HIPPOCRATES WOULD ROLL OVER IN HIS GRAVE: AN EXAMINATION OF WHY INTERNET HEALTH CARE PROGRAMS SHOULD OBTAIN INFORMED CONSENT FROM THEIR USERS

I. INTRODUCTION

A study by Microsoft revealed that approximately eight million people do a health related internet search daily.\(^1\) A poll from 2007 found that approximately seventy-six percent of adults who are fifty-five years old or older searched for medical diagnoses using the internet.\(^2\) From these searches alone, 500 million to one billion dollars were generated each year from the advertising that appeared during the searches.\(^3\) A Microsoft executive estimated that the dollars generated from the aforementioned advertising would increase to five billion dollars within five to seven years.\(^4\) Planning to make money from advertising which was to appear on its own search engine, Microsoft created HealthVault ("HealthVault") as an online, secure storage site for health information.\(^5\) Microsoft created HealthVault to allow users to upload personal medical records to one location and to then share the medical records with their families, physicians, and programs that have teamed up with HealthVault.\(^6\) A number of programs and websites joined HealthVault to provide services such as monitoring a variety of health information and creating health plans for users.\(^7\) HealthVault created a convenient place to find and share medical information for an overall more effective health care experience.\(^8\) Fur-

---

3. Id.
4. Id.
5. Neupert, supra note 1; Greene, supra note 2.
thermore, there is no charge to use HealthVault for users, physicians, and programs that have teamed up with HealthVault.9

Additionally, Google's Chief Executive Officer, Eric Schmidt, stated that a health-related search is the most important internet search an individual can do.10 Thus, Google was motivated to create a health-based internet program as well.11 Google created a health-based internet program called Google Health, a health-based internet program, which allowed users to store medical records on an internet site.12 Google Health also allows users to share medical records with third parties, such as their families, physicians, and programs.13 Signing up for Google Health is free for users.14 In 2008, Google made the majority of its earnings on advertising revenue that equated to twenty-one million dollars.15 Unlike HealthVault, Google currently does not allow advertising on Google Health.16 However, Google admitted that advertising may appear on Google Health in the future.17 Schmidt also expressed hope that Google Health will generate revenue for Google if its users click on advertisements on other connected Google sites.18

Upon developing their patient health record systems, Microsoft and Google did not adequately address the privacy issues involved with uploading medical information to the internet.19 Medical records contain a myriad of private information including radiology history, prescription drug information, blood-pressure results, lab results, and other personal medical history.20 Many individuals are skeptical about putting such private, medical information in an electronic format because they fear the information will not be adequately pro-

11. Id.
13. Id.
14. Id.
18. Id.
Thus, Microsoft and Google attempted to assure HealthVault and Google Health users that the users' information would remain secure. Noting the importance of maintaining security of their user's health information, Microsoft and Google both claim their sites, HealthVault and Google Health respectively, are safe and secure. In privacy statements associated with HealthVault and Google Health, Microsoft and Google emphasized that the user controls who accesses the user's information and what information is uploaded to the user's account. Further, the first line of HealthVault's privacy statement states, "Microsoft is committed to protecting your privacy." However, much of the criticism that Microsoft and Google received from an academic privacy research center pertains to the security of medical records on the internet. While Microsoft claimed they were committed to protecting a HealthVault user's privacy, one of the programs who partnered with Microsoft, Kaiser Permanente, had a history of privacy breaches. Microsoft stated that its privacy commitments in regards to HealthVault were industry leading and that Microsoft established...

26. See Antón, supra note 19 ("It is critical to address these privacy concerns in the design of PHR systems before we deploy them with vulnerabilities that will ultimately lead to yet another rash of data breaches.").
stringent privacy principles for programs like Kaiser Permanente that connected with HealthVault. However, Kaiser Permanente allowed the breach of private medical records and information on numerous occasions. In 2002, Kaiser Permanente accidently sent hundreds of e-mails, some containing sensitive medical information, to seventeen individuals who were not the intended recipients of the private medical information. The e-mails that Kaiser Permanente sent to the seventeen unintended recipients contained patient addresses, telephone numbers, and answers to sensitive medical questions. In 2002, Kaiser Permanente accidently sent hundreds of e-mails, some containing sensitive medical information, to seventeen individuals who were not the intended recipients of the private medical information. The e-mails that Kaiser Permanente sent to the seventeen unintended recipients contained patient addresses, telephone numbers, and answers to sensitive medical questions. In 2005, Kaiser Permanente was fined for posting 150 patients' medical lab results, names, phone numbers, and addresses on a publicly accessible website. The 150 patients' medical information was posted for four years without the patients' consent. Further, in 2006, a laptop computer containing medical information, names, birthdays, and other private information of 38,000 Kaiser Permanente members was stolen out of a Kaiser Permanente's employee's car. Also in 2006, 160,000 Kaiser Permanente members' private medical information was stolen from a computer in one of Kaiser Permanente's secure offices. The 160,000 Kaiser Permanente members' stolen medical information included appointment information, names, phone numbers, and Kaiser Permanente member numbers.

As Kaiser Permanente's record indicates, there is no guarantee that medical information will remain secure on the internet. This Note argues that whenever personal information is on the internet, users run the risk of exposing that information to data breaches, regardless of the provider's reputation. A general lack of understanding of privacy law, and confusing privacy statements, gives users a

---

28. See Kaiser Permanente & Microsoft Empower Consumers to Take Charge of Their Health, http://www.microsoft.com/presspass/press/2008/jun08/06-09KaiserPR.mspx (last visited Mar. 25, 2009) [hereinafter Kaiser Permanente & Microsoft] ("HealthVault is designed to support Kaiser Permanente's transfer of My Health Manager data in adherence with federal standards and includes advanced safeguards to help protect members' personal information. HealthVault is built on the principle that people should have a copy of their own health information, have control over it and have the ability to privately share information with whomever they choose in a security-enhanced environment. In consultation with consumer privacy experts, Microsoft developed and implemented industry-leading health privacy commitments and stringent privacy principles for health technology providers connecting with HealthVault.").

29. Martinez, supra note 27.
30. Id.
31. Id.
32. Vrana, supra note 27.
33. Lee, supra note 27.
34. Laptop With Patient Info Stolen, supra note 27.
36. Id.
37. Id.
38. See infra notes 56-126 and accompanying text.
false sense of security relating to the safety of the users' medical records on the internet. HealthVault and Google Health both have confusing privacy statements, which generally reserve HealthVault's and Google Health's right to access their users' private health information. HealthVault and Google Health claim that they will only access users' uploaded information under limited circumstances, but a careful reading of the privacy statements indicates that the circumstances where HealthVault and Google Health can access user's uploaded information are quite broad. The language of HealthVault's and Google Health's privacy statements is such that HealthVault and Google Health can very easily justify accessing their users' private, uploaded information. This Note argues that because putting medical records on the internet is not completely secure, Microsoft and Google should be required to obtain informed consent from their users prior to users agreeing to their services. In this way, users will have a better understanding of the possible consequences of putting their personal medical records on the internet.

This Note proceeds in three sections. First, this Note's Background examines Microsoft's and Google's electronic health record programs, HealthVault and Google Health respectively, including their privacy statements. Next, this Note's Background reviews the history of privacy in the medical profession and the applicable federal laws that relate to medical information. This Note's review of the federal law relating to medical information includes the Health Insurance Portability and Accountability Act (“HIPAA”) and the common law doctrine of informed consent as it pertains to medicine and special education. Second, this Note's Argument Section explains four reasons why HealthVault and Google Health have a duty to obtain informed consent from their users before the users sign up for these sites. First, this Note argues that HealthVault and Google Health should obtain informed consent from their users to warn their users of the potential risks of uploading their medical information to the internet because HealthVault and Google Health have a duty to disclose

39. See infra notes 56-163 and accompanying text.
40. See infra notes 67-110 and accompanying text.
41. See infra notes 67-110 and accompanying text.
42. See infra notes 67-110 and accompanying text.
43. See infra notes 67-110 and accompanying text.
44. See infra notes 67-110 and accompanying text.
45. See infra notes 67-110 and accompanying text.
46. See infra notes 67-110 and accompanying text.
47. See infra notes 67-110 and accompanying text.
49. See infra notes 67-110 and accompanying text.
50. See infra notes 67-110 and accompanying text.
the consequences associated with signing up for their programs. Second, this Note argues that HealthVault and Google Health should obtain informed consent from their users because HealthVault and Google Health do not meet HIPAA's definition of covered entities, rendering HIPAA's privacy protection inapplicable to HealthVault and Google Health. Third, this Note argues that HealthVault and Google Health should obtain informed consent from their users to reflect HIPAA's purpose of protecting medical records. Fourth, this Note argues that HealthVault and Google Health should create an informed consent doctrine that models the special education requirement of parental consent. Finally, this Note concludes that because HealthVault and Google Health has a duty to disclose to their users the consequences of the users' submitting health records to an electronic health record program, HealthVault and Google Health should develop a doctrine of informed consent that would allow their users to make an informed decision regarding the uploading of their private health information onto the internet.

II. BACKGROUND

A. MEDICAL RECORDS, HEALTHVAULT, AND GOOGLE HEALTH IN GENERAL

An electronic health record is a digital copy of an individual's health record. An individual's electronic health record includes information about the individual's prescription drugs, x-rays, and lab results. The main goal of creating an electronic health record for an individual was to provide timely, accurate data and to improve the individual's medical care. Electronic health records also create an organized history of an individual's medical treatment, making it easier for physicians to find an individual's health information, improve communication with the individual, and improve the individual's care and efficiency. An individual's electronic medical records can be ac-
cessed at anytime, anywhere, by any health care provider.\textsuperscript{60} Supporters of electronic health records posited that electronic health records will significantly reduce an individual’s medical costs, help individuals make more informed decisions about their own health care, and prevent errors in the individual’s medical records.\textsuperscript{61} Physicians claim that electronic health records provide a system to check an individual’s prescriptions, thereby eliminating misread prescriptions and monitoring drug allergies.\textsuperscript{62} Physicians also stated that unlike paper health records, electronic health records cannot be misplaced.\textsuperscript{63} In 2004, President George W. Bush called for electronic health records to be available to all U.S. citizens by 2014.\textsuperscript{64} President Barack Obama also has identified that reforming the United State's medical system is a top priority for his administration, a reform that is achieved in part with the conversion of paper medical records into electronic medical records.\textsuperscript{65} Electronic health records are now a national goal.\textsuperscript{66}

