Cloudy Confidentiality: Clinical and Legal Implications of Cloud Computing in Health Care

Carolina A. Klein, MD

The Internet has grown into a world of its own, and its ethereal space now offers capabilities that could aid physicians in their duties in numerous ways. In recent years software functions have moved from the individual's local hardware to a central server that operates from a remote location. This centralization is called cloud computing. Privacy laws that speak to the protection of patient confidentiality are complex and often difficult to understand in the context of an ever-growing cloud-based technology. This article is a review of the legal background of protected health records, as well as cloud technology and physician applications. An attempt is made to integrate both concepts and examine Health Insurance Portability and Accountability Act (HIPAA) compliance for each of the examples discussed. The legal regulations that may inform care and standards of practice are reviewed, and the difficulties that arise in assessment and monitoring of the current situation are analyzed. For forensic psychiatrists who may be asked to provide expert opinions regarding malpractice situations pertaining to confidentiality standards, it is important to become acquainted with the new digital language from which these questions may arise.

J Am Acad Psychiatry Law 39:571–8, 2011

Many people remember playing the telephone game with friends when they were younger. The basic premise of the game is that one person whispers a secret into another's ear, and that person whispers it to another. As that process is repeated from person to person, large distortions emerge from cumulative small errors as the information is passed along. As health care professionals, physicians know that ensuring the accuracy of confidential information in a collaborative setting involves more technical approaches, to avoid a telephone game outcome. Information is recorded on secured systems, backups, hard drives, flash drives, shared folders, professional networks—the list can go on endlessly. Just as information management in the digital era was finally getting worked out in legislation and practice, a new modality appeared, one that physicians may be ill-prepared to accommodate. Cloud computing is the term used for the concept of operating from a remote server, without information or executable files in the physical hardware that is being manipulated by the user. Software for virtually all purposes is moving toward this approach, as it offers many advantages from the perspectives of accessibility, maintenance, and cost. A comprehensive discussion of the advantages and disadvantages of cloud computing extends beyond the purposes of this article.

This article is a review of privacy rulings as technology moves toward web-based applications and storage. Included is a review of the clinical, legal, and ethics-related implications of these changes. Cloud computing has been widely available for several years, yet the literature speaks scantily if at all about its impact on the practice of medicine. Concrete application of current confidentiality safeguards may prove insufficient to meet the standards of care or to allow for effective use of the advantages that the cloud has to offer.

The government has long recognized the importance of regulating the privacy and security of electronic personal records. The development of standards to ensure privacy has progressed over the decades. The United States Department of Health and Human Services has published a summary of legislation that has been implemented for this purpose in a clear, tabular format that is available on

Dr. Klein is Forensic Psychiatrist, Saint Elizabeths Hospital, Department of Mental Health, Washington, DC. Address correspondence to: Carolina A. Klein, MD, 3850 Elmwood Towne Way, Alexandria, VA 22303. E-mail: carolina.klein@gmail.com.

Disclosures of financial or other potential conflicts of interest: None.

their website.[1] Perhaps most known to physicians is the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[2] which set forth standards and general requirements for protecting health information at a time in which information processing was becoming more digitalized, and electronic information systems were being used for the purposes of managing clinical functions and providing health care services. Clinical applications included physician orders, electronic health records (EHR), radiology services, laboratory services, and pharmacy systems. HIPAA included the Privacy Rule[3] and the Security Rule,[4] the latter pertaining to the security standards for protecting health information that is held or transferred in electronic form. A proposed security rule was published in 1998 and revised after receiving numerous public comments. Its final version was published on February 20, 2003. It addresses technical and nontechnical safeguards for responsible (covered) entities to use in securing the electronic protected health information (e-PHI) of the individual. The Privacy Rule governs how entities may use or disclose e-PHI for the purposes of treatment, payment of health care, health care operations, research, and public health.[5] It also grants individuals rights over their health information. The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) enforces these rules through voluntary compliance activities and civil financial penalties.[1]

