Balancing between two goods: Health Insurance Portability and Accountability Act and ethical compliancy considerations for privacy-sensitive materials in health sciences archival and historical special collections

Judith A. Wiener, MLIS; Anne T. Gilliland, JD

See end of article for authors' affiliations.

DOI: 10.3163/1536-5050.99.1.005

Objective: The investigation provides recommendations for establishing institutional collection guidelines and policies that protect the integrity of the historical record, while upholding the privacy and confidentiality of those who are protected by Health Insurance Portability and Accountability Act (HIPAA) or professional ethical standards.

Methods: The authors completed a systematic historical investigation of the concepts of collection integrity, privacy, and confidentiality in the formal and informal legal and professional ethics literature and applied these standards to create best practices for institutional policies in these areas.

Results: Through an in-depth examination of the historical concepts of privacy and confidentiality in the legal and professional ethics literature, the authors were able to create recommendations that would allow institutions to provide access to important, yet sensitive, materials, while complying with the standards set by HIPAA regulations and professional ethical expectations.

Conclusion: With thoughtful planning, it is possible to balance the integrity of and access to the historical record of sensitive documents, while supporting the privacy protections of HIPAA and professional ethical standards. Although it is theorized that collection development polices of institutions have changed due to HIPAA legislation, additional research is suggested to see how various legal interpretations have affected the integrity of the historical record in actuality.

INTRODUCTION

Special collections professionals in institutions with health sciences history collections balance on a legal and ethical tightrope of preserving and providing access to the historical record, while at the same time respecting the confidences of those whose lives are reflected in the records. Although a great deal of information is available on the topics of privacy and the ethical responsibility of the archivist to the historical record, there is little formal information on how to reconcile these two distinct professional responsibilities when providing access to collections. These issues and responsibilities can come up for any librarian in a health sciences setting, such as a hospital librarian who is given or acquires old medical records. This article is a synthesis of the information available on these two subjects with the goal of making recommendations that balance protecting the future historical record and collection integrity with guarding the privacy of those who are protected by the Health Information Portability and Accountability Act (HIPAA).

The analysis and recommendations presented here are based on a review of the ethical, legal, and professional literature as well as the experience of the authors. The formal historical, legal, ethical, and archival literature on the requirements of HIPAA, related privacy and confidentiality laws, and privacy norms of professional ethical codes were surveyed. Many of these sources are listed in the Science, Technology, and Healthcare Roundtable of the Society of American Archivists and the Archivists and Librarians in the History of the Health Sciences online resource guide [1]. A number of institutions have placed their HIPAA-related policies online, and these

Highlights

- Ethical standards call upon special collections professionals to collect and provide access openly, while protecting individual privacy.
- A systematic historical investigation of legal and professional ethics literature can lead to standard best practices that address issues of privacy and access.

Implications

- Special collections professionals can establish guidelines that preserve the historical record and maintain collection integrity and access, while adhering to privacy legislation and ethical concerns.
- The framework suggested here can be used to write a collection development and access policy that complies with the Health Insurance Portability and Accountability Act.
- Librarians who interact regularly with hospital administrators or researchers using patient data need to be aware of the ethical and legal issues involved in patient data retention.

were consulted as well. The authors also found the policies of the Alan Mason Chesney Medical Archives of the Johns Hopkins Medical Institutions [2] and of the Augustus C. Long Health Sciences Library Archives and Special Collections of Columbia University helpful [3]. From this survey, it became apparent that there are both legal and ethical issues that must be considered in developing collection policies in this arena.

LEGAL CONSIDERATIONS

The evolution of the law of confidentiality and privacy mirrors the changes in the way society has come to think about these issues over time. Technological innovations have provided the impetus for many of these changes in thinking. A brief review of the development of law in this area and the basic requirements of HIPAA shows the context in which the special collections professional who manages an historic medical collection must work today.

