medical records, not the government. Unlike the case with FCA qui tam actions, with HIPAA violations, even if information relating to a violation is gathered through public resources, individuals still have a personal interest in ensuring that their electronic medical records remain private. Individuals, therefore, must be allowed to file complaints on behalf of themselves and others affected by the breach, regardless of whether they have any personal knowledge of any violation so long as they meet other pleading requirements. This option would grant individuals a viable option for legal and economic redress when a company violates HIPAA and thereby exposes electronic medical records to privacy breaches.

Anyone who has been affected by a HIPAA violation should stand to gain from any monetary fine imposed against a corporation, as it is that individual who is personally damaged by a violation that results in the potential exposure of their private health records. Therefore, creating a qui tam like action for HIPAA should be different in nature from the qui tam action promulgated by the FCA. Under this proposal, the parties who file and take part in the prosecution of the violation, whether that is the government or an individual relator, should stand to receive an award equal to a certain percentage of the final resolution or settlement to
incentivize proper prosecution. With this plan, however, all the individuals who were affected by the violation will also receive a percentage of the final resolution or settlement to compensate them for their violated medical privacy. This entails that even if OCR is the only party enforcing a HIPAA violation, individuals who are damaged by the violation will still recover a percentage of the final resolution or settlement. The principles of equity and fairness demand that individuals receive a percentage, regardless of whether they take formal measures to help enforce HIPAA, because they are the ones who are being damaged by the violations not the government.

Procedurally, a *qui tam* action under HIPAA should look very similar to a *qui tam* action under the FCA. Anyone who becomes aware of a HIPAA violation that causes his or her private medical records to be wrongfully exposed may file a complaint to the DOJ. The DOJ would then investigate the claim to determine if OCR has already undertaken any enforcement efforts or work with OCR to determine the validity of the claim and if it is worth pursuing for the government. If OCR has already undertaken enforcement measures, the individual would be barred from joining the government’s action against the violator, and could only receive the same portion of the final resolution or settlement as other individuals who were damaged by the actions of the violator. Accordingly, OCR should regularly make public to individuals what actions are being investigated and allow individuals to submit inquiries before filing any complaints with the DOJ. If, however, an individual feels that the final resolution or settlement reached by OCR for any claim would result in under enforcement, they should be allowed to appeal that resolution or settlement. Upon any appeal, if it is determined that the original settlement or resolution was inadequate and would lead to under-enforcement, than the individual who filed the appeal should receive a percentage of any additional settlement or resolution. If OCR has taken no enforcement measures, than the DOJ would be allowed to determine if it is in the government’s interest to join in the suit. This should be determined within 30 days of the relator’s initial claim filed with the DOJ. Once this decision is made the claim should be filed within 30 days at the appropriate Federal Court, at which point the Federal Rules of Civil Procedure should govern the process of the pleadings.

If multiple parties file separate complaints with the DOJ against an identical party for an identical or substantially similar HIPAA violation, than the matters should be joined together. For fairness and pragmatic purposes, however, once the DOJ has decided whether the government will join the relator’s suit within 30 days of the relator’s initial filing, than no additional parties may be added on as relators. If multiple parties are added as relators, than each party shall share in the percentage of the final settlement or resolution that the Court determines the relator should receive.

Under this proposal, any relator who files a claim in which the government does not join as a party would be able to collect anywhere from fifteen to thirty percent of the final settlement or resolution, with the remainder going into a fund to remedy all those damaged by the violation(s). If the government chooses to join a relator’s claim, then the relator and the government could each receive between fifteen and twenty percent of the final settlement or resolution, again with the remainder going to a fund to remedy all those damaged by the violation(s). In either case, the relator(s) additionally should receive from the HIPAA violator full compensation for their attorneys’ fees if they are successful on the merits of the case.

If the government alone takes enforcement actions through OCR, then the government should receive forty percent of the final resolution or settlement; however, the government does
not need to be reimbursed for its attorneys’ fees and enforcement measures, as this could be more difficult for a court to calculate because the enforcement attorneys for the government may have a difficult time separating the hours spent working on each particular case when they have the potential to handle many at one time. This balanced approach gives both individuals and the government the proper economic incentives to adequately enforce HIPAA regulations. Furthermore, this also provides the government funds to allow for the further policing of a violator to ensure that the violations are cured and any corrective plans mandated by a settlement or resolution are fully and adequately implemented.