A brief review of a few definitions may be useful here. Covered entities include health care providers and health management plans that transmit information in electronic form for the purposes of certain standard transactions, such as analysis of patient safety and health care claims.[6] A protected health record (PHR) is an electronic record of an individual's health information by which the individual controls access to the information and may have the ability to manage, track, and participate in his or her own health care. An electronic health record (EHR), on the other hand, is held and maintained by a health care provider and may contain, in electronic form, all the information that once existed in a patient's paper chart.[7] The HIPAA Privacy Rule does not apply to PHRs unless they are offered or accessed by a covered entity.

In December 2008, the Secretary of HHS stated:

> Consumers need an easy-to-read, standard notice about how their personal health information is protected, confidence that those who misuse information will be held accountable, and the ability to choose the degree to which they want to participate in information sharing. . . . Over time, consumer confidence in the handling of health information is likely to grow just as consumer confidence in online banking has grown, but that won't happen without similar protections and transparency about the use of their information [Ref. 8].

The Secretary noted eight principles that should govern the legislation and implementation of such standards: individual access; correction; openness and transparency; individual choice; collection, use, and disclosure limitations; data integrity (data should not be destroyed or altered in an unauthorized manner); safeguards; and accountability.

This article will focus on the Security Rule, as it pertains to the particulars of digital pitfalls. The general principles of the rule include that a covered entity must maintain "reasonable and appropriate" administrative, technical, and physical safeguards to protect e-PHI, which include requirements to ensure confidentiality, integrity, and availability of information; anticipation and protection against possible threats to the privacy of the information or against inappropriate use; and compliance by the entity's workforce. The determination of what is "reasonable and appropriate" depends on the entity's particular risk, security, and financial situations.[9]

All covered entities must have been in compliance with the Security Rule no later than April 20, 2005. To achieve compliance, the Privacy and Security Toolkit[10] implements the principles in The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information (privacy and security framework). The safeguards of the toolkit include the three areas with requirements shown in Table 1.

The standards[11] set forth by HIPAA speak to identifiable patient information.[12] De-identification requires the elimination of primary (name, date of birth, treating provider, and medical record number) and secondary (those from which the patient's identity can be deduced) identifiers. In order for information to be de-identified, 18 elements of identification must be removed (Table 2).

De-identified information should be preferred whenever possible for matters of utilization review, monitoring, and research. Providing such anonymity, however, may be difficult, especially when trying to disseminate the practice to a broader scope of users.[13] An authorized user who wishes to encrypt PHI when creating de-identified information must ensure

Table 1 Privacy and Security Toolkit[10]

Administrative
Routine risk analysis of systems and personnel involved in their processes
Security personnel and a designated security officer
Implementation of policies and procedures for authorizing role-based access to information
Authorization, training, and supervision of workforce members, and application of appropriate sanctions should those procedures be violated
Periodic assessment and evaluation of meeting of standards
Physical
Limited and differentiated facility access and control
Development of policies and procedures regarding workstation and device security, including transfer, removal, disposal, and reuse of electronic media containing e-PHI
Technical
Development of policies and procedures to control access to e-PHI, and to ensure the integrity of e-PHIs
Implementation of hardware, software, and/or procedural mechanisms to record and examine activities of e-PHI
Implementation of technical security measures that guard against unauthorized access to e-PHI while being transmitted over an electronic network

that the code or other means of record identification is not derived from or related to information about the individual that it is not otherwise able to be translated so as to identify the individual and that anyone involved does not use or disclose the code or other means of record identification and does not disclose the mechanism used for re-identification.

The scientific literature speaks briefly[14] about the impact of legal regulations on the use and manipulation of clinical information. The legal regulations may have shortcomings, as digitalized manipulation of data grows in scope and dissemination, ultimately resulting in decreased protection of privacy.