1. \textit{The Creation of Microsoft's HealthVault}

In October 2007, Microsoft launched an internet-based program known as Microsoft HealthVault ("HealthVault").\textsuperscript{67} Microsoft created HealthVault to allow individuals to better manage their health records.\textsuperscript{68} Microsoft’s vision for HealthVault was to bring the technology and health care industries together in a way that would create a more user-friendly service for individuals to manage their own health information.\textsuperscript{69} Microsoft further stated that HealthVault would allow individuals to obtain their private health records and health care companies to deliver services and tools to HealthVault.\textsuperscript{70} The increased number of individuals who used the internet to conduct health-related

\begin{itemize}
\item \textsuperscript{61} HHS Announces Project to Help 3.6 Million Consumers Reap Benefits of Electronic Health Records, \textit{supra} note 59.
\item \textsuperscript{62} Kelley, \textit{supra} note 60.
\item \textsuperscript{63} Id.
\item \textsuperscript{66} Id.
\item \textsuperscript{69} Id.
\item \textsuperscript{70} Id.
\end{itemize}
searches prompted, in part, the emergence of HealthVault.\textsuperscript{71} As the population ages, Microsoft anticipated that individuals would want more control in the management of their own health records, specifically using online services such as HealthVault.\textsuperscript{72}

From HealthVault's beginning, HealthVault stated that it allowed its users to store their health records in one easily accessible location where its users could also share the health records with designated individuals.\textsuperscript{73} An individual using HealthVault, otherwise known as its user, can allow family members and physicians to view designated health information after the health information is uploaded.\textsuperscript{74} HealthVault's users can specify the degree of access that an individual is allowed to have in regards to the users' health records such as the duration in which the individual can view the users' health records or whether an individual can alter the users' health records.\textsuperscript{75} The individual who created the original health record is the custodian of that health record by default, but HealthVault's user can allow other individuals to act as custodians.\textsuperscript{76} A designated custodian has full control over the health record and can delete, modify, and share all of the HealthVault user's health information in the exact same manner as the health record's original creator.\textsuperscript{77} A HealthVault user with custodial access to a health record can also grant other users permission to access, view, and modify the health record.\textsuperscript{78} The HealthVault user's own access to his or her own health record can even be revoked by an individual with custodial level access.\textsuperscript{79}


\textsuperscript{72} See id. ("An aging population with more health concerns are expected to prompt consumers to take a larger role in managing their own care, including using online tools.").


\textsuperscript{75} Id.

\textsuperscript{76} Id.

\textsuperscript{77} See id. ("You can also choose to grant custodian access to other persons, such as your spouse, for any record of which you are a custodian. Custodian access is the broadest level of access, so you should think carefully before you grant custodian access to a record. Every custodian of a record has the same access to the record, including accessing, modifying, deleting, and sharing all the information in the record. A custodian can also revoke access to a record from any other custodian of the record, including you.").

\textsuperscript{78} Id.

\textsuperscript{79} See id. ("A custodian can also revoke access to a record from any other custodian of the record, including you.").
HealthVault also permits its users the option of sharing their health records with separate systems that work with HealthVault, systems known as Programs. Programs are websites that request access to a HealthVault user’s data to help monitor the user’s health records and daily health conditions such as blood pressure, blood-sugar levels, and fitness goals. Similar to a custodian, a HealthVault user can grant Programs permission to add, change, or delete information in the user’s health record. Some Programs store a copy of the information they access from a HealthVault user’s health records. The Programs may not disclose the HealthVault user’s health record without express consent from the user. However, if the Program is operated by an insurer, health care provider, or other health care entity that is subject to laws that govern health care information, privacy, and disclosure, the Program must comply with those laws.

2. HealthVault’s Privacy Statement

HealthVault’s privacy statement explains that Microsoft is “committed to protecting your privacy,” but HealthVault qualifies its privacy statement with three broad instances in which protection of its user’s privacy might not be possible. HealthVault’s privacy statement states that, if necessary, Microsoft may access and/or release its users’ personal information in order to “(a) comply with the law or legal process served on Microsoft; (b) protect and defend the rights or property of Microsoft (including the enforcement of our agreements); or (c) act in urgent circumstances to protect safety and welfare of users of Microsoft services or members of the public.”

HealthVault’s privacy statement also states that Microsoft uses a variety of security measures to keep its users’ information safe. The medical information HealthVault users provide is stored on computer servers located in controlled facilities. Furthermore, access to

80. Id.
82. See Privacy Statement Oct. 2008, supra note 74 (“Every custodian of a record has the same access to the record, including accessing, modifying, deleting, and sharing all the information in the record.”).
83. Id.
84. Id.
85. Id.
86. See id. (discussing circumstances under which Microsoft can disclose user’s information).
87. Id.
88. Id.
89. Id.
HealthVault's users' health records is limited. For instance, except for e-mails, communications sent through HealthVault are encrypted. Additionally, if HealthVault users are custodians of health records, the users can see a history of access and actions related to those health records. However, HealthVault users are not required to read HealthVault's privacy statement when signing up for HealthVault.

3. The Creation of Google Health

Similarly, Google launched a program designed to store health records in one convenient location called Google Health. The stated purpose of Google Health is to manage and store its users' health records. Google Health states that its users own their health records and should thus be in control of their own health records. Some of the uses for Google Health include keeping a Google Health user's physicians updated on the current health status of the user, eliminating paperwork, and storing all of the user's lab results in one location. Google Health requires that its users be at least eighteen years of age before using the program. Google Health also allows its users to share health records with third parties. However, Google Health does not allow its users to grant custodial level status to third parties, meaning that third parties can never alter or delete the user's health records.

90. See id. (“For example, we store the personal information you provide on computer servers with limited access that are located in controlled facilities.”).
91. Id.
92. Id.
96. Id.
97. See id. (“Keep your physicians up-to-date, stop filling out the same paperwork every time you see a new physician, avoid getting the same lab tests done over and over again because your physician cannot get copies of your latest results, don't lose your medical records because of a move, change in jobs or health insurance, share your information securely with a family member, caregiver, or physician.”).
100. See Google Health Help: Sharing Your Profile, http://www.google.com/support/health/bin/answer.py?answer=138423&topic=14387 (last visited Mar. 26, 2009) (“Sharing your profile lets others see your profile, but not edit it; only you can do that.”).
health records. If a Google Health user chooses to delete information from his or her health records, such deletions take place immediately, and a backup copy of the health record is deleted in a short amount of time.

4. Google Health’s Privacy Statement

Google Health’s privacy statement states that without express consent from the user, Google will not share, rent, or sell its user’s health records except in limited situations. Google Health can provide its users’ health records to its subsidiaries, affiliated companies, and trusted people or businesses for the purpose of processing its users’ health records. Google Health can also share its users’ health records in order to comply with a law or government request. Further, Google Health can share its users’ health records to enforce Google’s Terms of Service or to detect, prevent, or address fraud or security issues. Finally, Google Health will share its users’ health records to protect Google’s rights. Google Health’s privacy statement also states that Google employees, contractors, and agents will have access to its users’ personal information in order to develop or improve Google Health’s services. Google employees, contractors, and agents who do have access to Google Health’s users’ personal information are bound by the privacy policies of Google and face criminal prosecution if they violate this confidentiality. However, Google Health users are not required to read Google Health’s privacy statement when signing up for Google Health.

B. The Risks Associated With Electronic Medical Records

The benefits to an individual of putting his or her health records online include easy access to the health records through online programs, reduction of medical costs, increased medical efficiency, and
reduction in error by pharmacists and physicians. Recognizing the benefits of electronic health records, the Institute of Medicine stated that protecting electronic health records is essential. However, the Institute of Medicine released a report which concluded that the current rules protecting electronic health records are inadequate and must be overhauled to ensure health record confidentiality. Further, the Institute of Medicine’s report cites to numerous health record security breaches and indicates that such breaches are a growing problem. These aforementioned health record security breaches are a concern for users of Microsoft’s HealthVault (“HealthVault”) and Google’s Google Health (“Google Health”).

The eHealth Vulnerability Reporting Program (“EHVRP”) released a report in 2007 which found that electronic health record systems were very vulnerable to being breached. The EHVRP was formed by technology providers and health care practitioners to evaluate the security of electronic health records. The EHVRP’s report indicated that EHVRP successfully and quickly breached every electronic health system it tried to hack. The EHVRP reported that the electronic health systems are easy to hack because there are defects in the electronic health systems themselves. The EHVRP report also indicated that electronic health systems with vulnerabilities either

112. Healy, supra note 65.
113. Id.
114. Id.
117. Id.
did not disclose the defects to consumers nor provide adequate disclosure of such defects.\textsuperscript{120}

Despite the findings in the EHVRP report, data breaches jumped forty-seven percent from 2007 to 2008.\textsuperscript{121} According to the Identity Theft Resource Center, there were 656 reported data breaches in 2008 that potentially affected 35.7 million records.\textsuperscript{122} Of the 656 reported data breaches in 2008, ninety-seven were health and medical breaches.\textsuperscript{123} Of the 656 reported data breaches, 29.6 percent of the data breaches were caused by hacking and insider theft and 35.2 percent of the data breaches were human error such as accidental exposure.\textsuperscript{124} Electronic data breaches far out-numbered paper breaches, with 82.3 percent of the data breaches affecting electronic data.\textsuperscript{125} As indicated by the EHVRP Report and The Identity Theft Resource Center, not only are electronic health record programs vulnerable to hacking, electronic data hacking is on the rise.\textsuperscript{126}

\section*{C. Privacy Law With Regard To Medical Records}

The foundation of the health care system is based upon maintaining an individual's privacy.\textsuperscript{127} Maintaining an individual's privacy in medical practice became a priority when the "Father of Medicine," Hippocrates, revolutionized medicine in Greece in the fourth or fifth century B.C.\textsuperscript{128} Hippocrates discovered that in order to treat a patient, the patient must trust the physician.\textsuperscript{129} In order to gain a patient's trust, Hippocrates noted it was essential to keep all communications between the patient and the physician confidential.\textsuperscript{130} A patient's right to privacy is so important that Hippocrates'

\begin{itemize}
  \item \textsuperscript{120} See id. ("The lack of disclosure is particularly disturbing in an industry required by law to evaluate and manage risk. If vendors are not disclosing vulnerabilities on systems that hold sensitive data, health organizations cannot manage risk.").
  \item \textsuperscript{122} Id.
  \item \textsuperscript{123} Id.
  \item \textsuperscript{124} Id.
  \item \textsuperscript{125} Id. (stating 17.7\% of the breaches came from paper data).
  \item \textsuperscript{126} See id. (discussing the increase in identity theft from 2007-2008); see also Tucci, \textit{supra} note 116 (discussing a study that found electronic medical information is vulnerable to hacking).
  \item \textsuperscript{127} Patient Privacy Rights Foundation, http://www.patientprivacyrights.org/site/PageServer?pageName=the_Important_Issues (last visited Mar. 27, 2009).
  \item \textsuperscript{128} MSN Encarta, Hippocrates, http://encarta.msn.com/encyclopedia_761576397/Hippocrates.html (last visited Mar. 27, 2009); see Patient Privacy Rights Foundation, \textit{supra} note 127 (discussing the history and development of privacy regarding medical information).
  \item \textsuperscript{129} Patient Privacy Rights Foundation, \textit{supra} note 127.
  \item \textsuperscript{130} Id.
philosophy is still present in modern medicine. Upon becoming a physician, physicians take the Hippocratic Oath ("Oath"), which requires physicians to never reveal communications between the physician and the patient that arise during the course of treatment and care. In pertinent part, the Oath reads, "Whatever, in connection with my professional practice, or not in connection with it, I see or hear in the life of men, which ought not to be spoken abroad, I will not divulge, as reckoning that all such should be kept secret."

