Exploring the Evolution of Access: Classified, Privacy, and Proprietary Restrictions

William C. Carpenter, Charlene Nichols, Sarah A. Polirer, and Judith A. Wiener

Abstract

You found the information, but can the researcher have access to it? These essays explore the issues of information access in an evolving digital and post-9/11 world. If you're an archivist, records manager, or historian in a government, university, or business repository, access restrictions probably apply to your collections. These essays focus on the evolution of national security, health, and proprietary restrictions in the context of conflicting archival mandates for distributing information freely but responsibly.

Introduction

Charlene Nichols

A professional media coach who had never met an archivist recently listened to a description of the tasks performed in the trade: accessioning, processing, reference, and conservation. Based on these descriptions, the coach characterized archivists as "information gatekeepers."

Although at first this may seem like a limited view, the knowledge of the archivist and the decisions made on the job (e.g., the records chosen, the level

Session 602 at the 75th Annual Meeting of the Society of American Archivists, Chicago, Illinois, Saturday, 27 August 2011. Charlene Nichols chaired this session and the speakers were Sarah A. Polirer, William C. Carpenter, and Judith A. Wiener. These essays reflect the views of the authors and should not be regarded as the official position of their employing institutions.

of description) all contribute to the information that will be accessible to future researchers. Even those documents that survive through time, however, that have been lucky enough to land in a safe, dry place—kept by their creators, maintained by their custodians, chosen by professionals, and described in infinitely replicating Web-welcoming bytes—even these fortunate few still may never make it to the posterity poets promise.

Who is "posterity"? A scholar? A U.S. citizen? An employee? A lawyer? A thief? Are government archives open to all? Will a corporate archives offer the same access as a university archives? A corporation is required to keep a competitive advantage in the marketplace, a university is mandated to educate and enlighten. Could a military archives provide the same access as a state archives? These essays approach access from the different perspectives of the university, business, and government.

The new SAA core values describe access this way: "Archivists promote and provide the widest possible accessibility of materials, consistent with any mandatory access restrictions, such as public statute, donor contract, business/institutional privacy, or personal privacy."[1] This statement balances the need to provide the greatest access possible while acting responsibly and professionally. These essays explore all aspects of mandatory access restrictions in the twenty-first century, including statutes, policy, and privacy.

The complex ways that technology, funding, and laws change over time also affect access. In the 1990s, many public and private archives began to digitize their collections. This trend followed a federal mandate to make all publications of the Government Printing Office (GPO) available electronically, switching over to a digital Federal Depository Library Program. Share! Everything changed after 11 September 2001. In one month, a single government agency, the Department of Energy, took down nearly sixteen thousand electronic records, and it was not alone. If every government document is available electronically, how do we keep the terrorists from seeing them? Suddenly the mantra was Don't Share! Interestingly, the 9/11 Commission decided that the tragedy could have been stopped if information was shared more efficiently between government agencies, and it created a new technological tool, NetCentric Diplomacy, to enable collaboration.[2] Share! But in 2010, after the scandals that followed Wikileaks, this new tool was taken down. Just this year, we were brought full circle when proposed budget cuts in a bill that passed the House in July would

[1] See Society of American Archivists, "Core Values," http://www2.archivists.org/statements/core-values-of-archivists, accessed 14 September 2011.

[2] For more information on this concept, see *Wikipedia*, s.v. "Net-centric," http://en.wikipedia.org/wiki/Net-centric, accessed 12 November 2011. See also National Commission on Terrorist Attacks upon the United States, *The 9-11 Commission Report* (2004), available at http://www.9-11commission.gov/report/index.htm, accessed 12 November 2011.

keep the GPO from providing electronic access by cutting the line item for its main electronic repository.[3]

These essays discuss how changing technologies and laws have affected access restrictions over time by exploring three complex restrictions on access and how they are implemented in different institutional settings. This exploration includes an in-depth analysis of the changing statutes and communities of practice that have influenced access through time in various archival settings. Each essay focuses on different access restrictions within a specific institutional setting, including governmental classified restrictions, the proprietary restrictions of business archives, and various privacy restrictions and legislation, including the Health Insurance Portability and Accountability Act (HIPAA)[4] imposed on access to medical archives.