Discussion

The Conflict

The relevance of ensuring protection of e-PHI stands on its own as a way of guaranteeing basic rights of privacy for each individual. It also promotes continuity of care; effective collaboration among providers, with decreased redundancy and cost of workups; and development of a nationwide health system that can be accessible, regardless of the patient's location. While breaches of compliance may occur, ensuring privacy in the digital era appears to be more error proof than securing its predecessor, the paper record.[15]

Cloud-based computing presents itself as a modality that offers increased access to data regardless of patient or provider location. It offers efficient technical management through a centralized system that regularly updates and monitors functioning of software. Furthermore, it reduces the risk of unauthorized tampering by drastically reducing the number of devices containing critical software or information that can be tampered with. It may also offer reduced costs, although this is an area of ongoing debate. Many services are available free, steep purchase prices are eliminated, and service costs are reduced. However, a required monthly fee for those services may prove more costly in the long run. On the other hand, cloud computing poses some conflict, in that the server itself cannot be monitored by a security-trained officer of the covered entity. Finally, while the conditions for technical safeguards may be agreed on at the moment of contracting with the cloud service, the service providers ultimately hold the right to change their safety standards in the future. Examples of these may include degree of safety of password requirement, level of encryption, and collaboration features.

The discussion acquires another layer of complexity when certain sociopolitical views are taken into account. Multiple businesses based on HIPAA compliance have arisen to assist institutions or providers,

Table 2 Identifiable Patient Information

Names
All geographic subdivisions smaller than a state (street address, city, county, precinct, Zip code, and their equivalent geocodes, with some exceptions)
All elements of dates (except year) for dates directly related to an individual (birth date, admission date, discharge date, date of death)
Telephone numbers
Fax numbers
Electronic mail addresses
Social security numbers
Medical record numbers
Health plan beneficiary numbers
Account numbers
Certificate/license numbers
Vehicle identifiers, including license plate numbers
Device identifiers and serial numbers
Web universal resource locator (URLs)
Internet Protocol (IP) address numbers
Biometric identifiers, including finger and voice prints
Full-face photographic images and any comparable images
Any other unique identifying number, characteristic, or code

given the ever-increasing complexities of the law.[16] These services can be costly, often much more so than web-based services, which exposes the contradiction of HIPAA's aiming to reduce costs of health care while triggering staggering expenses for compliance.[17] Especially for the small practice covered entities, moving forward in record management in the digital age while satisfying compliance regulations may prove to be inefficient or outright impossible to achieve.[18] There are financial incentives,[19] but the upfront investment could be insurmountable for many entities. Furthermore, the commercial interest of HIPAA compliance-based businesses introduces a bias that raises the question of whether improved patient care is the priority. Finally, consideration must be given to the argument of who should ultimately decide on the scope and method of access: the patient, the practitioner, or the government. Some advocate for it to be the patient, as it would increase patient empowerment and decrease governmental involvement.[20] Others believe that the practitioners are best for assessing the needs of their particular practice. Advocates of legislative decision-making emphasize the need for federal regulations to prevent individual indiscretions.

From Concepts to Consoles: Applications and the Applicability of the Law

The security standards were designed to be technology-neutral, to accommodate changes that arise in technological developments. They also allow for certain flexibility in consideration of the fact that needs may differ from one institution to the next, from one software program to the next, or from one software program to its newer version. HIPAA does not certify software as compliant or noncompliant, and it is therefore up to the institution to ensure that the requirements are met. In cloud computing, the software is dynamic, and monitoring of functionality or security parameters occurs far removed from the covered entity.

When Does the Cloud Rain on Us?