The need within the medical profession to maintain privacy arises for two reasons. First, individuals may be hesitant to disclose intimate information about themselves unless they are guaranteed confidentiality. Second, the very nature of certain information requires confidentiality. The American Medical Association discussed a modern approach to confidentiality in its Principles of Medical Ethics, which states that a physician must safeguard information disclosed during a patient-physician relationship to the greatest degree possible. The principle that communications between a patient and physician must be kept confidential also applies to hospitals, as adapted by the American Hospital Association's Patient's Bill of Rights. Despite the fact that these general aforementioned principles are not law, many courts have treated these principles as enforceable legal obligations.

At common law, medical records which were disclosed without a patient's authorization violated the patient's right to privacy, resulting in a tort action. The common law tort action protected against

131. See 3 ROBERT E. DEWITT ET AL., TREATISE ON HEALTH CARE LAW § 16.02[1][b] (Alexander M. Capron & Irwin M. Birnbaum eds., 2008) ("Hippocrates realized that a patient's willingness to trust his or her physician was absolutely essential to the practice of Medicine. Therefore, he codified the physician's duty to keep the patient's communications private. The Hippocratic Oath requires physicians to put the patient's need for privacy first and foremost, ahead of all else. The key promise every physician makes in taking the Hippocratic Oath upon becoming a physician is never to reveal patients' sensitive communications heard during the course of care and treatment. The importance of acting only on behalf of the patient, which means only with the patient's permission or consent, was later codified into the American Medical Association's (AMA) Principles of Medical Ethics and the ethical principles of every other health profession, as well as the American Hospital Association.").

132. Id.

133. Id.

134. Id. (describing the two reasons for requiring confidentiality).

135. Id.

136. Id.

137. Id.

138. Id. The American Hospital Association's Patient's Bills of Rights was published in 1973. Id.

139. Id.

140. Id. § 16.02[3][b][i].
an invasion of a patient’s privacy interests. Nearly every state has codified a law protecting confidentiality of patients’ medical records. In some states, it is a criminal offense to disclose a patient’s confidential medical records without the patient’s consent.

D. THE CREATION OF HIPAA TO REFORM HEALTH CARE PROCEDURES

As electronic means of paying medical bills and collecting health insurance claims became more widespread, so did the potential for abuse of patients’ medical records. Congress acknowledged a need for health care reform in 1996, specifically when it came to dealing with health care fraud and abuse. On August 21, 1996, Congress enacted the Health Insurance Portability and Accountability Act (“HIPAA”). HIPAA was enacted to make wide-spread changes in the effectiveness and efficiency of the health care system by establishing standards and requirements for the transition of electronic health care information. One of HIPAA’s main goals created standardized confidentiality and focused on the security of medical data, requiring that only authorized individuals have access to patient health information and that the authorized individuals are only allowed access to the patient’s health information that they need. For example, if a patient was referred to a different medical office than the patient normally attended, the new medical office should only receive the medical file, not the billing information, for that patient.

HIPAA created the Security Rule, a national standard for keeping individuals’ private medical information confidential. The Security Rule states that covered entities may not use or disclose an individ-

141. Id.
142. See id. § 16.02[2][a] (“[P]ractically every state has a statute providing for a physician-patient or psychotherapist-patient privilege.”).
143. Id.
147. 3 SUSAN GODSTONE, TREATISE ON HEALTH CARE LAW § 13.01[1][a] (Alexander M. Capron & Irwin M. Birnbaum eds., 2008).
148. HIPAA PRIVACY & SECURITY, supra note 144.
149. Id.
150. GODSTONE, supra note 147.
ual's protected health information.\textsuperscript{151} The Security Rule includes exceptions to the disclosure of an individual's protected health information, for example when the individual gives consent to the disclosure of his or her protected health information.\textsuperscript{152} The Security Rule states that when disclosing or using an individual's protected health information, a covered entity must take reasonable steps to minimize the protected health information released.\textsuperscript{153} The phrase covered entities applies to health care providers, health plans, and health care clearinghouses.\textsuperscript{154} HIPAA defines a health care provider as an individual who provides health or medical services or any individual who provides medical supplies.\textsuperscript{155} A health plan is defined as an individual or group plan which pays the cost of medical care or provides medical care.\textsuperscript{156} A health care clearing house is defined as an entity that processes elements of health information, transforming nonstandard data to standard data.\textsuperscript{157}

HIPAA created standards to regulate covered entities from releasing individuals' protected health information.\textsuperscript{158} An individual's protected health information includes any information that can identify an individual, such as an individual's past and present physical or mental health conditions or an individual's health care payments.\textsuperscript{159} Prior to HIPAA's implementation, each state, and possibly even every

\begin{itemize}
\item \textsuperscript{151} 45 C.F.R. § 164.502 (2009). A covered entity includes health care providers, health plans and health care clearinghouses. \textit{Id.}
\item \textsuperscript{152} \textit{Id.}
\item \textsuperscript{153} \textit{See id.} ("When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.").
\item \textsuperscript{154} GODSTONE, supra note 147; see Microsoft HealthVault & HIPAA, http://msdn.microsoft.com/en-us/healthvault/cc507320.aspx (last visited Apr. 2, 2009) ("Microsoft HealthVault is not a covered entity or business associate as defined by HIPAA;"); see Google Health & HIPAA, http://www.google.com/intl/en-US/health/hipaa.html (last visited Apr. 2, 2009) ("Google Health is not regulated by the Health Insurance Portability and Accountability Act (HIPAA), a federal law that establishes data confidentiality standards for patient health information. This is because Google does not store data on behalf of health care providers. Instead, our primary relationship is with the user.").
\item \textsuperscript{155} 42 U.S.C. § 1320d(3) (2006).
\item \textsuperscript{156} § 1320d(5) (defining different variations of health plans).
\item \textsuperscript{157} § 1320d(2) (stating the entity can be public or private).
\end{itemize}
health care organization, had different rules and regulations relating to the disclosure of an individual’s health records.\textsuperscript{160} Essentially, there was no consistency when it came to protecting an individual’s health records.\textsuperscript{161} Thus, HIPAA created a basic level of privacy and security pertaining to an individual’s health records that is uniform across the United States.\textsuperscript{162} However, state law continues to take precedence over HIPAA if a state implements more strict regulations regarding the privacy and security of an individual’s health records.\textsuperscript{163}

E. THE DOCTRINE OF INFORMED CONSENT

The doctrine of informed consent can be found in two fields: the medical field and the special education field.\textsuperscript{164} In both fields, the idea of informed consent requires that a patient must know about the consequences of a procedure so that the patient can make an educated, informed decision of whether or not to undergo the procedure.\textsuperscript{165}

1. Informed Consent in the Medical Profession

When it comes to making decisions about medical care, a physician must discuss any relevant information needed for his or her patient to make an informed decision.\textsuperscript{166} After a physician discusses the various options and repercussions of the medical procedure with the patient, and a patient fully understands and agrees to the treatment, the patient’s approval of the medical procedure is called informed consent.\textsuperscript{167} The legal doctrine of informed consent developed from the common law rule that a patient subjected to non-consensual medical procedures could hold a physician liable under tort law.\textsuperscript{168}

The doctrine of informed consent developed out of the ethical and legal principles that a patient had the right to participate in his or her health care decisions, and the physician had a duty to involve the patient in the health care decision-making process.\textsuperscript{169} The doctrine of informed consent stemmed from the idea that patients have the right to make informed decisions about matters involving their physical and

\textsuperscript{160} HIPAA PRIVACY & SECURITY, supra note 144.
\textsuperscript{161} Id.
\textsuperscript{162} Id.
\textsuperscript{163} Id.
\textsuperscript{164} 34 C.F.R. § 300.300 (2006); JAMES E. LUDLAM, INFORMED CONSENT 6 (1978).
\textsuperscript{165} See infra notes 166-235 and accompanying text.
\textsuperscript{166} JESSICA W. BERG ET AL., INFORMED CONSENT: LEGAL THEORY AND CLINICAL PRACTICE 11(2nd ed. 2001).
\textsuperscript{167} See id. at 11-12 (discussing the process involved to obtain informed consent).
\textsuperscript{168} LUDLAM, supra note 164, at 19.
mental welfare. Today, informed consent emphasizes both the physician’s duty owed to the patient as well as the patient’s individual rights. A physician owes his or her patient the duty of providing his or her patient with all information necessary for the patient to make an informed decision. The law of informed consent recognizes that the average individual is not knowledgeable in the field of medicine and that the average individual might consent to a medical treatment or procedure while unaware of the medical treatment’s or procedure’s consequences. When a patient is aware of all possible consequences of a proposed medical treatment or procedure, the patient’s consent is informed.


In Schloendorff v. Society of New York Hospital, the New York Court of Appeals stated that individuals have a right to decide what will happen to their own bodies. In Schloendorff, Mary Schloendorff (“Schloendorff”) sued the Society of New York Hospital for medical battery after Schloendorff consented to a medical examination to determine the character of a tumor. Without Schloendorff’s consent, the tumor was removed. Schloendorff testified that a physician performed an operation to remove her tumor without her knowledge or consent. Even though the court found the hospital was not liable for the actions of its physicians, the court addressed the issue of the physician’s individual liability. The court stated that a physician who operates on a patient without the patient’s consent has committed an assault on the patient.

The court reasoned that patients have a right to consent to the medical treatment they receive. The court stated the reason that the physician’s behavior was an assault on Schloendorff’s body be-

170. See LUDLAM, supra note 164, at 8 (discussing the development of the doctrine of informed consent).
171. Id. at 6.
172. Id. at 8.
173. Id. at 72.
174. Id.
175. 105 N.E. 92 (N.Y. 1914).
177. Schloendorff, 105 N.E. at 93.
178. Id.
179. Id.
180. See id. at 95 (finding the hospital was not liable for its physician’s actions).
181. Id. at 93.
182. See id. (“Every human being of adult years and sound mind has a right to determine what shall be done with his own body; and a surgeon who performs an opera-
cause Schloendorff did not consent to any medical treatment other than an examination.183

3. Cobbs v. Grant: The Supreme Court of California Expanded the Reasons Why Informed Consent is Required in Medical Procedures.