Although the terms ''confidentiality'' and ''privacy'' are often used inexactly or interchangeably, they are not equivalent, as it is possible to keep information private while still breaching confidentiality [4]. For example, a physician who discusses a patient's illness with family members or close friends may have kept the information from the public eye but may still have breached the patient's confidence. Traditionally, the physician's code of ethics, not the common law or statute, governed the sanctity of the communications between patient and doctor [5]. If a patient resorted to law to redress a physician's breach of duty, the patient brought the suit as a tort, a civil action brought by an individual, not by the state. Prior to 1890, the law of confidence predicated such actions, not the law of privacy. Under this legal theory, a plaintiff suffers an injury when a trusted relationship, such as that between a physician and a patient, is damaged by the betrayal of a confidence [6].

Thinking about the legal basis of the confidentiality and privacy in the United States began to change in 1890 when Warren and Brandeis published ''The Right to Privacy'' in the *Harvard Law Review.* They argued that the law should protect not only the confidential relationships between people, but also prevent disclosure of information to the wider public [7]. One of their reasons for this conclusion was that the law of confidence did not provide enough protection in a world where technological advances allowed a photographer to take a picture and publish it without the subject's knowledge or consent [8]. The law should not only protect close relationships, but also protect people ''as against the world'' [9].

The law of privacy developed quickly in the United States after Warren and Brandeis published their article, with most states adopting the theory through case law or statutes [10]. In 1960, Prosser, the leading torts authority of his day, defined four privacy torts, all of them predicated on the theory of the right ''to be let alone'': public exposure of private facts, false light, misappropriation of name and likeness, and intrusion upon the plaintiff's seclusion or solitude or into an individual's private affairs [11]. Today, privacy law has developed substantially in the United States, and it is not only a tort concept, but also a legal right that underpins much of US jurisprudence [12].

During the same period, the tort law of confidence in the United States developed more slowly. Eventually, most states recognized a tort cause of action for breach of confidence, often in the context of medical care. Two cases from Ohio, *Hammonds v. Aetna Insurance* in 1965 and *Biddle v. Warren General Hospital* in 1999, illustrate the gradual recognition of this concept, which started with the ethical duty of a physician, then moved to the privilege of the patient's communications to a physician during court proceedings, and finally encompassed both the physician's tort liability for breaking a patient's confidentiality and the liability of a third party who induced the physician's disclosure [13, 14]. Today, the HIPAA Privacy Rule preempts much of state law for breach of confidence and for breach of privacy in the health arena, but both remain valid causes of action against entities not covered by HIPAA, where state law protection is greater than HIPAA's provisions, or for private redress [15].

HIPAA aims to cover both the confidentiality and privacy of health information [16]. Congress passed the law in 1996 amidst concerns about technology's impact in both areas. The new law had two intentions. The first was to facilitate the electronic exchange of health information by quieting concerns over privacy and confidentiality. The second was to provide more security for health information when workers changed jobs and faced the possibility of being denied health insurance coverage in the new workplace because of preexisting conditions. The Secretary of Health and Human Services (HHS) was charged with issuing the administrative regulations in this area through the privacy rule and setting the penalties for noncompliance [17].

The privacy rule applies to three types of organizations: health plans, health care clearinghouses, and health care providers that transmit ''health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA'' [18, 19]. Health plans are defined in the US Code and the Code of Federal Regulations and include most entities that pay for or provide for health care [20, 21]. Health care clearinghouses are defined as organizations that receive and process health information [22]. Health care providers include all entities that provide health services [23, 24]. Health care providers must also transmit ''health information in electronic form in connection with a [covered] transaction'' in order to be covered entities [18].

The privacy rule places no time limit on the bounds of confidentiality or privacy for the records that it covers, with the rationale that concerns about hereditary diseases and genetic risks might continue after the subjects' deaths. This creates significant concerns and challenges for special collections librarians and

archivists and for historical researchers who work with material subject to HIPAA's requirements [25]. In the past, archivists and special collections librarians have often used rules of thumb, such as ''grandfather'' clauses, for controlling access to sensitive material, but if information is subject to the privacy rule, these thresholds are no longer adequate. At this writing, proposed revisions to HIPAA that have been put forward for public comment would relax HIPAA's restrictions after decedents have been dead for fifty years. Although this loosening of regulations would facilitate historical research, it would not relieve the special collections professional of the burden to provide a policy for access [26]. In many cases, it is not easy to determine when a subject died, and so considerable thought and consultation would still be necessary in order to fulfill HIPAA's legal requirements, even if the proposed rules become law.