Here are some examples of how ubiquitous this conflict may be in all areas of medical practice and management. It must be taken into account that most practitioners own more than one computer, and increasingly, more work is being completed from home.[21] We physicians have long moved past discussing the potential security threats of using portable pen drives to facilitate continuation of work or ensure accessibility of information at a remote location—for example, while in transit to and from work. The cloud offers a solution to almost any problem a practitioner may encounter. Here are some examples:

Document management. GoogleDocs is a cloud-based system for management of text documents, spreadsheets, surveys, and more. It is available free of charge, is accessible from any computer and from many smartphones, and allows for sharing and collaboration. As with any cloud-based service, once information is submitted (even if deleted later by the owner), it is replicated and stored in the cloud server. The copy stored in their server is beyond the control of the user. The cloud service claims that data are used solely for the purposes of automated statistics. Once data are stored, they are dispersed in a proprietary fashion through the web server and cannot be reconstructed unless the private service's algorithm is known. The biggest obstacle remains its lack of hierarchy and the fact that levels of hierarchy cannot be accomplished, except through selective sharing of data.[22]

Storage. Dropbox stores information in an individual folder on a web server and automatically synchronizes the information in that folder with any computer or smartphone in which Dropbox is installed. It is offered free, with an option to increase storage space for a fee or through referrals. It allows for sharing of folders. Information is available from the Dropbox website or directly from the updated folder in the computer or device where it has been installed. Dropbox is password protected, but password requirements are not specified. The password does not have to be periodically updated, and the website does not offer information on the level of encryption the server uses. However, differential access is achieved, as individuals only have access to their own information or that specifically shared with them by another user.

Collaboration tools. GQueues is a project management tool offered by Google that allows for task management and differential assignments among workforce members. It automatically synchronizes with e-mail and calendar services and has reminder functions that can be received on any computer or smartphone. Its security specifications are almost identical with those for GoogleDocs. HIPAA

promotes collaboration among practitioners and even across states, through the Health Information Security and Privacy Collaboration (HISPC), which now comprises 42 states, but cloud-based services have not been considered as a means of achieving that collaboration.[23]

Databases. Grubba is a cloud database that can be built easily by any user at no cost. Security is limited to password-protected entry into the website, which does not have specific requirements or scheduled updates. No information is available on the website regarding encryption.

Patient management. Samedi offers a network-based system for management of workflow, medical appointments, and transmittal. It emphasizes a collaborative relationship between doctors and patients, with benefits for both. It is available for a fee, and it is approved in its country of origin, Germany, for use across institutions. Medicine Brain offers a cloud-based, comprehensive electronic medical record (EMR) system that uses some Google parameters while ensuring privacy standards.

Billing. BillingBoss and Billing Manager both offer free cloud-based billing services. Invoices are stored in the server and are accessible through a password protected site or through a smartphone.

Webhosting. LuxSci is a cloud-based management system for e-mail transmittal and website hosting. The website states that the service is HIPAA compliant and is protected against threats by well-known systems such as McAfee and Truste. The service is available for a fee, although the fee schedule is flexible according to the provider's need.

Communication. E-mail protection can be achieved in different ways. As Microsoft Outlook moves to a cloud-based operation, other cloud-based services must also be considered. The use of Gmail or Yahoo global servers as e-mail hosts has been advised against because of the potential for breaches. However, compliance with HIPAA would require only the lack of identifiable information, an e-mail notice or disclosure of confidentiality, and informed consent.[24] Furthermore, with services such as Google Voice, voicemails are transcribed and sent via e-mail or text message to the provider's computer or cell phone device. The current standards do not speak to situations in which the security level cannot be accurately measured. Doximity offers a private physicians' network service that facilitates locating other health care professionals and health institutions and offers HIPAA-compliant text messaging among physicians.

Teleconferencing. Skype is a teleconferencing (voice-over Internet protocol) service that is free of charge and allows international phone calls for a fee. It is cloud based and can be accessed directly through the website or by installing the application in the user's computer or cell phone. Users are required to set up a user name and a secure password. It uses the same encryption as banks do. Because of its video capabilities, hacker impersonators could easily be identified through video. Malware has been designed that masquerades as Skype and prompts for password disclosure; however, such scams have occurred with many reputable services and software programs, including those of banks. Skype proposes itself as a viable option for telepsychiatry.