In Cobbs v. Grant,184 the Supreme Court of California held that a physician owes a duty to a patient to disclose available choices of medical treatment and the inherent dangers involved with the various choices of medical treatment.185 In Cobbs, Ralph Cobbs ("Cobbs") sued Dr. Dudley Grant ("Grant"), a surgeon, for medical malpractice after Cobbs underwent two surgeries to treat internal bleeding that resulted from damage to Cobbs's spleen during a prior surgery.186 Prior to the two surgeries, Grant explained the surgery's procedure to Cobbs.187 However, Grant did not discuss any inherent dangers involved with the surgery with Cobbs.188 The court held that a physician must discuss, with each patient, possible medical treatments and any dangers associated with the medical treatments.189

The court in Cobbs listed four reasons why it required a physician to obtain informed consent from a patient before performing a medical treatment or procedure.190 First, because patients generally are uneducated in medicine, courts can assume that a patient's and a physician's knowledge of medicine are not equal.191 Second, adult patients have a right to exercise control over their bodies and decide whether to undergo a medical treatment.192 Third, the consent from patients before a medical treatment or procedure can be performed must be an informed consent.193 Fourth, because patients are uneducated in the medical sciences, patients depend upon their physicians for information about medical treatments or procedures in making their informed decisions.194

183. Id. at 93-94.
186. Cobbs, 502 P.2d at 4-5.
187. Id. at 4.
188. Id.
189. Id. at 10.
190. Id. at 9.
191. Id.
192. Id.
193. Id.
194. See id. ("And the fourth is that the patient, being unlearned in medical sciences, has an abject dependence upon and trust in his physician for the information
The court in Cobbs posited that a causal relationship must exist between the patient’s injury and the physician’s failure to tell the patient of necessary information. The court stated that if a physician withholds facts that are necessary for a patient to give an educated and informed consent to a medical treatment or procedure, then the physician has violated a duty owed to the patient.


In Cobbs v. Tongen, the Supreme Court of Minnesota stated that a physician is liable to a patient if the physician does not inform the patient of significant risks associated with medical treatment or if the physician does not explain alternative treatments to the patient. In Cobbs, Jerome Cobbs brought a wrongful death action against Dr. Lyle Tongen ("Tongen"). Tongen performed an operation on Cobbs’s decedent, Phyllis Cobbs, which resulted in her death. Cobbs alleged that Tongen acted negligently after Tongen received abnormal test results concerning Phyllis Cobbs and failed to consult a specialist about Phyllis Cobbs’s test results. Additionally, Tongen performed the operation on Phyllis Cobbs despite the abnormal test results. Cobbs further alleged Tongen was negligent when Tongen failed to inform Phyllis Cobbs of the increased risks of surgery after receiving the abnormal test results.

The court in Cobbs stated that patients have a right to determine what is done with their bodies, but the right is only meaningful if the patients are fully informed of the benefits and risks of a treatment. The court further stated that a physician can be liable to a patient if the physician does not inform the patient of a significant risk involved with a medical treatment or procedure, or the existence of an alternative medical treatment, regardless of whether the physi-
cian adhered to normal medical practice. The court opined that the extent of information a physician must disclose to a patient about a medical treatment or procedure is the amount of information that a physician in good standing would have provided in similar circumstances.


In Kinikin v. Heupel, the Supreme Court of Minnesota stated that a physician has a duty to warn patients of the risks associated with medical procedures. In Kinikin, Harriet Kinikin (“Kinikin”) sued her surgeon, Herman Huepel (“Huepel”), for medical malpractice after Kinikin underwent breast surgery. Specifically, Kinikin consented to a breast surgery called bilateral adenomammectomy. However, Huepel performed a subcutaneous mastectomy. Kinikin stated that she understood the surgery meant a breast reduction with the actual purpose of removing diseased tissue. Kinikin contended that Huepel never explained the term adenomammectomy and the phrase subcutaneous mastectomy to her before she consented to the surgery. Therefore, the issue in Kinikin was whether Huepel properly informed Kinikin of the risks associated with the surgery and whether the surgery was actually the one Kinikin consented to receive. Huepel claimed that his standard to disclose the risks associated with the surgery applied only with regard to significant risks, such as death or serious harm. Ultimately, the court determined that while there is no question that physicians must disclose significant risks of medical treatments or procedures to their patients, such as death and serious harm, physicians must also disclose the risks of medical treatments or procedures that skilled physicians of good standing in their communities would disclose to their patients.

205. Id. at 702
206. Id. (quoting Cobbs, 502 P.2d at 11).
207. 305 N.W.2d 589 (Minn. 1981).
209. Id. at 592.
210. Id.
211. Id.
212. Id.
213. Id. at 593.
214. Id. at 591.
215. See id. at 595 (“Now Dr. Huepel contends Cornfeldt II relieved him of his obligation to disclose this risk . . . . Defendant misconstrues Cornfeldt II. A physician must disclose risks of death or serious bodily harm which are of significant probability; to this there is no contention.”).
216. Id.

Public agencies are required to obtain informed consent from parents of special education children before a public agency administers an initial evaluation to determine if a child needs to be placed in a special education program.217 The Individuals With Disabilities Education Act218 ("IDEA") promulgated state standards to improve the educational opportunities for children with disabilities and standards to involve the parents of children with disabilities in determining educational opportunities and placement for their children.219 The IDEA's standard requiring informed consent from the parents of children with disabilities was created to protect the children's liberty interests.220 An individual's liberty interest consists of a right that protects an individual's freedom from government deprivation without proper due process.221 Liberty interests of children are most vulnerable during the initial evaluation and placement of the children in the education system because it is during this time that a child is treated and identified as a child with special education needs.222 Because a misclassification or a misplacement of a child in the education system infringes on the child's liberty interests, the child's parents need to fully understand the implications of child educational evaluations and placement.223 When a child is labeled as needing special education, there is often a stigma that attaches to such a label.224 This stigma was part of the IDEA's decision to create the parental consent requirement associated with the parents' children's educational choices.225 Additionally, it is so important that parents participate in the educational choices of their children that the IDEA has made participation in such choices mandatory through its consent requirements.226

As part of the standard created from the IDEA, schools are required to obtain informed consent from parents.227 Obtaining in-

---

217. 34 C.F.R. § 300.300(a) (2008).
218. Id.
220. Id. at 175.
222. Huefner, supra note 219, at 175.
223. Id.
224. See Laura F. Rothstein, Special Education Law 107 (3rd ed. 2000) ("Before a child can receive special education or related services, the child must first be identified as having a disability, and an assessment of the particular needs of that child based on the condition must be made.").
225. Id.
226. Id.
formed consent in regards to regulations under the control of the Department of Education rests on three elements. First, the child's parent must be completely informed about all the relevant information pertaining to the activity in question in the parent's native language or through another appropriate form of communication. Second, the child's parent must understand and agree, in writing, to the activity for which the consent is sought. The child's parent's written consent must include the activity described, any records that might be related to the consent, and the identity of the individual to whom the records might be released. Third, the child's parent must voluntarily give consent with the understanding that their informed consent can be revoked at any time.

Consent must be obtained from a child's parent before the child is initially evaluated to determine eligibility under the IDEA. A child's parent's consent must also be obtained before a child receives any special education services and before any reevaluations occur. A school may not simply notify a child's parent that their child is to be evaluated for special educational needs, rather the parent must consent to the school's evaluation or placement of the child.

III. ARGUMENT

A. HEALTHVAULT AND GOOGLE HEALTH SHOULD BE REQUIRED TO OBTAIN INFORMED CONSENT FROM USERS SO USERS ARE FULLY AWARE OF POTENTIAL DANGERS.

Microsoft's HealthVault ("HealthVault") and Google's Google Health ("Google Health") current systems do not adequately warn HealthVault's and Google Health's users of the potential dangers of their services when their users initially sign-up for these services. This Note argues that under the same rationale as the medical and education field, HealthVault and Google Health should require that their users give informed consent to use their services so that their users are warned of the potential risks associated with uploading health records onto the internet before their users actually upload health records. The purpose of this Note is to examine the policies

228. 34 C.F.R. § 300.9 (2008).
229. § 300.9(a).
230. § 300.9(b).
231. Id.
232. § 300.9(c)(1).
233. HUEFNER, supra note 219, at 174.
234. Id.
235. ROTHSTEIN, supra note 224, at 238.
236. See infra notes 252-55 and accompanying text.
237. See infra notes 275-416 and accompanying text.
of HealthVault and Google Health in the context of the Health Insurance Portability and Accountability Act\textsuperscript{238} ("HIPAA") because by definition, HealthVault and Google Health are not covered entities under HIPAA and are thus not required to comply with the privacy standards HIPAA created.\textsuperscript{239} Requiring HealthVault and Google Health to obtain informed consent from their users before the users could upload health records onto their systems would allow their users to make educated decisions when signing up for HealthVault and Google Health.\textsuperscript{240} Finally, just as in medicine and education, mandating that HealthVault and Google Health implement the doctrine of informed consent before allowing their users to make decisions relating to the upload of the users' health records to the internet would mean that the users would know of any potential consequences.\textsuperscript{241}

There is a general lack of understanding about privacy laws with regard to the laws' application to health records.\textsuperscript{242} HealthVault and Google Health do not adequately address how privacy laws affect users of their programs, nor do HealthVault and Google Health warn their users of the potential consequences associated with their programs.\textsuperscript{243} Because health records contain such highly sensitive information about an individual, HealthVault and Google Health need to obtain informed consent from their users so that their users are fully aware of the potential dangers associated with their programs.\textsuperscript{244} Due to the fact that users of HealthVault and Google Health should be fully aware of the potential consequences of such programs because of the highly sensitive information contained within health records, the users should be required to consent to such consequences before the users sign up for the programs.\textsuperscript{245}

HealthVault and Google Health can limit the danger that their users may not understand the possible consequences of posting sensitive health records onto the internet if HealthVault and Google Health implement an informed consent requirement, similar to the doctrine of informed consent used in the medical profession.\textsuperscript{246} In the medical profession, a physician must discuss the various health care options and information relevant to the patient's circumstances with the pa-

\textsuperscript{239} See infra notes 333-84 and accompanying text.
\textsuperscript{240} See infra notes 275-416 and accompanying text.
\textsuperscript{241} See infra notes 275-416 and accompanying text.
\textsuperscript{242} See infra notes 275-416 and accompanying text.
\textsuperscript{243} See infra notes 275-416 and accompanying text.
\textsuperscript{244} See infra notes 275-416 and accompanying text.
\textsuperscript{245} See infra notes 275-416 and accompanying text.
\textsuperscript{246} See infra notes 275-332 and accompanying text.
tient. The physician must ensure that a patient understands the risks associated with a proposed medical treatment, and agrees to it, before the physician can begin the medical treatment. The doctrine of informed consent emphasizes the ethical and legal principle that patients have the right to participate in health care decisions and that a physician has the duty to inform and involve the patient in the patient's health care decisions. A physician must obtain a patient's informed consent before beginning a medical treatment or procedure because average patients do not have a total understanding of the proposed medical treatment and procedures; therefore patients might otherwise consent to a medical treatment or procedure while unaware of the potential consequences. A patient's consent to a medical treatment or procedure is informed when the patient is aware of the medical treatment's or procedure's consequences.