Similar to the FCA, under this proposed plan an individual would have to file an actual legal complaint with DOJ to be deemed a relator in a *qui tam* action for a HIPAA violation. Traditional “complaints” to OCR, however, would not grant the individual the right to any of the money from a settlement or resolution reached between the violator and OCR, other than what they would receive as an individual damaged by the violation. This is because these simple complaints to OCR do not rise to the same level and legal requirements a complaint sent to DOJ must meet. As the DOJ may simply choose not to act on any complaint sent to them, this means that the legal complaint filed to DOJ must meet federal pleading requirements, which requires that the relator plead specific facts and does not allow for conclusory statements. Traditional OCR complaints, on the other hand, do not require that an individual plead anything, it simply allows individuals to complain whenever they believe their privacy rights were violated. Therefore, requiring that an individual file a legal complaint with the DOJ before being deemed a relator in *qui tam* matter still allows an individual the ability to protect his privacy interests and rights while at the same time preventing any individuals who just file mere grievances with OCR from collecting on any settlements or resolutions reached by OCR or DOJ. The simple way of breaking up this dichotomy would be to allow OCR to continue receive “complaints” and have OCR conduct separate enforcement actions for HIPAA violations, and only allow the DOJ to act and an individual to become relators after the individual files a complaint with DOJ.

In addition to the procedural differences between the FCA *qui tam* actions and the proposed HIPAA *qui tam* actions, HIPAA will also require a different type of fine structure than what currently exists in the FCA. As HIPAA is currently set up, each violation of the statute subjects a covered entity or business associate to a certain fine based on the egregiousness of the violation. The fine, however, is not based on how many private electronic medical records are exposed by the violation. In theory, there could be an accidental, non-egregious violation of either the Privacy or Security Rule that causes millions of electronic medical records to be exposed. The cloud-computing service provider would only be subject to a small fine for their slight oversight, which would not justify the significant damage caused by the breach. To correct this imbalance, HIPAA’s fine structure should be made to resemble the FCA’s.

Under the FCA, violators of the act are punished for each false claim that is made with fines based, in part, on the egregiousness of the violation and are subject to treble damages. This helps to create a balance so that violators are punished for both the amount of damage they cause, and the egregiousness of the violation. Congress can create a similar balance to punish HIPAA violators. Namely, fines should be based on a system that balances the number of electronic medical records that are exposed along with the egregiousness of the violation that led to the exposure. This can be done in a manner very similar to the FCA’s sliding fine scale,
however, the breadth of the fine scale would likely need to be larger for HIPAA violations because of the nature of how HIPAA violations occur and the damage that is caused by the exposure of private medical records. As discussed above in Part II, cloud-computing service providers have the potential to expose millions of electronic medical records through a simple violation. Therefore, if the fine scale were not low enough, when calculated for each breach the fines would be far too substantial for any company to risk. At the same time, however, if the fine scale were not high enough, than extremely egregious violations of just a few choice records would go under punished and would not properly deter cloud computing service providers from violating HIPAA’s Privacy and Security Rules. This problem makes developing a scale rather tricky. Furthermore, any maximum fine limit must be adequate to properly incentivize large cloud-networks that store millions of records.

To solve this problem, however, it may be simpler to break up the types of breaches that can occur, and then create a fine structure around such breaches. First, the types of breaches should be divided into how many electronic medical records are exposed. Next, the amount of each fine should be based on the egregiousness of each violation, and the potential damage caused by each breach. The table below lays out a simple fine plan and structure that could be implemented under this proposal:

<table>
<thead>
<tr>
<th>Number of People Affected by the Breach</th>
<th>Base Fine Scale for Potential Damage Caused by Breach per each Record Exposed</th>
<th>Base Fine Scale for Egregiousness of the Breach</th>
<th>Total Range for any Violation that Causes Record Exposure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-50</td>
<td>$500-10,000</td>
<td>$100-1,000,000</td>
<td>$600-1,500,000</td>
</tr>
<tr>
<td>51-100</td>
<td>$300-5,000</td>
<td>$500-3,000,000</td>
<td>$20,400-3,500,000</td>
</tr>
<tr>
<td>101-500</td>
<td>$200-4,000</td>
<td>$1,000-5,000,000</td>
<td>$21,100-5,200,000</td>
</tr>
<tr>
<td>501-1,000</td>
<td>$100-2,500</td>
<td>$5,000-8,000,000</td>
<td>$55,100-10,500,000</td>
</tr>
<tr>
<td>1,001-10,000</td>
<td>$100-2,000</td>
<td>$10,000-10,000,000</td>
<td>$110,100-30,000,000</td>
</tr>
<tr>
<td>10,001-100,000</td>
<td>$50-1,000</td>
<td>$15,000-15,000,000</td>
<td>$515,050-115,000,000</td>
</tr>
<tr>
<td>100,001-1,000,000</td>
<td>$50-250</td>
<td>$20,000-20,000,000</td>
<td>$5,020,050-270,000,000</td>
</tr>
<tr>
<td>1,000,000+ to a maximum of 10,000,000</td>
<td>$50-100</td>
<td>$25,000-25,000,000</td>
<td>$50,025,000-1,025,000,000</td>
</tr>
</tbody>
</table>

This fine structure would help to incentivize implementation of HIPAA’s Privacy and Security Rules for all covered entities and business associates, while at the same time it would not overly deter the use of cloud computing technologies. Under this proposed structure, smaller
entities that store far less records are exposed to the threat of much lower fines. Therefore, Medical Offices and Care Facilities that only store a few hundred or a few thousand records would be exposed to much less potential liability for an accidental violation than an insurance provider or cloud-service provider that may store millions of records. Unlike the current HIPAA fine structure, which only takes into account the egregiousness of the violation, this fine structure would balance the damage caused by the violation along with the egregiousness of the violation when determining the correct fine. This creates a fair system that will have a correct deterrent effect across the spectrum, from the smallest medical provider to the largest cloud-computing service provider.

This system works for many of the different types of breaches that face electronic medical records that are stored via cloud computing or otherwise. Take for example the factual scenario in Yath where a single health record was purposefully made public by a healthcare professional. Here it is arguable that the egregiousness of the violation calls for a larger fine, despite the fact that only one record was exposed. These types of targeted exposures need to be efficiently deterred. Under the proposed fine structure, the violating party in a Yath scenario would be subject to a maximum penalty of $1,010,000. This number would be based both on the value of the private information to the exposed individual, and the egregiousness of the violation. With the threat of such high fines, there is a high deterrence factor to deter individuals from committing such egregious acts as occurred in Yath.

The fine structure as proposed is also in conformity with some of the recent fines OCR has administered for smaller breaches. In July 2011, OCR fined UCLA $865,500 for repeated violations over a three year period relating to only two health records. According to OCR, UCLA employees had repeatedly viewed and disseminated the private health records of two well-known celebrities over a three-year period. Therefore, the overall size of the fine was largely due to the egregiousness of the violation. Calculating a fine under the proposed structure would allow for a maximum fine in the amount of $1,020,000 for the same offense. What this shows is that the proposed fine structure is built to handle egregious violations that involve only a few records, while at the same time it has the ability to punish larger breaches far more harshly, which currently is impossible under HIPAA.

Another example of a smaller breach that OCR harshly punished can be seen in the $1,000,000 fine imposed against Massachusetts General Hospital. Here an employee lost a laptop on a subway train that had private health records of 26 patients with infectious diseases such as HIV on it. Again, under the proposed fine structure the same penalty for the egregious nature of the violation can be issued. Under the proposal, the fine for a violation of this nature could be as high as $1,260,000. This fine is again very close to the actual fine that was administered under the current HIPAA legislation and fine structure.