Outsourcing of medical services. Half of the medical transcription and data processing of the United States, estimated at $20 billion, is outsourced. These offshore processors are considered business associates of HIPAA-covered entities. Transmission of data or monitoring of the offshore security parameters may not be optimal. Furthermore, an assumption could be made that offshore HIPAA business associates are cloud based, and therefore, HIPAA may be indirectly supporting cloud computing.[25]

Cell phones and cell phone applications (*Apps*). Many cloud-based services are available on portable devices such as cell phones, netbooks, and e-readers, among others. These services allow for continuity of care, prompt response to patients' needs, coordinated access to updated information, ubiquitous access to information, and automatized backups for protection of information. Cell phone security systems, including encryption options, are different from computer-based applications and browsers, and currently available safeguards do not incorporate such technologies into consideration of standards.

Legal Implications

It is pertinent to review the legal impact of standards on every day clinical practice.

Consequences of HIPAA noncompliance. HIPAA is a federal law, and violations are therefore tried in federal courts. Statutory damages can also be applied. All violations are considered felonies, and the person tried is the person considered to have breached

security or leaked information inappropriately. According to § 1177 of HIPAA, a person is in violation of HIPAA regulations who knowingly uses a unique health identifier or causes one to be used, obtains individually identifiable health information relating to an individual, or discloses individually identifiable health information to another person. Such persons are subject to the following penalties: a fine of up to $50,000, or up to 1 year in prison, or both (Class 6 felony); if the offense is committed under false pretenses, a fine of up to $100,000, or up to 5 years in prison, or both (Class 5 felony); or if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of up to $250,000, or up to 10 years in prison, or both (Class 4 felony). HHS can also impart civil penalties for HIPAA violations on a tiered scale on any person who participates in such a violation. For a person who was unaware of compliance requirements, the maximum is $100 for each violation, with the total amount not to exceed $250,000 for all violations of an identical requirement or prohibition during a calendar year (Class 3 felony). For persons who willfully neglect to comply with HIPAA, penalties range from $10,000 to $50,000 per violation up to $1.5 million per calendar year for an identical violation, if corrective action is not taken.

Court cases. Case precedents have been argued on the basis of the right to privacy derived from the Fourth Amendment. In the case of *Goldman v. United States*,[26] electronic surveillance without physical penetration of the premises by a tangible object was deemed not to violate constitutional protections. However, this decision was overruled in the case of *Katz v. United States*.[27] Justice Harlan famously wrote, "privacy may be defeated by electronic as well as physical invasion." In *Kyllo v. United States*,[28] the Supreme Court ruled that law enforcement's use of thermal imaging technology to view the interior of a residence was impermissible.[23] Pertinent to HIPAA violations specifically, in *Acosta v. Byrum*,[29] the appellate court stated that a HIPAA violation constitutes negligence *per se* and awarded accordingly to the plaintiff. Numerous cases have followed suit, rendering it impossible to cite them comprehensively in this article. As recently as June 2010, in *Connecticut v. Health Net, Inc.*,[30] a settlement of $250,000 was reached for what was considered a HIPAA violation under the HITECH (Health Information Technology for Economic and Clinical Health) Act of 2009.

What to Do

The literature has shown that fear of HIPAA violations has negative affects on patient care.[31] I propose a series of measures that a clinician can take to prevent such negative effects on patient care or legal breaches.

Government tools. Ensure administrative, physical, and technical safeguards, as provided by HIPAA (briefly described above). HIPAA also provides interstate collaboration tools (see above). Federal tools have also been developed in an effort to assist entities in the understanding and implementation of appropriate privacy safeguards and are readily available for download through the Internet.[32]

Mitigation. In the event that a security breach or data loss occurs involving e-PHI, HIPAA requires that specific steps be taken to address such an incident and that actions be documented.