The procedures that HealthVault and Google Health currently have in place do not properly inform their users of the potential consequences associated with signing up for the programs. Neither HealthVault nor Google Health warn their users that a lack of the users' understanding of the users' privacy rights could result in users' health records ending up in unwanted hands. There are potential dangers associated with uploading an individual's health records onto the internet. The dangers associated with uploading an individual's health records onto the internet include the chance that: (i) unauthorized third parties could access electronic health records, (ii) a data breach will allow the free dissemination of the electronic health records, (iii) an unauthorized third party could hack the electronic health records, (iv) an unauthorized third party could sell the elec-

---

248. See id. at 11-12 (discussing requirements for informed consent).
250. Id.
251. Id.
252. See infra notes 275-416 and accompanying text.
Electronic health records, and (v) a HealthVault or Google Health insider could steal the electronic health records.\textsuperscript{255}

A study released by eHealth Vulnerability Reporting Program ("EHVRP") found that electronic health record systems were vulnerable and easy to hack.\textsuperscript{256} Additionally, a report by the Identity Theft Resource Center found that data breaches rose forty-seven percent from 2007 to 2008.\textsuperscript{257} Electronic data breaches far outweighed traditional paper data breaches, with 82.3 percent of the known data breaches affecting electronic data in 2007.\textsuperscript{258} Thus, electronic record programs are susceptible to individuals hacking into them, and furthermore, electronic record program hacking is on the rise.\textsuperscript{259} However, HealthVault and Google Health do not warn their users about the potential and possibility that individuals could very well hack HealthVault’s and Google Health’s electronic record programs.\textsuperscript{260}

HealthVault’s and Google Health’s privacy statements also create a danger to their users, a danger of which their users should be aware.\textsuperscript{261} Under both HealthVault’s and Google Health’s privacy statements, HealthVault’s and Google Health’s users’ private health records are at serious risk of disclosure because HealthVault and Google Health have broad, ambiguous reasons why HealthVault and Google Health will access and disclose their users’ health records.\textsuperscript{262} Because HealthVault’s and Google Health’s privacy statements are so broad, users of these programs are relinquishing all of their privacy rights to HealthVault and Google Health.\textsuperscript{263}

HealthVault and Google Health can implement the doctrine of informed consent to inform their users of the possible dangers associated with uploading health records onto the internet, if they model the informed consent requirements found in special education law.\textsuperscript{264} Special education law requires that schools obtain a child’s parent’s informed consent prior to assessing a child’s special education needs.\textsuperscript{265} The Individuals With Disabilities Education Act\textsuperscript{266}

\begin{thebibliography}{99}
\bibitem{256} Tucci, supra note 254.
\bibitem{257} Data Breaches Soar in 2008, supra note 255.
\bibitem{258} Data Breaches Soar in 2008, supra note 255.
\bibitem{259} Tucci, supra note 254; Data Breaches Soar in 2008, supra note 255.
\bibitem{260} See Privacy Statement Oct. 2008, supra note 253 (discussing HealthVault users’ privacy rights); see Google Privacy Policy, supra note 253 (discussing Google Health users’ privacy rights).
\bibitem{261} See infra notes 275-416 and accompanying text.
\bibitem{262} See infra notes 275-416 and accompanying text.
\bibitem{263} See infra notes 275-416 and accompanying text.
\bibitem{264} See infra notes 385-416 and accompanying text.
\bibitem{265} 34 C.F.R. § 300.300(a) (2008).
\bibitem{266} 34 C.F.R. § 300.9 (2008).
\end{thebibliography}
"IDEA") established standards that provide opportunities for children with disabilities and established that a child’s parents must involve themselves in the placements of their children in special education programs.\textsuperscript{267} Specifically, the IDEA requires that a school must obtain the child’s parent’s informed consent before evaluating the child for special educational needs so the child’s liberty interests are protected.\textsuperscript{268}

Parents need to concern themselves with the consequences of a school’s evaluations and placements of their child because a school’s misplacement of the child in special education programs may infringe upon their child’s liberty interests.\textsuperscript{269} The Department of Education mandates that schools meet three requirements before it will find that a parent gave informed consent in relation to the educational opportunities and evaluations afforded to the parent’s child.\textsuperscript{270} First, a school must fully inform a child’s parent about the necessary information pertaining to the activity that requires the parent’s consent, with the necessary information presented in the parent’s native language or other appropriate form of communication.\textsuperscript{271} Second, a school must have the child’s parents indicate, in writing, that they understand and agree to the consented activity.\textsuperscript{272} Third, the child’s parent’s consent to the school’s activity must be voluntary and revocable at any time.\textsuperscript{273} HealthVault and Google Health should model the IDEA’s informed consent requirements so HealthVault’s and Google Health’s users are adequately informed of the potential dangers associated with the programs.\textsuperscript{274}

B. CASE LAW SHOWS THAT INFORMED CONSENT IS REQUIRED BEFORE PHYSICIANS PERFORM A MEDICAL PROCEDURE AND THAT PHYSICIANS HAVE A DUTY TO DISCLOSE RISKS TO PATIENTS, A DUTY WHICH SHOULD APPLY TO HEALTHVAULT AND GOOGLE HEALTH.

The Supreme Courts of Minnesota and California, and the New York Court of Appeals, held that a patient’s physician must obtain informed consent before a medical treatment or procedure can occur because patients have a right to make decisions about their medical

\textsuperscript{267} DIXIE SNOW HUEFNER, GETTING COMFORTABLE WITH SPECIAL EDUCATION LAW: A FRAMEWORK FOR WORKING WITH CHILDREN WITH DISABILITIES 23, 25 (2000).
\textsuperscript{268} Id. at 175.
\textsuperscript{269} Id.
\textsuperscript{270} 34 C.F.R. § 300.9.
\textsuperscript{271} § 300.9(a).
\textsuperscript{272} § 300.9(b).
\textsuperscript{273} § 300.9(c)(1).
\textsuperscript{274} See infra notes 385-416 and accompanying text.
treatments or procedures. The reasoning established by the aforementioned supreme courts, and their related case law, should apply to service providers such as Microsoft’s HealthVault (“HealthVault”) and Google’s Google Health (“Google Health”) so that their users are aware of the significant risks they face upon signing up for such programs. While there is no informed consent requirement related to these programs, HealthVault and Google Health should have to obtain informed consent from their users to disclose the risks associated with the programs, before allowing their users to upload the users’ health records onto the internet.

Case law has consistently determined that a physician has a duty to disclose all available medical treatments and procedures, and any risks associated with medical treatments and procedures, to their patient. Based on this duty, case law states that physicians are required to obtain informed consent from the patient prior to a medical treatment or procedure. In Schloendorff v. Society of New York Hospital and Cobbs v. Grant, the New York Court of Appeals and the California Supreme Court, respectively, reasoned that informed consent is required in the medical profession because patients have the right to make fully informed decisions about their bodies including whether or not to undergo a medical procedure. In Schloendorff, Mary Schloendorff (“Schloendorff”) was suffering from a stomach disorder when her physician advised her to undergo an operation on her stomach. Schloendorff’s physician sought to examine the tumor. Schloendorff consented to the physician’s examination of the tumor, but she did not consent to an operation. However, the physician performed a surgery on Schloendorff that removed the tumor without Schloendorff’s consent. The New York Court of Appeals stated that when a physician operates on a patient without the patient’s consent, the physician has committed an assault on the pa-

275. Kinikin v. Heupel, 305 N.W.2d 589, 595 (Minn. 1981); Cornfeldt v. Tongen, 262 N.W.2d 584, 701-02 (Minn. 1977); Cobbs v. Grant, 502 P.2d 1, 10 (Cal. 1972); Schloendorff v. Society of N.Y. Hosp., 105 N.E. 92, 93 (N.Y. 1914).
276. See infra note 278-332 and accompanying text.
277. See infra note 278-416 and accompanying text.
278. Kinikin, 305 N.W.2d at 595; Cornfeldt, 262 N.W.2d at 702; Cobbs, 502 P.2d at 10; Schloendorff, 105 N.E. at 93.
279. Kinikin, 305 N.W.2d at 595; Cornfeldt, 262 N.W.2d at 702; Cobbs, 502 P.2d at 10; Schloendorff, 105 N.E. at 93.
280. 105 N.E. 92 (N.Y. 1914).
282. Cobbs, 502 P.2d at 9; Schloendorff, 105 N.E. at 93.
283. Schloendorff, 105 N.E. at 93.
284. Id.
285. Id.
286. Id.
2009] \textit{INTERNET HEALTH CARE PROGRAMS} 761

tient.\textsuperscript{287} In \textit{Cobbs}, Ralph Cobbs ("Cobbs") underwent two operations to treat internal bleeding that resulted from a previous operation.\textsuperscript{288} The physician, Dudley Grant ("Grant"), did not discuss with Cobbs any of the inherent dangers involved with the original operation that lead to the internal bleeding.\textsuperscript{289} In \textit{Cobbs}, the California Supreme Court held that Grant breached his duty to inform Cobbs of any complications that may arise during the first operation.\textsuperscript{290} Therefore, the court held that Grant had a duty to disclose the available choices with regard to medical treatments and procedures, and the inherent dangers involved or potentially involved in such treatments and procedures to Cobbs before performing the operation, which resulted in Cobbs' internal bleeding.\textsuperscript{291} Thus, in \textit{Schloendorff} and \textit{Cobbs}, both the New York Court of Appeals and the California Supreme Court deemed that a physician must obtain informed consent from his or her patient because patients have the right to be made aware of the consequences that may result from the patient's medical procedure.\textsuperscript{292} Further, both courts held that physician's have a duty to inform their patients of the consequences that may result from the patient's medical procedure.\textsuperscript{293}

Moreover, courts have consistently determined that physicians are liable to their patients when they fail to disclose any risks or consequences of a medical treatment or procedure.\textsuperscript{294} For instance, the Supreme Court of Minnesota's decisions in \textit{Cornfeldt v. Tongen}\textsuperscript{295} and \textit{Kinikin v. Heupel}\textsuperscript{296} are two such examples.\textsuperscript{297} In \textit{Cornfeldt}, the Supreme Court of Minnesota held that physicians can be liable to patients if they fail to disclose significant risks associated with a medical treatment or procedure to their patients.\textsuperscript{298} In \textit{Cornfeldt}, Jerome Cornfeldt ("Cornfeldt") brought a wrongful death action against Lyle Tongen("Tongen"), a physician, after Phyllis Cornfeldt underwent an operation that resulted in her death.\textsuperscript{299} The day before Tongen operated on Phyllis Cornfeldt, routine tests were performed on Phyllis

\begin{itemize}
\item \textsuperscript{287} \textit{Id.} at 129-30.
\item \textsuperscript{288} \textit{Cobbs}, 502 P.2d at 4, 5.
\item \textsuperscript{289} \textit{Id.} at 4.
\item \textsuperscript{290} \textit{Id.} at 10.
\item \textsuperscript{291} \textit{Id.}
\item \textsuperscript{292} \textit{Schloendorff}, 105 N.E. at 93; \textit{Cobbs}, 502 P.2d at 9.
\item \textsuperscript{293} \textit{Id.}
\item \textsuperscript{294} \textit{Kinikin}, 305 N.W.2d at 595-96; \textit{Cornfeldt}, 262 N.W.2d at 702; \textit{Cobbs}, 502 P.2d at 9; \textit{Schloendorff}, 105 N.E. at 93.
\item \textsuperscript{295} 262 N.W.2d 684 (Minn. 1977).
\item \textsuperscript{296} 305 N.W.2d at 595(Minn. 1988).
\item \textsuperscript{297} Kinikin v. Heupel, 305 N.W.2d 589, 595 (Minn. 1981).
\item \textsuperscript{298} \textit{Cornfeldt}, 262 N.W.2d at 702.
\item \textsuperscript{299} \textit{Id.} at 689-91.
\end{itemize}
The routine tests came back with abnormal results. However, neither Tongen, nor anyone else, disclosed the test results to Phyllis Cornfeldt. After Phyllis Cornfeldt’s death, Cornfeldt brought a cause of action against Tongen which alleged that Tongen acted negligently in not consulting with a specialist about Phyllis Cornfeldt’s abnormal test results and not informing Phyllis Cornfeldt of the added risks of the operation due to the abnormal test results.