From Pearl Harbor to Abu Ghraib: The Evolution of Classified National Security Information and Declassification Policy and Practice

William C. Carpenter

Secrecy vs. Classified National Security Information

The tension between the right of Americans to access information about their government and the government's requirement to restrict at times access to its workings dates to the earliest years of the nation. The Continental Congress, meeting in Philadelphia, resolved in 1775 that its delegates not divulge anything debated in Congress or anything that a majority of them ordered be kept secret. Article I, Section 5 of the Constitution requires both legislative houses to publish their proceedings, "excepting such Parts as may in their Judgment require Secrecy." In these early years, in the context of a looming war for independence and the consolidation of the early Republic, secrecy was defined as a necessary, though not necessarily desirable, condition for conducting the business of governing and legislating. Although the U.S. government may restrict public access to the information it collects or produces for many reasons, the category of classified national security information is perhaps the most significant. Seventy-six million classification decisions were made in FY 2010, according to the most recent annual report of the Information Security Oversight Office (ISOO), the office within the National Archives and Records Administration that oversees the classification system throughout the

[3] For more on this bill, see OMB Watch, "House Questions Future of Government Printing Office," http://www.ombwatch.org/node/11786, accessed 12 November 2011.

[4] For more information on the Health Insurance Portability and Accountability Act of 1996 (HIPAA), see U.S. Department of Health and Human Services, "Health Information Privacy," http://www.hhs.gov/ocr/privacy/, accessed 12 November 2011.

government.[5] This essay focuses on the evolution of declassification policy and practice over the last seventy years.[6]

Early Classification Authority and Policy: From Statute to Executive Order

Military and diplomatic necessity have caused the military components and the Department of State to establish their own practices for restricting access to sensitive information since the late eighteenth century. Legislation, beginning with the Defense Secrets Act of 1911, which was later repealed by the Espionage Act of 1917 that remains in effect in amended form, defined what constitutes national defense information in broad terms and the criminal penalties for its unauthorized disclosure. Not until March 1940, during a period of militarization before the entry of the United States into World War II, did a single executive branch, government-wide policy define the handling of classified national security information. Franklin Delano Roosevelt's Executive Order (or EO) No. 8381 cited a statute from 1938 as its basis.[7] This EO, which served throughout WWII and its aftermath, was replaced and expanded during the Truman administration. The second Truman order, EO No. 10290, was the first in which the president's constitutional role as commander-in-chief stood as the primary authority for administering a security classification system. This EO was also the first to recognize the special status of "Restricted Data" as defined by the Atomic Energy Act of 1946, which effectively classified information regarding nuclear weapons' design from their creation and placed the control of that information in a new civilian agency, the Atomic Energy Commission, later the Department of Energy.[8]

Truman's order and those of presidents Kennedy, Nixon, Carter, Reagan, Clinton, George W. Bush, and Obama differ in detail, but all follow a similar pattern of establishing clear parameters for who may classify information in the first place, the levels of classification, reasons for classification, duration of

[5] National Archives and Records Administration, Information Security Oversight Office (ISOO), *2010 Annual Report to the President*, 12, http://www.archives.gov/isoo/reports/2010-annual-report.pdf, accessed 15 September 2011.

[6] For a general overview of secrecy in American government, see Timothy L. Ericson, "Building Our Own Iron Curtain: The Emergence of Secrecy in American Government," *American Archivist* 68 (2005): 18–52.

[7] Executive Order No. 8381, as well as all subsequent orders, is available at the comprehensive website of the Federation of American Scientists, "Selected Executive Orders on National Security," http://www.fas.org/irp/offdocs/eo/index.html, accessed 15 September 2011. Current Information Security Oversight Office policy documents are available at National Archives, "Classified National Security Information," http://www.archives.gov/isoo/policy-documents/, accessed 17 November 2011.

[8] This section also draws upon Robert M. Pallitto and William G. Weaver, *Presidential Secrecy and the Law* (Baltimore: The Johns Hopkins University Press, 2007), 65–76.

classification, and storage and transmission requirements. These orders differ significantly in the area of declassification.