The first issue in deciding how to handle HIPAA compliance for historical collections is to learn the institution's designation. For HIPAA purposes, there are three types of entities: covered entities, non-covered entities, and hybrid entities. The Department of HHS has a decision support tool that can be used to answer whether people, businesses, agencies, or programs are covered entities [27]. Only a covered entity, or the covered part of a hybrid entity, must comply with the privacy rule, although other federal or state privacy and confidentiality laws may apply to non-covered entities [28]. In cases where the institution's status has already been determined, that decision should be easily discovered, because covered entities and hybrid entities must provide notice of privacy practices [29], establish written privacy policies, train staff in those policies, and appoint a privacy officer [30, 31].

If an organization performs both covered and non-covered functions, it may elect to be a hybrid organization by designating the health care components in its operations as covered functions. Although the covered entity still has responsibility for the enforcement of the privacy rule, only the health care components must apply with most of the rule's provisions once the organization's hybrid status is established [32].

The privacy rule protects a subset of individually identifiable health information, which it calls ''protected health information'' (PHI). This information includes names; postal address other than town, city, state, or zip code; telephone numbers; fax numbers; email addresses; Social Security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate or license numbers; vehicle identifiers and serial numbers; device identifiers and serial numbers; uniform resource locators (URLs); Internet protocol (IP) addresses; biometric identifiers, such as fingerprints; and full-face photographic images and other similar images. All of this information must be stripped if information is to be freely shared [33]. The rule defines individually identifiable health information as ''information, including demographic information collected from an individual and is created by a [covered entity] and relates to the past, present, or future physical mental health of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual'' [18]. Further, individually identifiable health information either ''identifies the individual [or provides a] reasonable basis to believe the information can be used to identify the individual'' [19]. Within that definition of individually identifiable health information, the rule defines protected health information as that which is ''transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium'' [18].

A covered entity may not use or disclose protected health information except as either the privacy rule requires or allows or when the subject of the information (or that person's representative) authorizes the disclosure or use [34]. One of the situations where a covered entity may, but is not required to, disclose PHI is for research purposes [35, 36]. However, PHI is still subject to a number of restrictions when it is disclosed: In most cases, whether for research or in other situations, the covered entity must limit the use and disclosure of PHI to the minimum necessary, and it must develop guidelines and policies to keep use within those limits [37]. A covered entity may disclose and use PHI for research without the subjects' authorization if an institutional review board (IRB) or privacy board has approved a waiver of the authorization; if the researcher can attest that the use and disclosure of PHI is only for the preparation of a research protocol or similar activity; or if the researcher can attest that the research will only use the PHI of decedents, that the research is necessary, and that the researcher can provide documentation on the death of the subjects if it is requested [38].

Alternatively, a researcher may freely use a limited data set with a wide array of information redacted from the PHI [39]. This de-identified information can be used or disclosed without restrictions, but only if the covered entity has no ''actual knowledge that the remaining information could be used alone or in combination with other information to identify the individual who is the subject of the information'' [40]. As an alternative to de-identification, a researcher who wishes to use PHI may obtain an authorization from the subjects. An authorization must be specific to a particular research project; it may not allow a number of unspecified uses for future research [41].

When research cannot be conducted with de-identified PHI or when it is not feasible to obtain an authorization, a researcher may pursue a waiver or alteration of authorization from an IRB or a privacy board. An IRB may consider these waivers or alterations in addition to its other work overseeing research. Either one of these boards may approve a partial or complete waiver [42].

HIPAA applies to documents that covered entities held on April 14, 2003, when the privacy rule went into effect, or documents that were subsequently

acquired or created by these entities, and so it governs documents that are held by many, although not all, archives that collect historical medical records. For example, records of a hospital that closed in the nineteenth century would not be from a covered entity and neither would physician's notes from the same period. On the other hand, if a university that is a hybrid entity holds these records in an archive that has been designated as part of the health care component, then the documents would be governed by the privacy rule [43].