In *Kinikin*, the Supreme Court of Minnesota also held that a physician had a duty to warn his or her patients of any risks involved in a medical treatment or procedure. In *Kinikin*, Harriet Kinikin (“Kinikin”) underwent breast surgery. Kinikin gave consent to her physician, Herman Heupel (“Heupel”), to perform a breast operation called a bilateral adenomammectomy, however Heupel performed a subcutaneous mastectomy. Kinikin brought a cause of action against Heupel which alleged that she understood and consented to only a breast reduction, when in reality the primary goal of the operation was to remove diseased tissue. Kinikin contended that Heupel never explained the meaning of adenomammectomy or subcutaneous mastectomy. Kinikin also stated that had Heupel informed her of the risks and complications of the operations, she would not have given her consent. Essentially, the issue in *Kinikin* was whether Heupel properly informed Kinikin of the risks associated with the operation. Ultimately, the court determined that Heupel had a duty to warn Kinikin of any risks involved in a medical treatment or procedure before performing the actual medical treatment or procedure. Thus, in both *Cornfeldt* and *Kinikin*, the Minnesota Supreme Court stated that a physician has a duty to disclose the significant risks related to a medical treatment or procedure to a patient.

Similar to the physicians in *Schloendorff, Cobbs, Cornfeldt*, and *Kinikin*, HealthVault and Google Health have failed in their duty to disclose the potential dangers of the service they provide to their
users. Just as the physicians in the aforementioned cases had a duty to disclose the significant dangers of the medical treatments or procedures they recommended to their patients, HealthVault and Google Health have a duty to disclose significant risks to individuals who use HealthVault and Google Health. As indicated by numerous studies, there are significant risks associated with electronic health record systems. Such risks of electronic health record systems include potential data breaches, insider theft, hacking, and accidental breaches of the electronic health records. For instance, HealthVault has a duty to disclose to its users the history of breaches that its own partners have allowed in the past.

Specifically, one of HealthVault's partner's, Kaiser Permanente's, electronic health record systems were breached on a number of occasions. Kaiser Permanente's electronic health record systems that

313. Compare Kinikin, 305 N.W.2d at 595 (stating a physician has a duty to warn patients of risks associated with medical procedures), and Cornfeldt, 262 N.W.2d at 702 (stating a physician has a duty to disclose significant risks to a patient when making health care decisions), and Cobbs, 502 P.2d at 10 (stating a physician owes a duty to a patient to disclose inherent dangers and available choices of medical treatments to a patient), and Schloendorff, 105 N.E. at 93 (stating patients have a right to decide what happens to their bodies and therefore physicians must obtain patients' consent before performing operations), with Microsoft HealthVault Information Site Beta Version Privacy Statement, http://www.healthvault.com/privacy-policy.html (last visited Mar. 23, 2009) [hereinafter Privacy Statement June 2008]) (including no warning of potential dangers or consequences of uploading medical records to the internet), and Google Health Privacy Policy, http://www.google.com/intl/en-US/health/privacy.html (last visited Mar. 26, 2009) (stating the benefits of signing up for the program, but listing no possible consequences or dangers associated with using the program).

314. See infra notes 318-32 and accompanying text.

315. Tucci, supra note 254.


317. See infra notes 318-32 and accompanying text.

were breached often contained personal patient information such as contact information, answers to sensitive medical questions, birthdays, and names.\textsuperscript{319} Similarly, HealthVault and Google Health's electronic health record systems could be breached, therefore exposing HealthVault's and Google Health's users' private health records.\textsuperscript{320} HealthVault's privacy statement also leaves HealthVault with ample opportunity to take advantage of its users' private health records.\textsuperscript{321} While HealthVault's privacy statement claims that HealthVault is committed to protecting its users' health records, its privacy statement's broad exceptions for accessing such records leads to the opposite conclusion.\textsuperscript{322} Thus, HealthVault's users run a serious risk of exposing their health records when uploading such records to HealthVault because of HealthVault's overly broad privacy exceptions.\textsuperscript{323} Google Health's privacy statement also leaves Google Health ample opportunity to access its users' health records.\textsuperscript{324} Finally, HealthVault and Google Health face the possibility that hackers could infiltrate the programs.\textsuperscript{325}

Furthermore, just as the patients in Schloendorff, Cobbs, Cornfeldt, and Kinikin were unaware of the risks associated with their medical treatments or procedures, so are HealthVault's and Google Health's users.\textsuperscript{326} Therefore, HealthVault and Google Health have a duty to inform their users of the potential dangers associated with their programs.\textsuperscript{327} HealthVault and Google Health should both be aware of the dangers associated with uploading an individual's pri-

\textsuperscript{319} Kaiser Joins Lost Laptop Crowd, supra note 318; Laptop With Patient Info Stolen, supra note 318; Lee, supra note 318; Martinez, supra note 318; Vrana, supra 318.


\textsuperscript{321} PRIVACY RIGHTS CLEARINGHOUSE, supra note 320.

\textsuperscript{322} Id.

\textsuperscript{323} Id.

\textsuperscript{324} Herrin, supra note 320.

\textsuperscript{325} PRIVACY RIGHTS CLEARINGHOUSE, supra note 320; Herrin, supra note 320.

\textsuperscript{326} Compare Kinikin, 305 N.W.2d at 595 (discussing whether the patient was properly informed of the risks associated with the operation the patient received), and Cornfeldt, 262 N.W.2d at 702 (discussing Mrs. Cornfeldt's physicians did not disclose the risks associated with her operation, which resulted in Mrs. Cornfeldt's death), and Cobbs, 502 P.2d at 10 (discussing plaintiff underwent two operations without knowing the inherent dangers associated with the operations), with Privacy Statement June 2008, supra note 313 (discussing no risks associated with using the service), and Google Health Privacy Policy, supra note 313 (listing no possible consequences or dangers associated with using the program).

\textsuperscript{327} See infra notes 330-32 and accompanying text.
vate health records onto the internet.\textsuperscript{328} Despite HealthVault's stated commitment its users' privacy, it never disclosed the multiple breaches of secure data that occurred at Kaiser Permanente.\textsuperscript{329}

Using the analogous analysis established in \textit{Schloendorf, Cobbs, Cornfeldt, and Kinikin}, HealthVault and Google Health should have a duty to disclose the inherent dangers associated with their programs to their users.\textsuperscript{330} Under the reasoning set forth by the Supreme Courts of Minnesota and California, and the New York Court of Appeals, HealthVault and Google Health should be required to adopt the doctrine of informed consent so their users are aware of the potential danger that the users' health records face before the users are allowed to sign up for the programs.\textsuperscript{331} Therefore, HealthVault and Google Health should implement a mechanism for informed consent into their respective program's sign-up procedure.\textsuperscript{332}

C. \textbf{HEALTHVAULT AND GOOGLE HEALTH NEED TO OBTAIN INFORMED CONSENT FROM USERS BECAUSE, UNDER THE DEFINITIONS SET FORTH IN HIPAA, HEALTHVAULT AND GOOGLE HEALTH ARE NOT COVERED ENTITIES AND ARE THUS NOT PROTECTED BY HIPAA'S GUIDELINES.}

Microsoft's HealthVault ("HealthVault") and Google's Google Health ("Google Health") need to obtain informed consent from their users to ensure that their users are properly informed of the potential risks associated with uploading the users' personal health records to their programs because, contrary to public opinion, the Health Insurance Portability and Accountability Act ("HIPAA")\textsuperscript{333} does not protect health records on HealthVault or Google Health.\textsuperscript{334} Under HIPAA's definitions, HIPAA does not apply to HealthVault or Google Health because such programs are not "covered entities."\textsuperscript{335}

Congress enacted HIPAA to establish standards and requirements for the transmission of electronic health records.\textsuperscript{336} Specifically, HIPAA requires covered entities to take reasonable steps to

\begin{itemize}
  \item \textsuperscript{328} See infra notes 329-32 and accompanying text.
  \item \textsuperscript{329} Privacy Statement June 2008, supra note 313; Kaiser Permanente and Microsoft; supra note 318.
  \item \textsuperscript{330} See supra notes 275-329 and accompanying text.
  \item \textsuperscript{331} See supra notes 275-329 and accompanying text.
  \item \textsuperscript{332} See supra notes 275-329 and accompanying text.
  \item \textsuperscript{333} 42 U.S.C. § 201 (2006).
  \item \textsuperscript{334} See infra notes 336-51 and accompanying text.
  \item \textsuperscript{336} 3 SUSAN GODSTONE, TREATISE ON HEALTH CARE LAW § 13.01[1][a] (Alexander M. Capron & Irwin M. Birnbaum eds., 2008).
\end{itemize}
limit the use and disclosure of protected health records.337 A covered entity, under HIPAA, includes health care providers, health plans, and health care clearinghouses.338 As defined by HIPAA, a health care provider offers health or medical services or is a person providing health care services and supplies.339 HIPAA defines a health plan as a group or individual plan which provides medical care or pays the cost of medical care.340 A health care clearinghouse is a private or public entity that processes nonstandard health data information into standard data.341 HIPAA’s Security Rule requires covered entities to create appropriate and sensible administrative and technical measures to protect electronic health records.342

By definition, HealthVault and Google Health are not covered entities under HIPAA.343 Specifically, HealthVault and Google Health do not fit under the definitions of health care providers, health plans, or health care clearinghouses.344 First, HealthVault and Google Health are not health care providers because they do not perform health services.345 Second, HealthVault and Google Health are not health plans because they do not pay the cost of medical care.346

337. 45 C.F.R. 164.502 (2009). ("When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.").