Systematic Declassification and Special Initiatives

The earliest orders recognized that information ought to be declassified once it no longer meets the standards for classification. But in 1961, President Kennedy's EO No. 10964 substituted a significant paragraph in a Truman order, requiring an even greater responsibility for the U.S. government to declassify its secrets and reduce overclassification. Holding that the nation's classified information would be better protected if the classification system were not overloaded, Kennedy's order established limited classification periods as well as automatic downgrading and declassification instructions for most routinely classified information. President Nixon's 1972 EO No. 11652 took this process one step further by ordering that "All Information and material classified after the effective date of this order shall, whether or not declassification has been requested, become automatically declassified at the end of thirty full calendar years after the date of its original classification," except for specific information to be determined by department heads. Subsequent orders later superseded this provision, which did not apply to records classified prior to 1972, though it did plant a seed for future declassification policy.

Perhaps surprisingly, where the Nixon order stands out is in establishing formal structures for declassification. Although individuals with classification authority have always been able to declassify information according to need or expediency, Nixon's 1972 order codified two avenues of declassification. First, the National Archives was required to develop a program for the periodic review and declassification of thirty-year-old classified records specifically for public release. This program was called *systematic review*. The second avenue, called *mandatory declassification review*, allowed a U.S. citizen to request the declassification of specific classified records from an agency.

The systematic review provisions of Nixon's order resulted in the creation of a declassification establishment at the National Archives. Federal agencies that had accessioned classified records to the National Archives were required to develop detailed guidance that described information for withdrawal from public access (such as details of intelligence activities abroad, still sensitive military plans or technology, or information that would damage foreign relations if released). National Archives staff would withdraw documents containing sensitive information from records series identified by archivists as having high researcher interest, insert withdrawal notices in their places in the processed series, and maintain the withdrawn items in parallel series. If a researcher found a withdrawal notice in the open stacks, he or she could use that notice to request

a mandatory declassification review or a Freedom of Information Act (FOIA) review for that document.[9]

This systematic review program at the National Archives resulted in the declassification of millions of pages of World War II records, State Department consular files, and other records. Concurrent with the systematic review program focused at the National Archives, information could be declassified as a result of targeted reviews of special topics. One such initiative was that of the Department of Defense to declassify and publish records concerning the decryption of Japanese communications prior to and during World War II—the "Pearl Harbor" of the title of this essay.[10] This initiative, concluded in 1977, predated the declassification of the very existence of the National Security Agency (NSA). Later, in the 1990s, the NSA undertook a similar initiative to declassify the intercepted and decrypted communications between the Soviet Union and its agents in the United States in the 1940s, known as the VENONA project.[11]

Automatic Declassification, 1995–2010

This declassification establishment—of systematic declassification review conducted by National Archives staff using guidance provided by agencies, of mandatory declassification review for specific documents requested by the public, and special initiatives for records on certain topics—could not possibly have coped with the massive volume of classified records that the U.S. government had created in the fifty years since the end of World War II. In the period after the dissolution of the Soviet Union and the end of the Cold War as we knew it then, information policymakers at the highest levels of the U.S. government saw an opportunity to transform how records became declassified and to actually implement the principle of automatic declassification hinted at in the Nixon order.

In 1995, President Clinton's EO No. 12958 established the principle of automatic declassification that remains in effect today. In this principle, information contained in records determined to have "permanent historical value" under Title 44 of the *U.S. Code* and to be more than twenty-five years old shall be automatically declassified, whether the records have been reviewed or not,

[9] This was the process that occurred for the several documents declassified by the Central Intelligence Agency in 2011 regarding secret writing detection techniques used by the U.S. government during World War I. The Archivist of the United States, David Ferriero, has commented on these documents at AOTUS, National Archives, "Spies and Secret Writing," 22 April 2011, http://blogs.archives.gov/aotus/?p=2658, accessed 15 September 2011.

[10] Department of Defense, *The "Magic" Background of Pearl Harbor*, 5 vols. (Washington, D.C.: U.S. Government Printing Office, 1977).

[11] John Earl Haynes and Harvey Klehr, *Venona: Decoding Soviet Espionage in America* (New Haven: Yale University Press, 1999).

unless an agency actively exempted from declassification records containing information that a new presidential panel approved for exemption under one of nine categories. This measure came into full effect on 31 December 2006, following two postponements of the automatic declassification date. The nine categories, which have not fundamentally changed since 1995, are intelligence sources and methods, weapons of mass destruction, cryptology, state-of-the-art weapons technology, war planning information, foreign policy and diplomatic relations, protection of the president, emergency preparedness, and treaties or statutes.