While the proposed fine structure seems to mirror HIPAA’s current fine structure for smaller, egregious breaches, the difference between the two mainly comes when there are large breaches. The proposed fine structure, unlike the current HIPAA fine structure, punishes for the egregiousness of a violation while at the same time it also works to correctly incentivize larger companies that have huge breaches of electronic medical records. For example, in the Providence case handled by OCR and discussed further above, roughly 386,000 individuals had their protected health information exposed due to an accidental breach caused by a violation of HIPAA’s Privacy Rule. In that case OCR only fined Providence $100,000 despite the fact that
so many people had been damaged by the exposure. The proposed fine structure would have had Providence paying anywhere between $19,320,000 and $98,500,000. While this number is considerably higher than the fine imposed by OCR, it makes sense from a deterrence aspect. The effect of OCR’s original fine against Providence was that Providence was forced to pay only $0.26 per electronic medical record that was exposed to the breach. This can be compared with the $38,461.53 paid per medical record exposed in the Massachusetts General Hospital scenario. Being forced to pay a little more than a Quarter for each record that Providence caused to be exposed because of their violation of HIPAA’s Privacy Rule is simply unjust when compared with the smaller breaches despite having relatively the same information being revealed, and furthermore it serves as only a token deterrence against large-scale breaches.

The under deterrence of a fine issued in the same manner as the Providence case highlights the impotence of HIPAA’s current fine system. With cloud-based health networks that store millions of records the under deterrence will only become amplified. There must be significantly total higher fines and maximum fine limits to correctly incentivize these new players in the health data storage industry. If the correct deterrent amount is not properly calculated, than there is a risk that millions of individuals’ private health information will be exposed by inadequate implementation of HIPAA’s Privacy and Security Rules by cloud-computing service providers.

Additionally, the significantly higher fines imposed by the proposed fine structure are justified by the valuable nature of private health records that are stored in electronic form. The current fines imposed by HIPAA are simply not enough to incentivize larger companies, such as cloud-computing servers, to implement HIPAA’s Privacy and Security Rules. Rather, under the current fine structure, it may be more valuable to those companies to completely ignore HIPAA’s Privacy and Security Rules altogether. This is why the fine structure needs to be revamped to at least resemble the proposed fine structure offered by this paper.

By implementing a fine structure similar to what is proposed, Congress would help solve the potential privacy storm facing healthcare in regards to cloud-computing. Service providers who store millions of records will have to implement the correct protective measures promulgated by HIPAA’s Privacy and Security Rules if they wish to continue to store electronic medical records. Furthermore, if Congress determines that this fine structure is too strict for covered entities that face a larger threat of regular smaller breaches, Congress could merely make this fine structure purely applicable to business associates that use cloud-computing technologies to store millions of records. As stated throughout this paper, the threat of millions of records being exposed through the increased use of cloud computing technologies in healthcare creates a problem with HIPAA’s current fine structure. Solving this problem will be crucial in moving the storage of electronic medical records into this burgeoning, beneficial technology while stile maintaining the security and privacy of individuals’ private health records.

One important aspect for relying on a fine structure instead of traditional legal damages through private tort actions is the problem faced with calculating actual damages caused by a breach in ones privacy. When records are exposed it can be almost impossible to tell what information was collected or what information was used for an improper purpose. These difficulties in determining who, if anyone, was damaged by a violation that led to an exposure makes it even more difficult in determining how much someone was actually damaged. Furthermore, even if one could know precisely what information was collected, it could still be
difficult to determine how much a person was damaged by the invasion of their privacy. If a private medical record is published online, how much is a person actually damaged by the publicity of this private information? As this is such a difficult question it makes sense to have a flexible fine structure in place, and not rely on the unpalatable idea of only having a private right of action.

Additionally, this plan allows for all the benefits that a more traditional private right of action would grant. Individuals would be able to enforce their own privacy rights by filing a *qui tam* action. Individuals are also incentivized to help OCR enforce HIPAA’s Privacy and Security Rules, thereby increasing compliance. Finally, under this plan individuals will be compensated for any damages that may have occurred to them due to a breach that exposes their private health records. The major difference is that this plan will also benefit all those who were also effected by the breach, as well as ensuring that courts are able to accurately calculate damages on the basis of a well known but flexible fine scale. This fine structure will also allow both covered entities and business associates to know the exact consequences of a breach, which will allow them to plan for any contingencies. Only allowing a private right of action through common law torts or State statutes could result in widely varying results amongst cases from district to district. This flexible fine structure helps prevent this variation, and helps give clarity to the consequences for violating HIPAA’s Privacy and Security Rules.