338. GODSTONE, supra note 336, § 13.01[1][a].


340. Id.

341. Id.


343. Compare Microsoft Health Vault and HIPAA, supra note 335 (stating HealthVault does not hold any records that are covered by HIPAA and the regulations do not apply to HealthVault), and Google Health and HIPAA, supra note 335 (stating Google is not a healthcare provider and thus HIPAA is not applicable to Google Health), with GODSTONE, supra note 336, § 13.01[1][a] (stating HIPAA is applicable to covered entities, which include health care clearinghouses, health care plans, and health care providers).

344. Compare Microsoft HealthVault and HIPAA, supra note 335 (indicating HealthVault is not a covered entity under HIPAA because HealthVault is not health care clearing house, health care plan or health care provider), and Google Health and HIPAA, supra note 335 (discussing HIPAA does not apply to Google Health because Google Health is not a healthcare provider), with GODSTONE, supra note 336, § 13.01[1][a] (discussing HIPAA is applicable to covered entities, which include health care clearinghouses, health care plans, and health care providers).

345. Compare Microsoft Health Vault and HIPAA, supra note 335 (indicating HealthVault is not a health care provider because HealthVault does not provide health care service or supplies), and Google Health and HIPAA, supra note 335 (indicating HIPAA does not apply to Google Health), with 42 U.S.C. § 1320d (2006) (defining a health care provider as a provider of health care supplies or services).

346. Compare Microsoft Health Vault and HIPAA, supra note 335 (indicating HealthVault is not a covered entity under HIPAA because HealthVault is not health care plan because HealthVault does not pay the cost of medical care or provide medical
Third, HealthVault and Google Health are not health care clearing-houses because they do not process nonstandard health data information into standard data.\textsuperscript{347} Thus, HealthVault and Google Health are not covered entities under HIPAA's definitions.\textsuperscript{348} Therefore HIPAA does not regulate HealthVault or Google Health.\textsuperscript{349}

Because HIPAA does not regulate HealthVault or Google Health, HealthVault and Google Health need to implement an informed consent requirement that will ensure that users who sign up for HealthVault or Google Health will know that their private medical information is not protected by HIPAA.\textsuperscript{350} HealthVault's and Google Health's informed consent requirement would mandate that such programs educate their users as to the fact that HIPAA does not apply to HealthVault and Google Health, and will therefore not protect HealthVault's or Google Health's users' private health records.\textsuperscript{351}

D. HEALTHVAULT AND GOOGLE HEALTH NEED TO OBTAIN INFORMED CONSENT FROM USERS BECAUSE HEALTHVAULT AND GOOGLE HEALTH DO NOT PROTECT HEALTH INFORMATION THE WAY HIPAA INTENDED.

Microsoft's HealthVault ("HealthVault") and Google's Google Health ("Google Health") need to obtain informed consent from users because obtaining informed consent would ensure that their users know that the Health Insurance Portability and Accountability Act ("HIPAA")\textsuperscript{352} does not apply to health records uploaded onto HealthVault and Google Health.\textsuperscript{353} HIPAA was created as an attempt to reform the health care system and provide protection to elec-

---

\textsuperscript{347} Compare Microsoft Health Vault and HIPAA, supra note 335 (indicating HIPAA does not apply to Google Health because Google Health is not a health care plan because Google Health does not pay for medical care or provide medical care), with 42 U.S.C. § 1320d (defining a health care plan as a group or individual plan which pays for and provides medical care).

\textsuperscript{348} Microsoft Health Vault and HIPAA, supra note 335; Google Health and HIPAA, supra note 335.

\textsuperscript{349} Microsoft Health Vault and HIPAA, supra note 335; Google Health and HIPAA, supra note 335.

\textsuperscript{350} See supra notes 333-49 and accompanying text.

\textsuperscript{351} See supra notes 333-49 and accompanying text.


\textsuperscript{353} See infra notes 354-84 and accompanying text.
Electronic health records. However, after patients gain control over their health records, HIPAA does not protect the patients' health records. Because patients have control over their health records when using HealthVault and Google Health, their health records no longer fall under the auspice of HIPAA's protection. Therefore, HealthVault and Google Health do not have adequate protection in place.

HIPAA was created to improve the effectiveness and efficiency of the health care system. Specifically, HIPAA was designed to protect a patient's private health records when the patient's health records are out of the patient's control. For example, HIPAA protects a patient's health records when the patient's health records are handled by a third-party for billing purposes. HIPAA's main focus required that only authorized individuals could have access to a patient's health records, and then only to necessary records. HIPAA created confidentiality standards for medical information and procedures for the security of medical data. HIPAA's standard, contained in its Security Rule, keeps individuals' protected medical records confidential. HIPAA's Security Rule states that disclosure and use of protected health records must be limited to the release of the health records necessary to achieve the intended purpose of the request. As part of HIPAA's guidelines, an individual has the right to obtain a copy of his or her medical records. However, once an individual obtains his or her medical records for personal use, HIPAA no longer regulates what that individual does with his or her medical records.

HealthVault's and Google Health's security measures do not protect their users' medical records to the degree HIPAA intended.

354. GODSTONE, supra note 336, § 13.01[1][a].
356. Microsoft HealthVault and HIPAA, supra note 355.
357. See infra notes 358-84 and accompanying text.
358. GODSTONE, supra note 236, § 13.01[1][a].
359. Microsoft HealthVault and HIPAA, supra note 355.
360. Microsoft HealthVault and HIPAA, supra note 355.
362. Id.
363. GODSTONE, supra note 336, at § 13.01[1][B][iii].
365. Microsoft HealthVault and HIPAA, supra note 355.
366. Microsoft HealthVault and HIPAA, supra note 355.
Congress’ intended purpose in enacting HIPAA was to protect an individual’s medical records from unauthorized use and disclosure, but HealthVault and Google Health do not have regulations in their privacy statements that serve a similar purpose. HealthVault and Google Health both claim that they protect their users’ medical records. However, the exceptions contained in HealthVault’s and Google Health’s privacy statements cause their users’ medical records to become vulnerable in that the privacy statements allow access and the potential for abuse of the medical records, which is in direct opposition to HIPAA’s intended purpose.

HealthVault’s privacy statement claims that HealthVault is committed to protecting its users’ privacy. However, HealthVault’s privacy statement lists three broad exceptions in which HealthVault can access and release its users’ private medical records. First, HealthVault’s privacy statement states that HealthVault may access and release its users’ medical records if such a release is necessary to follow the law. Second, HealthVault’s privacy statement states that HealthVault may access and release its users’ medical records if such a release is necessary to defend and protect the property and rights of Microsoft. Third, HealthVault’s privacy statement states that HealthVault may access and release its users’ medical records if


368. Compare 45 C.F.R. § 164.502 (noting covered entities must make reasonable efforts to protect health information), with Privacy Statement June 2008, supra note 367 (discussing health records can be released to comply with law, to protect Microsoft’s property and rights, and to protect Microsoft users or the public), and Google Health Privacy Policy, supra note 367 (noting health records can be released to comply with law, to protect Google’s property, to comply with Google’s Terms of Services and to provide information to affiliates and subsidiaries).


370. Compare 45 C.F.R. § 164.502 (allowing only authorized individuals to access protected medical information, and only the information that is absolutely necessary), with Privacy Statement June 2008, supra note 367 (stating Microsoft is committed to protecting user’s privacy, but reserves three instances in which Microsoft’s interests outweigh a user’s right to privacy), and Google Health Privacy Policy, supra note 367 (stating the user controls the record, but reserves a number of reasons when Google can take control of the record).


372. See id. (discussing situations when HealthVault can access and disclose users’ information).

373. Id.

374. Id.
such a release is necessary to protect the welfare and safety of Microsoft users or the public.\textsuperscript{375}

Google Health also reserves a number of situations in which it will release its users' private medical records.\textsuperscript{376} For example, Google Health's privacy statement states that Google may disclose its users' private medical records with other individuals and companies outside of Google if Google obtains the user's consent.\textsuperscript{377} Additionally, Google Health's privacy statement also states that Google reserves the right to share its users' private medical records with its subsidiaries, affiliated companies, and trusted businesses.\textsuperscript{378} Furthermore, Google Health's privacy statement states that Google may share its users' medical records if Google needs to comply with a governmental request or the law.\textsuperscript{379} Finally, Google Health's privacy statement states that it may release its users' medical records to enforce Google's Terms of Service and to protect Google's rights.\textsuperscript{380}

Before allowing their users to upload the users' medical records onto the internet, HealthVault and Google Health should obtain its users' informed consent to ensure that its users are fully aware that HealthVault's and Google Health's privacy statements do not provide their users the same level of protection in relation to the users' medical records as such records are afforded under HIPAA guidelines.\textsuperscript{381} Congress created HIPAA to prevent the disclosure of an individual's private medical records.\textsuperscript{382} The privacy statements of HealthVault and Google Health do not attempt to prevent the disclosure of an individual's private medical records.\textsuperscript{383} HealthVault and Google Health should educate their users of the discrepancy between the levels of protection afforded to an individual's medical records under their privacy statements and under HIPAA so that their users are aware of the potential dangers associated with uploading medical records to HealthVault and Google Health.\textsuperscript{384}

\begin{itemize}
\item \textsuperscript{375} Id.
\item \textsuperscript{376} Google Health Privacy Policy, supra note 367.
\item \textsuperscript{377} Google Health Privacy Policy, supra note 367.
\item \textsuperscript{378} See id. ("We provide such information to our subsidiaries, affiliated companies or other trusted businesses or persons for the purpose of processing personal information on our behalf. We require that these parties agree to process such information based on our instructions and in compliance with this Privacy Policy and any other appropriate confidentiality and security measures.").
\item \textsuperscript{379} Id.
\item \textsuperscript{380} Id.
\item \textsuperscript{381} See supra notes 352-80 and accompanying text.
\item \textsuperscript{382} See supra notes 352-80 and accompanying text.
\item \textsuperscript{383} See supra notes 352-80 and accompanying text.
\item \textsuperscript{384} See supra notes 352-80 and accompanying text.
\end{itemize}
E. HEALTHVAULT AND GOOGLE HEALTH SHOULD FOLLOW THE MODEL OF THE SPECIAL EDUCATION REQUIREMENTS FOR INFORMED CONSENT, SO THEIR USERS ARE AWARE OF THE DANGERS ASSOCIATED WITH UPLOADING MEDICAL RECORDS TO THE INTERNET.

Just as informed consent has been implemented in special education to ensure parents make informed decisions about the special needs of their children, Microsoft’s HealthVault ("HealthVault") and Google’s Google Health ("Google Health") should implement an informed consent requirement for users of their programs. In the special education system, the doctrine of informed consent successfully educates parents about the dangers of evaluation and placement of their children. HealthVault and Google Health should obtain informed consent from their users before their users join their programs, before users upload their medical records, and before users grant third parties permission to access their medical records. Similar to special education law, the proposed requirements concerning the informed consent that HealthVault and Google Health should obtain necessitates that all necessary information related to a user’s consent must be present, and in the user’s native language. Furthermore, HealthVault’s and Google Health’s users need to understand and agree, in writing, to what they are consenting. Finally, HealthVault and Google Health must obtain their users voluntary consent and must allow users to reserve the right to revoke their consent at anytime.