Agencies wishing to apply these exemptions are required to describe the information they wish to exempt in a declassification guide, which is in turn approved by the Interagency Security Classification Appeals Panel (consisting of representatives from the Departments of State, Justice, and Defense as well as the National Archives, National Security Council, Office of the Director of National Intelligence, and the Central Intelligence Agency).[12] In this manner, the authority to continue the classification of information beyond twenty-five years is no longer soley controlled by the originators of that information. This panel also adjudicates appeals of Mandatory Declassification Review requests.

The framers of EO No. 12958, including Steven Garfinkel, the long-serving director of the Information Security Oversight Office (itself established to oversee the government-wide classification system by President Carter's 1978 order), never envisioned that automatic declassification would necessarily result in the page-by-page review of records twenty-five years old or older prior to them being made available to the public. In 1998, however, following the inadvertent disclosure of some nuclear weapons information, Senators John Kyl and Trent Lott sponsored an amendment to the 1999 National Defense Authorization Act that effectively requires a page-by-page review of records prior to declassification to ensure that Restricted Data and Formerly Restricted Data, which are excluded from automatic declassification, are not improperly released.[13]

In anticipation of automatic declassification in the late 1990s, agencies that did not have a substantial declassification establishment worked to develop such a capacity. Recognizing that the systematic review system at the National Archives could not cope with the volume of records that needed to be reviewed, the National Archives provided space for teams of agency reviewers at the National

[12] Under EO No. 12958, the Central Intelligence Agency was a full member of the six-member panel. Section 5.3(a) of President Obama's EO No. 13526 assigned the Office of the Director of National Intelligence to the panel, while allowing the Central Intelligence Agency to appoint a temporary representative to participate as a voting member in all deliberations involving classified information originated by that agency. For these deliberations, the panel has seven members.

[13] The Federation of American Scientists has posted this statute on its website at http://www.fas.org/sgp/congress/hr3616am.html, accessed on 15 September 2011. For a critique of this legislation, see Ted Gup, *Nation of Secrets: The Threat to Democracy and the American Way of Life* (New York: Doubleday, 2007), 119.

Archives in College Park, and, in the case of the U.S. Army, allowed the temporary shipment of records to an off-site review facility. During these agency reviews, declassification reviewers would "tab" documents for exemption from declassification or, more commonly, for "referral" to another agency for future review. During archival processing, the National Archives would, in turn, withdraw the tabbed documents and make the remainder of the documents available to researchers. Between 1995 and 2010, this process resulted in agencies declassifying over one billion pages of records.[14]

EO No. 13526: The NDC and Exemption Reform

President Clinton's order, transformative as it was regarding declassification, created two significant problems not resolved until President Obama signed the current EO No. 13526 at the very end of December 2009. The first was the problem of referrals. Those one billion pages of declassified records included about four hundred million pages of records that remained in declassification "purgatory." These records had been reviewed for declassificatiovn by the responsible agency but they contained records referred for review by another agency and requiring processing by the National Archives before release. A small but significant change in President Obama's order has since restricted the types of information eligible to be referred. Nonetheless, by the late 2000s, the National Archives was faced with thousands of cubic feet of records that needed to be reviewed again by all of the agencies to which records had been referred by the primary reviewing agency.

The fundamental solution to the referral problem had been foreseen by the late senator Daniel Patrick Moynihan, chairman of the Commission on Protecting and Reducing Government Secrecy in the late 1990s and the author of the book *Secrecy*. He advocated for the creation of a National Declassification Center, which would colocate declassification specialists from across the government to increase the efficiency of review.[15] In 2007, the Public Interest Declassification Board, an advisory board of presidential and congressional appointees, also recommended the creation of such a center.[16] Section 3.7 of President Obama's order finally established the National Declassification Center at the National Archives, and a supplementary memo signed on the same day as the order charged it with processing the four-hundred-million page "backlog" of

[14] Information Security Oversight Office, *2010 Annual Report to the President*, 14.