The problem created by the use of cloud computing technologies in healthcare is that millions of private health records will be stored in an easily transferable medium, which, if not properly protected, could result in breaches the size of which has yet to be seen in the healthcare industry. HIPAA’s Privacy and Security Rules offer adequate protections against these breaches, but the history of the enforcement of these Rules highlights that the current enforcement strategy and mechanisms are largely ineffective. Congress can remedy this growing problem, however, by merely following their very own lead and modeling HIPAA enforcement after the FCA. Under the proposed plan discussed above, individuals will be compensated for the wrongful exposure of their private health records, they will be able to help in the enforcement of the Rules while at the same time protecting their own privacy, and finally companies that store large amounts of records will be adequately punished for their failures to meet the requirements of HIPAA’s Privacy and Security Rules that result in the exposure of large numbers of health records.

**Conclusion**

The healthcare industry has the opportunity to reap many of the benefits offered by the development and implementation of cloud computing technologies. Covered entities can now enlist cloud computing service providers as business associates to cheaply store, manage, and evaluate millions of electronic medical records. With all the benefits offered by cloud computing technologies, there are still threats and concerns relating to the privacy of medical records stored on cloud networks. Because the privacy of medical records is a long-standing legal right that has far reaching financial and personal consequences if not maintained, it becomes imperative that Congress adequately protect the privacy of these records.
While Congress has taken an important step in amending HIPAA via the HITECH Act to include business associates under many of the provisions of the Privacy and Security Rules, they have ultimately failed to give HIPAA satisfactory enforcement mechanisms by not providing individuals with any course of action to protect their privacy, capping yearly fines at $1,500,000.00, and not requiring stricter enforcement by OCR. Because the Privacy and Security Rules act as the primary legal regulation for the protection of private, sensitive electronic medical records that are stored and transmitted on the cloud, it becomes imperative that these protections are enforced or this private data will be at a higher risk for exposure to unauthorized parties.

Therefore, despite the overarching privacy protections that the Privacy and Security Rules offer electronic medical records that are stored and processed using cloud computing, unless Congress amends HIPAA to solve the problems with its enforcement, these viable Rules cannot be perceived to adequately protect the privacy of patient medical records that are stored on the cloud. Congress must act to ensure that these privacy rights are adequately protected. By following the success of the FCA, Congress could amend HIPAA to alleviate many of these concerns with enforcement and implementation. By increasing the enforcement measures of the Privacy and Security Rules, Congress can help ensure that cloud computing service providers are adequately punished in the event that large breaches expose millions of private health records. Without these proposed amendments, however, Congress is failing to protect our health records in the burgeoning age of cloud computing.

---

5 See Richard Acello, Get Your Head in the Cloud: Despite ethics questions, law firms are storing client data on the Net, A.B.A. J., Apr 1, 2010, http://www.abajournal.com/magazine/article/get_your_head_in_the_cloud/ (discussing some of the challenges and advantages facing law firms in converting to cloud computing, which many of the same advantages can also be attributed to the medical field).
7 See McCarthy, supra note 4, at 2253. A covered entity is a person, business, or agency that furnishes, bills, or receives payment for healthcare in the normal course of their business, and they transmit these transactions electronically. See U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, HIPAA General Information Covered Entity Charts (Dec. 14, 2005), available at https://www.cms.gov/hipaageninfo/downloads/CoveredEntityCharts.pdf.
8 See McCarthy, supra note 4, at 2253.
12 The term electronic medical record is to be used synonymously for the purposes of this Comment with electronic health record, because there is general confusion in the literature as the correct term and as one commentator notes that the HITECH Act’s definition of electronic health records is “one that is generally associated with electronic medical records.” Nicolas P. Terry, Personal Health Records: Directing More Costs and Risks to Consumers?, 1 DREXEL L. REV. 216, 257 (2009).
HHS has been charged by the United States Congress with the enforcement of the HIPAA legislation, which responsibility for enforcement of HIPAA’s Privacy and Security Rules has been specifically delegated within HHS to the Office of Civil Rights (OCR). See HIPAA Enforcement, HHS.gov.


See infra Part I.A.

See Part I.B.

See infra Part I.C.

See infra Part II.A.