De-identification. Some institutions offer a de-identification method that is compliant with HIPAA regulations.[33] Re-identification with a randomly assigned identifier devoid of all 18 HIPAA-stipulated identifiers (Table 2) is easily accomplished through available software such as Vicare.[34]

Informed consent. Ultimately, patients' awareness of and consent for how their health information will be kept, accessed, transferred, or protected are pivotal aspects that can determine to a large extent the choice of service utilized. Obtaining informed consent may also be a legal protection in the event of a subsequent lawsuit.

IT counsel. HIPAA compliance businesses have arisen and provide service to medical practices to assist with compliance regulation according to the particular needs of the institution. There is some literature[35] regarding software selection as it pertains specifically to psychiatry that may orient a provider seeking digital directives while remaining HIPAA compliant.

Conclusions

Communication within an institution, as it extends among coworkers, trainees, and other members of the treatment team, or among patients directly, is not just inevitable, but desired in favor of

optimizing patient care. The technology available to practitioners during this digitalized era should be utilized to its full extent if it serves the purposes of furthering education and patient care. Unfortunately, useful tools are often neglected or discarded due to a perceived threat of litigation that stems from a law that originated from a common goal: to further patient care as health information moves into an electronic format. While compliance with HIPAA is crucial, technology appears to be growing faster than the legislation that covers it, leaving certain legal aspects unresolved. There are several solutions to this conundrum. We have mentioned a few in this article, but on a broader level, there are projects under way, such as the Hippocratic Database,[36] which attempt to bring patient care, HIPAA, and the cloud together. In the meantime, physicians should become versed on the concept of cloud computing and how it may clinically and legally affect their practices.