Because the privacy rule governs information, not documents, the privacy rule applies to all of the individually identifiable health information in an archival collection of historical medical material once that unit has been designated as a covered entity. At the same time, the privacy rule does not govern documents that are held by the same unit but that do not contain individually identifiable health information [44]. Often, archival material will fall into a gray area. Do old letters that contain sensitive health information fall under the privacy rule if a covered entity holds them [45]? What about older, medically oriented photographs showing people who can be positively identified? At the same time, a covered entity might hold other material, such as administrative minutes of a medical society, that does not contain PHI.

These decisions have ramifications for a variety of uses that both researchers and archives staff may make of material, and they govern when researchers must seek a waiver before using material. They may also have a bearing on what material an archive or special collection digitizes. Nothing in the privacy rule requires the destruction of historical material that contains PHI, but institutions may reconsider what material to retain or collect in light of its restrictions.

ETHICAL CONSIDERATIONS

Appraisal and acquisition decisions in special collection and archival environments are usually fraught with equal measures of archival theory and educated guessing. Determining what the historian or researcher of the future will find interesting, useful, and enlightening is no easy task. Saving everything is usually not an option due to factors unrelated to historical significance, such as space limitations, funding, and staffing. In addition to legal concerns, ethical standards also muddy the waters when acquiring, preserving, and providing access to materials containing confidential or private medical information. Examples of important archival records that may contain sensitive information include patient records, physician journals, accounting and record books, and research study files. In addition, many records once used freely by institutions and researchers, such as photographs and promotional brochures featuring patients, now fall under privacy legislation strictures. It would appear to be shortsighted to discard, reject, or destroy all documentation containing PHI, because it is entirely possible that the average document will outlast the enforcement of HIPAA and/or because the privacy demanded by today's individual may not seem so sacred in the future [46]. Because the original purpose or use of a record is rarely connected to its historical future use, archivists need to protect not only the privacy of those reflected in the records, but also to seriously consider the alternate uses of such information in the future [47].

Although collecting and sealing all important documents if and until HIPAA changes to meet the records management needs of special collections professionals is a possibility, it is impractical. A more practical approach is to focus on policies that support the traditional function and goals of collections in medical history. These functions have included documenting the discoveries in medicine and the health sciences, contributing to the discovery of knowledge in these fields, and ensuring the accountability of health care providers to the public by maintaining an historical record of their practices. Institutions have also had more specific goals, such as documenting the history of a particular region, institution, or profession [48].

A targeted collection policy that articulates why retaining certain records is essential to the collecting organization's mission can be a strong argument against an administrative preference for destroying records because of HIPAA concerns. An archivist or special collections librarian can use examples of older historical documents in the collection that contain PHI and important historical works that used such documents in order to demonstrate the importance of preserving this material.

As stated at the outset, the archivist or special collections librarian must balance the protection of the historical record with a commitment to protect the privacy of the individuals reflected in those historical materials. This is not a new responsibility, nor is it one that is limited only to those individuals who curate health sciences historical materials. Privacy considerations are one of the profession's institutionalized altruisms, formalized in codes of ethics and as a long-standing topic in the professional literature [49]. HIPAA did not set the expectation of privacy considerations in archival work but rather shaped it from outside the profession [50].

Policies governing access to the patient record have historically relied on trust and good intentions. Medical records have always contained personal information, and patients have historically trusted that physicians and other caregivers would use this information responsibly and in patients' best interests. Likewise, physicians and other record holders controlled access to this information in this atmosphere of trust long before the advent of HIPAA-mandated privacy policies. It was not the nature of the records themselves that led to the HIPAA Privacy Rule, but rather the advent of technology and the privacy breaches made possible by widespread access to digital record systems [51]. Concerns about the ease of transmission of information via technological

means, not a breakdown in the ethical system ensuring privacy of personal information, sparked the perceived need for legislation. The universal understanding of the good of protecting personal, and potentially damaging, information has traditionally existed in medical records [52].