See infra Part II.B.

See infra Part III.

See infra Part IV.


See Khan, supra note 24, at 265.


See State v. Bellar, 217 P.3d 1094, 1110-11 (Ore. App. 2009) (Sercombe, J., dissenting) (stating that “most citizens would regard that data [stored in the ‘cloud’] as no less confidential or private because it was stored on a server owned by someone else.”); William Robison, Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act, 98 GEO. L.J. 1195, 1199 (2010).

See DeVore, supra note 9, at 371.

See Robison, supra note 28, at 1200.

See DeVore, supra note 9, at 369; Robison, supra note 28, at 1201.

See DeVore, supra note 9, at 369; Robison, supra note 28, at 1200.

See DeVore, supra note 9, at 368; Robison, supra note 28, at 1200.


See Marty Foltyn, The Cloud Offers Promise for Storage Users, ENTERPRISE STORAGE F. (Dec. 10, 2008), http://www.enterprisestorageforum.com/ipstorage/features/article.php/379038 (discussing companies that offer various cloud computing services include the likes of Google, Inc. and Amazon, Inc.).

“Anywhere” generally refers to any location where the user can obtain a connection to the Internet. Other restrictions to accessing third-party servers such as firewalls may also apply. See Joshua L. Simmons, Buying You: The Government’s Use of Fourth-Parties to Launder Data About “The People”, 2009 COLUM. BUS. L. REV. 950, 956 (2009) (stating, “cloud computing . . . allows the user to access his or her document from any computer connected to the Internet.”).


Id.

See McCarthy, supra note 4, at 2253.

For example, the cloud computing style website Wikipedia.org, which allows users to collaborate and update information stored on the “cloud” while also giving notification to the original creator of the information of a change, has been found to be just as accurate as the Encyclopedia Britannica by the British journal Nature, as reported by BBC News. See Wikipedia Survives Research Test, BBC NEWS ONLINE (Dec. 15, 2005, 10:42 AM), http://news.bbc.co.uk/2/hi/technology/4530930.stm.


Id.
Theft of communication between a physician and his patient, and that this policy has been established by the legislature in (1974) (holding that "[t]he physician-patient privilege expresses a long-standing policy to encourage uninhibited communication between a physician and his patient").


Ludwig Edelstein, The Hippocratic Oath: Text, Translation, and Interpretation, (1943) (stating that this is an excerpt from a version of the modern Hippocratic Oath which is still pledged by many medical students upon graduation). Another modern adaptation of the Hippocratic Oath reads, "I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know." The Hippocratic Oath: Modern Version, NOVA, http://www.pbs.org/wgbh/nova/doctors/oath_modern.html (last visited on Oct. 14, 2011).

See Whalen v. Roe, 429 U.S. 589, 599 (1977) (stating that an individual has a constitutional right to privacy which protects "the individual interest in avoiding disclosure of personal matters.").


See id.

Id.

Id.

Id.

Id.

Id.

Id.

291 Ala. 701 (1973).

Id. at 702.

Id. at 707.

Id. at 708.

See Whalen v. Roe, 429 U.S. 589, 599 (1977) (stating that an individual has a constitutional right to privacy which protects "the individual interest in avoiding disclosure of personal matters.").
Still Protect Patient Privacy Under a National Healthcare Information Network?

Health information are not defined as business associates and are not covered under HIPAA.

Companies that are classified as business associates usually tend to be data processors, management firms (i.e. cloud computing service providers).

Companies that are classified as business associates usually tend to be data processors, management firms (i.e. cloud computing service providers).

The term “business associates” are defined as those entities that perform activities for or provide services to covered entities. See 45 C.F.R. § 160.103(i)(10). Under HIPAA, in order for a covered entity to reveal protected health information to a third-party company they must enter into a contract that obligates the third-party company to implement certain privacy protections. See 45 C.F.R. § 160.103(i)(10). Companies that enter into these contracts with covered entities are deemed business associates, and originally were not subject to most of the fines that could be levied under HIPAA. Companies that are classified as business associates usually tend to be data processing and management firms (i.e. cloud computing service providers). See Sean McLaughlin, Pandora’s Box: Can HIPAA Still Protect Patient Privacy Under a National Healthcare Information Network?, 42 GONZ. L. REV. 29, 43 (2007).