References

1. Summary of Selected Federal Laws and Regulations Addressing Confidentiality, Privacy and Security. Available at http://www.google.com/url?sa=t&source=web&cd=1&ved=0CCUQFjAA&url=http%3A%2F%2Fhealthit.hhs.gov%2Fportal%2Fserver.pt%2Fgateway%2FPTARGS_0_11113_911059_0_0_18%2FFederal%2520Privacy%2520Laws%2520Table%25202%252026%252010%2520Final.pdf&rct=j&q=summary%20of%20selected%20federal%20laws%20and%20regulations%20addressing%20confidentiality%20privacy%20and%20security&ei=Vjd2TseNMTIsQLQ_YiMBQ&usg=AFQjCNHKb0_zqpjEY4_aP3D2xjj4gPPDKQ&sig2=6fMD5C3Kz_5GIDsOnNE_cw. Accessed September 18, 2011
2. Health Information Privacy. Available at http://www.hhs.gov/ocr/privacy. Accessed November 29, 2010
3. National Institute of Standards and Technology U.S. Department of Commerce. An introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Information Security. Available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist80066.pdf. Accessed November 29, 2010
4. Summary of the HIPAA Security Rule. Available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html. Accessed November 29, 2010
5. 45 C.F.R. § 164.506, 510, 512, 514(e) (2002)
6. 45 C.F.R. § 160.103 (2002)
7. Office for Civil Rights. Personal Health Records and the HIPAA Privacy Rule. Washington, DC: Department of Health and Human Services. Available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html. Accessed October 19, 2011
8. Secretary Leavitt announces new principles, tools to protect privacy, encourage more effective use of patient information to improve care, December 15, 2008. Available at http://www.hhs.gov/news/press/2008pres/12/20081215a.html. Accessed October 19, 2011
9. U.S. Department of Health and Human Services. Health Information Privacy Summary of the HIPAA Security Rule. Available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html. Accessed October 19, 2011
10. The Health IT Privacy and Security Toolkit. Available at http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov_privacy_security_framework/1173. Accessed September 16, 2011
11. Security Standards: Technical Safeguards. Available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf. Accessed November 29, 2010
12. Mendelson D: Healthcare identifiers legislation: a whiff of fourberie. J Law Med 17:660–76, 2010
13. El Emam K, Jabbouri S, Sams S, *et al*: Evaluating common de-identification heuristics for personal health information. J Med Internet Res 8:e28, 2006
14. Walsh D, Passerini K, Varshney U, *et al*: Safeguarding patient privacy in electronic healthcare in the USA: the legal view. Int J Electron Healthc 4:311–26, 2008
15. Myers J, Frieden TR, Bherwani KM, *et al*: Ethics in public health research: privacy and public health at risk: public health confidentiality in the digital age. Am J Public Health 98:793–801, 2008
16. Dougherty M, Washington L: Still seeking the legal EHR: the push for electronic records increases, the record management questions remain. J AHIMA 81:42–5, 2010
17. Edlin M, Johns S: High standards: a decade after the law went into effect, there is still debate about the pros and cons of the HIPAA privacy and electronic transaction regulations. AHIP Cover 47:26–9, 2006
18. Fontaine P, Zink T, Boyle RG, *et al*: Health information exchange: participation by Minnesota primary care practices. Arch Intern Med 170:622–9, 2010
19. May M: Focus on electronic health records. 'HIPAA2' legislation means more delicate handling of data. Nat Med 16:250, 2010
20. Falcao-Reis F, Costa-Pereira A, Correia ME: Access and privacy rights using web security standards to increase patient empowerment. Stud Health Technol Inform 137:275–85, 2008
21. Nine Smartphone Apps. Available at http://www.medscape.com/viewarticle/729536. Accessed November 29, 2010
22. Official Google response about HIPAA. Available at http://www.google.com/intl/en-US/health/hipaa.html. Accessed November 29, 2010
23. The Office of the National Coordinator for Health Information technology. Available at http://healthit.hhs.gov/portal/server.pt?open=512&objID=1175&parentname=CommunityPage&parentid=10&mode=2&in_hi_userid=10732&cached=true. Accessed November 29, 2010
24. Guidance on the use of email containing PHI. Available at http://hipaa.yale.edu/guidance/index.html. Accessed October 19, 2011
25. Perry N, Chester T: To HIPAA, a son: assessing the technical, conceptual, and legal frameworks for patient safety information, in Regulating for Patient Safety: The Law's Response to Medical Errors. Widener Law Rev 12:134, 2006
26. Goldman v. United States, 316 U.S. 129 (1942)
27. Katz v. United States, 389 U.S. 347 (1967)
28. Kyllo v. United States, 533 U.S. 27 (2001)
29. Acosta v. Byrum, 638 S.E.2d 246 (N.C. Ct. App. 2006)
30. Connecticut v. Health Net, Inc., 383 F.3d 1258 (11th Cir. 2004)
31. Touchet B, Drummond S, Yates WR: The impact of fear of HIPAA violation on patient care. Psychiatr Serv 55:575–6, 2004
32. Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices. Washington, DC: U.S. Department of Health and Human Services. Undated. Available at http://www.google.com/url?sa=t&source=web&cd=1&ved=

0CBYQFjAA&url=http%3A%2F%2Fhealthit.hhs.gov%2Fportal%2Fserver.pt%2Fgateway%2FPTARGS_0_10731_848086_0_0_18%2FSmallPracticeSecurityGuide-1.pdf&ei=LNb7TOeWI8Wclgfkvfy LBQ&usg=AFQjCNGeum6QplgMF7F5X1VBgeZWJ-s6Hw&sig2=hcC-zn2Guc_K4X68VM_WeQ. Accessed November 29, 2010

33. HIPAA Procedure 5039. De-identification and limited data set procedures. Available at http://www.yale.edu/ppdev/Procedures/hipaa/5039/5039PR1.pdf. Accessed November 29, 2010
34. Vicare. Available at http://www.openmedsoftware.org/wiki/8._HIPAA_de-identification. Accessed November 29, 2010
35. Houston M: The psychiatric medical record, HIPAA, and the use of electronic medical records. Child Adolesc Psychiatr Clin N Am 19:107–14, 2010
36. Agrawal R, Johnson C: Securing electronic health records without impeding the flow of information. Int J Med Inform 76:471–9, 2007