As records pass to the historical side of significance and away from their original purpose, the trust to protect privacy likewise passes from the former record holder to the archivist [53]. Protecting the privacy of the subjects of records receives its own statement in the codes of ethics of major archival associations. Section VII of the Society of American Archivists' code specifically mentions privacy. It urges professionals to respect the privacy of the subject of records as well as those who use the records and notes the importance of following one's institutional security procedures [54]. Both the Association of Canadian Archivists and the International Council on Archives state that a special protection of privacy should be afforded to those with no voice in the use or disposition of their records or information [55, 56]. Certainly, this special category of privacy protection applies to health sciences historical records containing PHI, even when the HIPAA Privacy Rule does not apply.

Under the environment of new privacy expectations and legislation, repositories ''now routinely make terms and conditions of acquisition and use explicit in their donor policies, donor agreements, and in the research protocols completed with individual users'' [57]. Such full disclosure of privacy allowances and expectations is one way of ensuring an institution's legal and ethical requirements and expectations are met. To meet this need to protect those who had no say in the disposition of their records, policies for what type of records are acquired and the amount of time after which a record can be made accessible can be written into acquisition and accessibility procedures. For example, Columbia University adds a reasonable time limit when providing access to records [58]. Special collections professionals can also focus on acquiring sources that contain similar information without large amounts of personal or individual data, such as annual reports [59].

The privacy protections central to HIPAA are those that are already written into the fabric of the special collections profession. The ethical conundrum is to determine how to balance this protection, which is now legally and often arduously mandated, against the good of ensuring the legitimacy of the historical record. The ethical standards—inherent in the professional sense of altruism, codes of ethics, and literature—coupled with sensible policies and procedures can aid in the tightrope walk done every day by all archivists in almost every setting.

RECOMMENDATIONS

If an archives or special collection determines that it holds or is likely to hold materials that fall under the purview of HIPAA, it is in the organization's best interest to establish policies and guidelines tailored to the unique nature of these materials with a collection and access policy that includes information on HIPAA compliance. Addressing such access and compliance issues early and head on can eliminate unnecessary ''access anxiety'' on the part of all concerned.* Also, a proactive approach gives an archive or special collections unit the opportunity to shape a balanced policy. These policies can be included in current collection documents of the institution or can be put together into a stand-alone document on privacy compliancy. The following section outlines a suggested process for developing such policies.

Preparation work

A first step toward creating a balanced institutional HIPAA-compliant policy is to survey the collections to gain a clear idea about what does and does not contain HIPAA-sensitive material. Once HIPAA-sensitive records have been identified, one should analyze the materials for their potential future use and importance to the historical record. It is important to note obviously important records, such as annual reports and older doctor ledgers. These examples may be useful when talking to administrators and lawyers who may review the policy about why it is important to retain such records and to make them accessible. The analysis may also identify records that should be marked for deaccession due to questions regarding legality of possession and/or limited potential for future use.

During this preparation stage, it is also a good idea to become familiar with HIPAA privacy clause regulations and the ways that they have been applied at similar institutions. Becoming familiar with legal terms needed to discuss the law in an informed way and being prepared with a knowledge of policies that are in line with the mission of the organization can make the next step of meeting with legal counsel more productive.

Meeting with institutional legal counsel or Health Insurance Portability and Accountability Act officer

Close collaboration, advice, and support from legal counsel or designated HIPAA officer is essential when writing a HIPAA-compliant policy because each institution has different interpretations and corporate policies for supporting the nuances of local, state, and national privacy. Since the inception of the HIPAA legislation, many major medical centers have hired legal counsel dedicated primarily to compliance issues. Smaller repositories outside of a medical center may need to discuss HIPAA issues with the organization's general counsel or contracted attorney. Regardless of the level of attention the organization

* Term coined by Lawrence, in ''Access Anxiety: HIPAA and Historical Research'' [16], on the unnerving process of delving into historical records containing privacy information.

pays to HIPAA, it is likely that the legal counsel will be unfamiliar with archival, special collections, or library operations. Therefore, an archivist or special collections librarian should be prepared to spend some time at meetings educating the representative about what an archive or special collections unit is and what professionals who work in them do on a daily basis.