Cloud computing service providers that are not under contract with a covered entity to store or maintain protected health information are not defined as business associates and are not covered under HIPAA.

McLaughlin, supra note 96.


The cloud computing service provider Microsoft HealthVault offers a simple contract for covered entities to enter into for cloud computing services that generally satisfies the requirements under HIPAA. See Becoming a HealthVault Solution Provider, HEALTHVAULT DEVELOPER CENTER, http://msdn.microsoft.com/en-us/healthvault/cc185139 (follow “HealthVault HIPAA Business Association Agreement” hyperlink).

Rather an internal network that was managed by the Virginia Department of Health Professionals and not a third party cloud computing service provider. See supra Part II.A. (May 5, 2009), at 286-87.


See Khan, supra note 24, at 286-87.


See infra Part II.A.

See McCarthy, supra note 4, at 2267.

Bob Coffield, Virginia Department of Health Professions Breach: Extortion Demand Regarding 8M Patient Records and 35M Prescriptions, HEALTH CARE LAW BLOG (May 5, 2009), http://healthblawg.visibli.com/8d9f35b3d72281e8/?web=7b6a14&dst=http%3A//healthcarebloglaw.blogspot.com/2009/05/virginia-department-of-health.html. The Health Information Network in this case was not cloud-based, but rather an internal network that was managed by the Virginia Department of Health Professionals and not a third party cloud-computing service provider.
The hacker left a ransom note on the secure site for the Virginia Prescription Monitoring Program that read:

I have your shit! In *my* possession, right now, are 8,257,378 patient records and a total of 35,548,087 prescriptions. Also, I made an encrypted backup and deleted the original. Unfortunately for Virginia, their backups seem to have gone missing, too. Uhoh: (For $10 million, I will gladly send along the password.)

Id.


David Drummond, A new Approach to China, THE OFFICIAL GOOGLE BLOG (January 12, 2010), http://googleblog.blogspot.com/2010/01/new-approach-to-china.html (discussing an attack against Google that originated in China that resulted in the loss of intellectual property and a failed attempt to hack the e-mail accounts belonging to Chinese human rights activists).

Id.

Id.

See PlayStation Network Restoration Begins, PLAYSTATION.COM, (May 17, 2011) uk.playstation.com/psnlatest/.

Id.


Id.

See PlayStation Network Restoration Begins, PlayStation.com, (May 17, 2011) uk.playstation.com/psnlatest/.

Id.


Id.


Id.


Aetna, Inc. is one of the nation’s largest health insurance companies and claims to have over 18.6 million medical insurance customers. See Aetna Facts, AETNA.COM, http://www.aetna.com/about-aetna-insurance/aetna-corporate-profile/facts.html (last visited Oct. 15, 2011).


Id.


See Exclusion of Service, GOOGLE TERMS OF SERVICE, http://www.google.com/accounts/TOS?hl=en (last visited Oct. 15, 2011) (stating that Google expressly disclaims all warranties and conditions of any kind, whether express or implied, including, but not limited to the implied warranties and conditions of merchantability, fitness for a particular purpose, and non-infringement).

See Privacy and Security: Keeping Data Private, GOOGLE DOCS, http://docs.google.com/support/bin/answer.py?hl=en&answer=87149 (last visited Oct. 15, 2011) (stating that information security is a top priority at Google, that they employ dedicated teams with experts in their fields to handle these important areas, and that files are, by default, set to private, but users can choose to publish them to the Internet or invite collaborators or viewers).

This is referring primarily to the potential for advertisers to use the wrongfully obtained private health data to target specific people in their marketing campaigns, and to the use of private health data by insurance companies to discriminate as to who is allowed access to health insurance. See supra Section I.B.

An example of which is the December 2009 cyber attack against Google as discussed above. See Michael Arrington, Google Defends Against Large Scale Chinese Cyber Attack: May Cease Chinese Operations, TECH CRUNCH (January 12, 2010), http://techcrunch.com/2010/01/12/google-china-attacks/.


See id.

See id. at 10-11.