In special education law, school districts are required to obtain consent from parents prior to the initial evaluation of their child, to the placement of their child, and prior to a re-evaluation of their child. The Individuals With Disabilities Education Act ("IDEA") created standards and procedural safeguards to provide children with special needs optimal educational opportunities. As part of IDEA, a school is required to obtain a child’s parents’ consent for a number of

385. See infra notes 391-416 and accompanying text.
386. See 34 C.F.R. § 300.9 (2009) ("Consent means that [t]hat the parent has been fully informed of all information relevant to the activity for which consent is sought, in his or her native language, or through another mode of communication.").
387. See infra notes 391-416 and accompanying text.
388. See infra notes 391-416 and accompanying text.
389. See infra notes 391-416 and accompanying text.
390. See infra notes 391-416 and accompanying text.
391. DIXIE S. HUEFFNER, GETTING COMFORTABLE WITH SPECIAL EDUCATION LAW: A FRAMEWORK FOR WORKING WITH CHILDREN WITH DISABILITIES 174, 175 (2000).
392. 34 C.F.R. § 300.9 (2009)
393. See id. at 25 ("In general, the Amendments focus on efforts to improve the outcomes for students with disabilities, largely by increasing access to general education reforms and the general education curriculum.").
reasons. First, it is important to involve the child’s parents in the decision-making processes that may affect their children. Second, a child’s parents need to be aware of the consequences of evaluating their child for special educational needs and the potential dangers of misclassification. Third, when an evaluation of a child is made, a label is placed on the child, often creating a stigma. The child is treated differently from other children, which in turn can make the child vulnerable. A child’s parents’ consent is thus required to inform the child’s parents of these aforementioned consequences and possibilities.

IDEA set forth three requirements necessary to properly obtain informed consent from a child’s parent. First, the child’s parent must be properly informed about all relevant information pertaining to the pertinent activity. The school presents the relevant information in the child’s parent’s native language or another method of communication that the child’s parent understands. Second, in writing, the child’s parent must agree and understand to carrying out the pertinent activity. Third, the child’s parent’s consent to the school’s recommended activity must be voluntary and revocable at any time.

Contrary to IDEA’s requirement that a child’s parents must give informed consent prior to a school’s evaluation or placement of the parent’s child in a special education situation, HealthVault and Google Health do not obtain informed consent from their users before their users post their medical records on the internet. Instead, HealthVault and Google Health provide their users with their respective consent agreements.

394. Id. at 174.
395. Id. at 25, 174, 175.
396. Id.
397. LAURA F. ROTHSTEIN, SPECIAL EDUCATION LAW 107 (3rd ed. 2000).
398. HUEFNER, supra note 391, at 175.
399. Id.
400. 34 C.F.R. § 300.9 (2009) (discussing the requirements for obtaining informed consent).
401. § 300.9(a).
402. Id.
403. § 300.9(b).
404. § 300.9(c)(1).
405. Compare § 300.9 (listing three requirements necessary to satisfy the consent requirement), and HUEFNER, supra note 391, at 174 (stating parental consent is required from parents prior to conducting an evaluation, placement or reevaluation), with Microsoft HealthVault Information Site Beta Version Privacy Statement, http://www.healthvault.com/privacy-policy.html (last visited Mar. 23, 2009) (hereinafter Privacy Statement June 2008) (including no requirement for informed consent, and not including any dangers associated with signing up for the service), and Google Health Privacy Policy, http://www.google.com/intl/en-US/health/privacy.html (last visited Mar. 26, 2009) (discussing no possible consequences of using the service and also does not requiring informed consent prior to signing up for the program).
tive service agreements when users sign up for the programs. In fact, users can easily read HealthVault's and Google Health's service agreements without comprehending the service agreements or skip reading the service agreements completely. Similar to the consequences and dangers of diagnosing a child as a special needs child, there are potential dangers associated with using HealthVault and Google Health. For example, by not requiring informed consent, HealthVault and Google Health are leaving their users susceptible to potential data breaches, insider theft, hacking, and accidental breaches.

Thus, applying the reasoning for requiring parental consent in special education situations, HealthVault and Google Health should obtain informed consent from their users before allowing their users to use HealthVault and Google Health so their users are aware of the dangers and consequences of using such programs. HealthVault and Google Health should establish requirements that model the requirements found in special education law. Just like the IDEA requirements of consent, HealthVault and Google Health should educate their users to the highest degree possible about any relevant information pertaining to the programs. HealthVault and Google Health should educate their users with information in the user's native language, or other appropriate communication method that the user will understand. Next, HealthVault's and Google Health's users should understand and agree to the activity for which HealthVault and Google Health are seeking their consent. Finally, the consent of a HealthVault or Google Health user must be voluntary.


407. See infra notes 408-16 and accompanying text.

408. Compare ROTHSTEIN, supra note 397, at 107 (stating a parent needs to know and consent to evaluations of children because of the dangers associated with the evaluations and placements), with What is HealthVault? Think Twice Before You Participate, PRIVACY RIGHTS CLEARINGHOUSE http://www.privacyrights.org/ar/healthVault.htm (last visited Apr. 4, 2009) (discussing privacy concerns with HealthVault that were not adequately addressed by HealthVault), and Liz Herrin, Google Health Announces New Improvements, Raises Old Concerns, rePELES, Feb. 26, 2009, http://www.ieplexus.com/industry-news/1110-google-health-announces-new-improvements-raises-old-concerns/ (discussing the dangers of Google Health, including Google's privacy policy and concerns over hackers).


410. See supra notes 385-409 and accompanying text.

411. See supra notes 385-409 and accompanying text.

412. See supra notes 385-409 and accompanying text.

413. See supra notes 385-409 and accompanying text.

414. See supra notes 385-409 and accompanying text.
and revocable at any time. Instituting a procedure that matches IDEA’s requirements will allow HealthVault and Google Health to provide their users with the appropriate opportunity to knowingly assent to any and all of the risks that accompany the use of their programs.

IV. CONCLUSION

Internet programs that allow their users to upload medical records for online storage should obtain informed consent from their users so their users have a complete understanding of the ramifications that are associated with putting personal information on the internet. Confusing privacy statements and a general lack of understanding on privacy law often leads Microsoft’s HealthVault’s (“HealthVault”) and Google’s Google Health’s (“Google Health”) users to mistakenly believe their health records, when posted to HealthVault and Google Health, are safe from abuse. HealthVault and Google Health both have confusing privacy statements which reserve HealthVault’s and Google Health’s right to access their users’ private health records. HealthVault and Google Health claim that they will only access their users’ health records under limited circumstances. However, a close reading of HealthVault’s and Google Health’s privacy statements indicates that the circumstances in which they can access their user’s health records are quite broad. The language of HealthVault’s and Google Health’s privacy statements is such that the companies can very easily justify accessing their users’ private health records.

There is the risk that HealthVault and Google Health might access their users’ health records, but there is also a risk that third parties might abuse the users’ health records if the users choose to share the users’ health records with a third party. Once a user’s health records are transmitted to a third party on HealthVault and Google Health, the third party has control over the user’s medical records. Even if HealthVault and Google Health’s users revoke the third

415. See supra notes 385-409 and accompanying text.
416. See supra notes 385-409 and accompanying text.
417. See supra notes 236-416 and accompanying text.
418. See supra notes 236-416 and accompanying text.
419. See supra notes 236-416 and accompanying text.
420. See supra notes 236-416 and accompanying text.
421. See supra notes 236-416 and accompanying text.
422. See supra notes 236-416 and accompanying text.
party's access to their health records, the third party might have already retained a copy of the record. Abuse of HealthVault's and Google Health's users' medical records could also easily result from an internet hacker or simple human error, as indicated by Kaiser Permanente's record. Abuse of HealthVault's and Google Health's users' medical records could also easily result from an internet hacker or simple human error, as indicated by Kaiser Permanente's record. Anytime individuals put personal information on the internet, the individuals run the risk that a third party may access the information even when the individual never intended to allow that third party access to the information. Neither HealthVault nor Google Health warns of this possibility.

HealthVault and Google Health should obtain their users' informed consent before allowing their users to post health records onto the internet because the Health Insurance Portability and Accountability Act (“HIPAA”) does not apply to HealthVault's and Google Health's services. HIPAA standardized confidentiality and security of medical data, requiring that only authorized individuals have access to patient health records, with a further restriction that only allows authorized individuals access to the patient health records they need. Within HIPAA, the Security Rule established a national standard for keeping electronic health records confidential. It is a common misconception that HIPAA acts as an all-encompassing rule to protect an individual's privacy rights when it comes to health

425. Id.

427. See supra notes 111-26 and accompanying text.
429. See supra notes 144-146 and accompanying text.
431. 3 SUSAN GODSTONE, TREATISE ON HEALTH CARE LAW § 13.01[1][B][iii] (Alexander M. Capron & Irwin M. Birnbaum eds., 2008).
records. Because of this misconception, many individuals assume that HIPAA applies to HealthVault and Google Health and therefore users’ private health records will be protected. Because HIPAA does not apply to HealthVault’s and Google Health’s services, HealthVault and Google Health should obtain informed consent from their users so that their users have a full understanding of HIPAA’s non-applicability to the programs.

While HealthVault is directly profiting from its users’ health related searches, HealthVault has failed to adequately protect its users’ private health records. HealthVault and Google Health should obtain informed consent from its users before allowing its users to post the users’ health records onto the internet because this would educate users on the policies of each site, the federal law, and the potential consequences of joining their programs. Similar to education law, HealthVault’s and Google Health’s requirements for informed consent should require that the users receive all the necessary information related to the consent in the users’ native language. A HealthVault or Google Health user needs to understand and agree to what the user is consenting in writing. Finally, HealthVault’s and Google Health’s users’ consent must be voluntary and the users should be able to reserve the right to revoke their consent at anytime. It is the responsibility of HealthVault and Google Health to protect the interests of their users, and the first step is educating the users. Until HealthVault and Google Health take the first step, they will truly never be a trusted provider, nor will they be committed to protecting an individual’s privacy. The revolution Hippocrates lead in protecting patient’s privacy rights remains inadequately addressed by HealthVault and Google Health, an aspect so important that the Father of Medicine would roll over in his grave.

Kathleen E. Prasse — ’09

432. See supra notes 236-416 and accompanying text.
433. See supra notes 236-416 and accompanying text.
434. See supra notes 236-416 and accompanying text.
435. See supra notes 236-416 and accompanying text.
436. See 34 C.F.R. § 300.9(a) (2008) (stating a parent must be fully informed about the necessary information pertaining to the activity that requires the consent). See supra notes 236-416 and accompanying text.
437. See § 300.9(b) (stating parents must agree in writing they understand and agree to carry out the consented activity).
438. See § 300.9(c)(1) (stating consent is voluntary and revocable at any time).
439. See supra notes 236-416 and accompanying text.
440. See supra notes 236-416 and accompanying text.
441. See supra notes 128-416 and accompanying text.