If applicable, one should be prepared to describe how these collections are different than medical records departments and the records they traditionally maintain. It is desirable to bring materials or have examples ready to show the variety of materials that are present in the institution that have PHI and to demonstrate why they are important to the institution's mission or to the parent organization. It is also important to go to the meeting with an idea of what the ideal HIPAA policy for archives or special collections would be and to have examples of workable policies from similar institutions. This meeting may also be a good time to look at privacy and confidentiality issues in general, even for materials not under the purview of HIPAA.

Questions for such a meeting include whether or not the institution, as a whole, is a covered entity or how, if it is a hybrid entity, it handles other departments that may be related to the archive or special collection. Do other, similar departments in the institution have procedures for collecting and providing access to material that contains PHI? During the conversation, it is useful to gauge how risk-averse the organization is and to determine whether the privacy officer or attorney considers the archives or special collections an area of concern. The privacy officer may have questions as well, such as what the purpose of the records is, if they were created during the course of research studies with human subjects or patient care, who created the records, and what type of records are involved. The privacy officer may also have policy questions about who has accessed the records and for what purpose.

Under the privacy rule, an historical researcher may seek a waiver of the requirement to obtain an authorization to use PHI or may seek an alteration of an existing authorization either through a privacy board or through an IRB. In most cases, an historical researcher will seek a waiver or alteration from a privacy board, not an IRB, because it is possible to set up a privacy board with members who are more familiar with the routines and nuances of historical research. When organizing a privacy board for overseeing access to historical medical collections, at least one member of the board should be familiar with the purposes and procedures of historical health sciences research. All members should be familiar with the legal and ethical issues of such research. Historical records custodians should be prepared to make researchers aware of the privacy board requirements and rationale and to provide detailed documentation and information for those who may be unfamiliar with the process of consulting such a board.

The privacy rule allows an IRB to deal with approval for a HIPAA alteration or waiver, either at the same time it approves research with human subjects or separately [60]. It is most likely that an historical researcher will seek a waiver or alteration of authorization from an IRB instead of a privacy board when the researcher is working in an area that the IRB normally oversees, such as when the researcher must obtain informed consent from living human subjects. In either case, the custodian of historical health sciences records should be prepared to support the researcher as necessary.

Policy documents and supporting forms

Introduction. A privacy policy introduction can provide the casual or nonmedical researcher with the background behind the policy and access restrictions. This section should include an introduction to privacy and confidentiality laws, their impact on research within the repository, and any general statement required by the institution regarding use of the materials.

Open and redacted information policy. This section should focus on materials that are open to use by the general public, including materials that the privacy rule does not cover, redacted open access copies, and materials that are older than HIPAA's reach. If the institution has established a grandfather date for access to records outside the privacy rule, this should also be noted in the policy. Researchers should be made aware of the types of information that may be missing in redacted records and pointed to later sections in the policy if they desire greater access.

Procedures for accessing confidential records. After discussing the types of records that are openly available, this section should focus on those that are restricted and the ways to obtain access for use and publication, including timelines, access, and information dissemination expectations. This section should also outline the IRB or privacy board process, especially for the nonmedical researcher who is unfamiliar with these procedures.

Institution's policy for future collecting. In addition to outlining access policies that take into account privacy and confidentiality issues, a policy should address future collecting in light of the privacy rule's legal restrictions as well as other factors, such as preservation, space, and costs. For example, collecting material with PHI may involve increased staff time to redact information or walk researchers through the process of accessing the records properly. Storage availability and costs may be prohibitive for large collections that researchers cannot access easily. In some cases, alternate, less-sensitive sources—such as annual reports, research or grant final reports, or other publications with aggregate data—may provide the same information without the restrictions of the

privacy rule. Other factors that have an impact on future collecting include the institution's risk-aversion level and current collection development mission and policy statements. Policy writers should consult other factors unique to their institutions when establishing HIPAA-compliant collection policies.