See Marianne Kolbasuk McGee, Medical IT Gets Personal, INFORMATIONWEEK HEALTHCARE (Nov. 16, 2009, 03:00 PM), http://www.informationweek.com/news/healthcare/EMR/showArticle.jhtml?articleID=221601548 (reporting that Duke University Health System was able to use data mining to sift through information on more than 20 million patients to identify who had risk factors for contracting H1N1 flu, to determine who needed most to receive a new vaccine shipment).


See id.


See Lohr, supra note 177 (reporting that Microsoft’s cloud computing service, Health Vault, is now offered to Kaiser Permanente’s 8.7 million members in nine states and the District of Columbia).

See supra Part I.C.

See supra Part II.A.

See supra Part I.C.


See supra Part I.C.


See O’Rourke & O’Rourke, supra note 185.

See Sullivant, supra note 75, at 678.


The Civil Rights Division of the Department of Health and Human Services was able to process 8,071 complaints in 2009, and these complaints were either resolved after intake, found to have no violation of HIPAA, or corrective
action was taken, and out of the 8,071 complaints that were processed, “corrective action” was obtained in 2,140 of them. See Enforcement Results by Year, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/historicalnumbers.html (last visited Oct. 15, 2011).


193 Id.


195 Id.

196 Id.

197 Id.

198 Id.

199 Id.

200 Note that the fines for violating the Privacy and Security Rules are capped at $1,500,000 per fiscal year, however, this case occurred over a period of three years which allowed for the $1,300,000 initial fine, and the later fine of $3,000,000 for failing to comply with OCR’s investigation over a 13 month period.

201 In 2011 OCR has also administered large fines for some smaller breaches. For example, a $1,000,000 fine against Massachusetts General Hospital for an employee leaving a laptop on a bus, which exposed 21 patient records, and a $865,000 fine for the repeated exposure of two celebrity health records over a three year period. See Sandra Yin, Patient info lost on subway earns MGH $1 million HIPAA fine, Fierce Healthcare, http://www.fiercehealthcare.com/story/patient-info-lost-subway-earns-mgh-1-million-hipaa-fine/2011-02-25#ixzz1bFnoxFz3 (Feb. 25, 2011), UCLA Must Pay $865,500 HIPAA Fine, Campus Safety, http://www.campussafetymagazine.com/Channel/Hospital-Security/News/2011/07/08/UCLA-Health-System-Settles-HIPAA-Case.aspx (July 8, 2011).


203 Id.

204 Id.

205 Id.

206 Id.


208 Id.

209 Id.

210 Id.

211 Id.


214 See id.

215 The minimum fine a business associate may face under HIPAA is $100.00, and is only optionally granted if they are found to have had no knowledge that they were in violation of HIPAA. See 42 U.S.C. § 1320d-5 (2010). Even when a business associate has no knowledge that they are in violation of HIPAA they are still subject to the maximum $50,000.00 fine. See 42 U.S.C. § 1320d-5 (2010).

216 See 42 U.S.C. § 1320d-5 (2010) (explaining that the yearly maximum fine is inclusive of all contracts held by a business associate with other covered entities, as applied to business associates via 42 U.S.C. § 17931 (2010)).

See supra Part II.B.

See supra Part II.B.

See supra Part I.C.


Id. at 3729(g).

Id. at 3730(c).

Id.

Id. at 3730(d).


Id.

Id.

ITA.

Note that the proposed system of filing a complaint with the DOJ for a HIPAA violation is a different process than filing a simple complaint with HHS. A DOJ complaint requires that the pleadings be able to stand on its own just as is the case with FCA complaints filed with the DOJ. Simple complaints filed with HHS may be baseless and require extra investigatory work by OCR. Therefore, those complaints filed with HHS will not allow an individual to claim relator status on the basis of the HHS complaint alone.


See Ashcroft v. Iqbal, 129 S.Ct. 1937 (2009) (holding that conclusory statements will not survive a motion to dismiss for failure to state a claim under Fed. R. Civ. Pro. 12(b)(6)).


Id.


Id.

Id.


Id.

Currently, each violation under HIPAA can result in a fine between $100 and $50,000 based upon the egregiousness of the fine. See 31 U.S.C. § 3730(d) (2010).

See DeVore, supra note 9, at 376.