CONCLUSION

Professionals who curate health sciences history collections are challenged by the seemingly contradictory obligations of adhering to the privacy legislation and ethical standards, while maintaining the integrity of and access to the historical record. Other health sciences librarians who become custodians of historical records may also face these challenges. There is a fair amount of speculation about what effect privacy legislation, such as HIPAA, has had on the retention and preservation of the historical record. This is especially true among institutions that have had a conservative approach toward the collection of and access to these materials. Further research is suggested in this area to assess whether this concern has been justified and if the balanced policy practices proposed here can remedy this imbalance.

It is indeed possible to strike a careful balance between these two professional mandates through careful planning and preparation. This planning should extend to institutional policies for a variety of collection activities. Although ethical concerns and privacy legislation, such as HIPAA, have caused a myriad of reactions that may have been, at times, heavy handed toward perceived legal compliance and against collecting and providing access to sensitive materials, provisions exist in the law and at most institutions that allow for the balanced acquisition of, and access to, such materials.

REFERENCES

1. Science, Technology, and Health Care Roundtable and Archivists and Librarians in the History of the Health Sciences. HIPAA resource page [Internet]. Chicago, IL: The Roundtable; [2009] [cited 9 Jul 2010]. <http://www.library.vcu.edu/tml/speccoll/hipaa.html>.
2. Alan Mason Chesney Medical Archives, Johns Hopkins Medical Institutions. Privacy forms for HIPAA [Internet]. Baltimore, MD: The Archives; [2010] [cited 9 Jul 2010]. <http://www.medicalarchives.jhmi.edu/hippaform.html>.
3. Augustus C. Long Health Sciences Library Archives and Special Collections, Columbia University. Access policies: access to records containing protected health information (PHI) [Internet]. New York, NY: The University; [2005] [cited 9 Jul 2010]. <http://library.cpmc.columbia.edu/hsl/archives/accesspatient.html>.
4. Winn P. Confidentiality in cyberspace: the HIPAA privacy rules and the common law. Rutgers Law J. 2002;33(3):618–20.
5. Winn, Confidentiality in cyberspace, p. 654–5.
6. Richards N, Solove D. Privacy's other path: recovering the law of confidentiality. Georgetown Law J. 2007;96(1):126.
7. Warren S, Brandeis L. Right to privacy. Harvard Law R. 1890;4(5):193.
8. Warren, Right to privacy, p. 195.
9. Warren, Right to privacy, p. 211.
10. Richards, Privacy's other path, p. 147.
11. Prosser D. Privacy. California Law R. 1960;48(3):389.
12. Richards, Privacy's other path, p. 154–6.
13. Hammonds v. Aetna Cas. & Surety Co. 243 F. Supp. (N.D. Ohio, E.D. 1965).
14. Biddle v. Warren Gen. Hosp. 715 N.E. 2d 518 (Ohio, 1999).
15. Department of Health and Human Services (US). Summary of the HIPAA Privacy Rule. [Washington, DC]: The Department; [2003?]. p. 17–8. (Available from: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf>. [cited 1 Jun 2010].).
16. Lawrence S. Access anxiety: HIPAA and historical research. J Hist Med Allied Sci. 2007;62(4):429–30.
17. Lawrence, Access anxiety, p. 426.
18. 45 C.F.R. Sect. 160.102 (2009).
19. Department of Health and Human Services (US), Summary of the HIPAA Privacy Rule, p. 2.
20. 42 U.S.C. Sect. 300gg–91(a) (2(2009)).
21. 45 C.F.R. Sect. 164.102–03 (2009).
22. 45 C.F.R. Sect. 160.103 (2009).
23. 42 U.S.C. Sect. 1395x(u) (2009).
24. 42 U.S.C. Sect. 1395x(s) (2009).
25. Lawrence, Access anxiety, p. 438.
26. Department of Health and Human Services (US), Office of the Secretary. Modifications to the HIPAA privacy, security, and enforcement rules under the Health Information Technology for Economic and Clinical Health Act. Proposed Rules. Fed Regist. 2010 Jul 14;75(134):40868–924. (Available from: <http://www.ncbi.nlm.nih.gov/bookshelf/br.fcgi?book=citmed&part=A42777>. [cited 17 Jul 2010].).
27. Department of Health and Human Services (US), Centers for Medicare and Medicaid Services. Covered entity decision tools [Internet]. [Washington, DC]: The Department [2003?] [cited 4 Jun 2010]. <http://www.cms.gov/apps/hipaa2decisionsupport/default.asp?>.
28. Department of Health and Human Services (US). Protecting personal health information in research: understanding the HIPAA Privacy Rule [Internet]. [Washington, DC]: The Department; [2003?]. p. 5. [cited 1 Jun 2010]. <http://privacyruleandresearch.nih.gov/pdf/HIPAA_Booklet_4-14-2003.pdf>.
29. 45 C.F.R. Sect. 164.520 (2009).
30. 45 C.F.R. Sect. 164.530(a)–(b).
31. 45 C.F.R. Sect. 164.530(i) (2009).
32. Department of Health and Human Services (US), Protecting personal health information in research, p. 6.
33. 45 C.F.R. Sect. 164.514(e)(2) (2009).
34. 45 C.F.R. Sect. 164.502 (2009).
35. Department of Health and Human Services (US), Summary of the HIPAA Privacy Rule, p. 4–9.
36. 45 C.F. R. Sect. 164.512 (2009).
37. Department of Health and Human Services (US), Summary of the HIPAA Privacy Rule, p. 10.
38. Department of Health and Human Services (US), Summary of the HIPAA Privacy Rule, p. 4–9.
39. 45 C.F.R. Sect. 164.514(e)(2) (2009).
40. Department of Health and Human Services (US), Protecting personal health information in research, p. 10.
41. Department of Health and Human Services (US), Protecting personal health information in research, p. 11.
42. Department of Health and Human Services (US), Protecting personal health information in research, p. 13.
43. Lawrence, Access anxiety, p. 431–2.
44. Lawrence, Access anxiety, p. 433–4.
45. Lawrence, Access anxiety, p. 434–5.

46. Craig B. Confidences in medical and health care records from an archive perspective. In: Behrnd-Klodt M, Wash P, eds. Privacy and confidentiality perspectives. Chicago, IL: Society of American Archivists; 2005. p. 250.
47. Craig, Confidences in medical and health care records, p. 248.
48. Craig, Confidences in medical and health care records, p. 253.
49. MacNeil H. Information privacy, liberty, and democracy. In: Behrnd-Klodt M, Wash P, eds. Privacy and confidentiality perspectives. Chicago, IL: Society of American Archivists; 2005. p. 79.
50. Novak S. The Health Insurance Portability and Accountability Act of 1996: its implications for history of medicine collections. Watermark. 2003;26(3):45.
51. Craig, Confidences in medical and health care records, p. 246–7.
52. Huffman E. Medical record management. Berwyn, IL: Physicians' Record Company; 1972. p. 379–80.
53. MacNeil, Information privacy, p. 67.
54. Society of American Archivists. Code of ethics for archivists [Internet]. Chicago, IL: Society of American Archivists; 2005 [cited 4 Jun 2010]. <http://www.archivists.org/governance/handbook/app_ethics.asp>.
55. Association of Canadian Archivists. Code of ethics [Internet]. Ottawa, ON, Canada: The Association; 1999 [cited 4 Jun 2010]. <http://www.archivists.ca/content/code-ethics>
56. International Council on Archives. Code of ethics [Internet]. Paris, France: International Council on Archives; 1996 [cited 4 Jun 2010]. <http://www.ica.org/en/node/37328>.
57. Craig, Confidences in medical and health care records, p. 248.
58. Novak, The Health Insurance Portability and Accountability Act of 1996, p. 49.
59. Craig, Confidences in medical and health care records, p. 252.
60. 45 C.F.R. Sect. 164.512(i)(2)(iv) (2009).

AUTHORS' AFFILIATIONS

Judith A. Wiener, MA, MLIS (corresponding author), judith.wiener@osumc.edu, Assistant Professor, and Assistant Director for Special Collections and Outreach; **Anne T. Gilliland, MLIS, JD,** anne.gilliland@osumc.edu, Head, Copyright Management Office; Prior Health Sciences Library and Center for Knowledge Management, The Ohio State University, 376 West Tenth Avenue, Columbus, OH 43210

Received June 2010; accepted August 2010