[15] Daniel Patrick Moynihan, *Secrecy: The American Experience* (New Haven: Yale University Press, 1998), 217–18.

[16] "Improving Declassification: A Report to the President from the Public Interest Declassification Board," December 2007, 23, available at National Archives, http:// http://www.archives.gov/pidb/improving-declassification.pdfwww.archives.gov/pidb/improving-declassification.pdf, accessed 15 September 2011. [FILE NOT FOUND]

reviewed but not released records by establishing interagency solutions to resolve referrals. The most recent biannual public report of the National Declassification Center states that, since January 2010, the center has processed eighteen million pages, 92 percent of which have been declassified and are available to the public.[17]

The second legacy of President Clinton's order resolved by President Obama is that of the ultimate disposition of records exempted from automatic declassification at twenty-five years. Under President Clinton's executive order, agencies that sought presidential panel approval to exempt information from automatic declassification were required to specify a date on which the exempted information would be declassified. This date was established on an agency-by-agency basis, but was, in most cases, about twenty-five additional years, which was not satisfactory to some agencies for their most sensitive information. Section 3.3(h) of President Obama's order clarified this murky situation by specifying that all records containing information exempted from automatic declassification at twenty-five years will be automatically declassified when those records reach fifty years, except for records that reveal the identity of a human intelligence source or key design concepts of weapons of mass destruction. Additionally, agencies may request exemptions at fifty years for specific information in "extraordinary cases" for information such as technical intelligence methods or highly charged diplomatic issues. These extraordinary exemptions may only be requested for information contained in records approaching fifty years old. Finally, all records containing information exempted from declassification at fifty years will be automatically declassified when those records reach seventy-five years, unless an agency head requests that even more specific information be exempted by the panel, and the panel agrees and sets a future declassification date. Agencies are developing their requests for special exemptions now, for submission to the panel one year before these new milestones come into effect at the end of 2012. Finally, since 2008, the ISOO has assessed the results of agency declassification reviews and published its findings, along with other pertinent statistics relating to records classification and declassification, in its annual report to the president.[18]

Declassification in Practice: Classification Outside of Government Control

Declassification policy intersects directly with the archival community outside the government when classified national security information leaves

[17] "Biannual Report on Operations of the National Declassification Center, Reporting Period: January 1, 2011 – June 30, 2011," National Archives, "NARA and Declassification," http://www.archives.gov/declassification/reports/2011-biannual-january1-june30.html, accessed 15 September 2011.

[18] Information Security Oversight Office, *2010 Annual Report to the President*, 23.

government control. Buried deep in the implementing regulations for President Obama's 2009 order, published in the *Code of Federal Regulations*, is 32 C.F.R. Part 2001.36: "Classified information in the custody of private organizations or individuals."[19] This section instructs nongovernmental repositories that find classified national security information in their collections to contact the Information Security Oversight Office for assistance. Classified information should never leave authorized control to begin with, but, historically, scientists, congresspeople, and senior government officials occasionally took copies of classified documents home with them upon leaving their official positions. When these individuals donate their papers to a manuscript repository, that institution finds itself in possession of classified information and a significant access problem. What happens after the initial contact by these repositories with the ISOO varies with each case, but in all cases ISOO will work with the repositories to ensure that national security information is properly handled while respecting the rights of the custodial organization. Among other archives, ISOO has worked with Bates College, Caltech, and the University of Mississippi.

Discretionary Declassification and the Problem of Leaks (Wiki- and Otherwise)

Records may also be declassified on the order of the president or an official to whom the president has granted classification authority. Section 3.1(d) of President Obama's order specifically provides for the declassification of classified information when the appropriate official determines that the public interest in the widest dissemination of that information outweighs the damage to national security that might result. We saw this with the declassification of the report by Major General Antonio Taguba regarding abuses at Abu Ghraib prison in Iraq in 2004, following significant public outcry. Details of interrogation methods, military prison administration, and operational military intelligence tactics were all properly classified and would likely have remained so for ten to twenty-five years, but the decision was made at the highest levels in the Department of Defense to declassify records related to those events in the interest of the fullest possible disclosure.[20]

[19] National Archives and Records Administration, Information Security Oversight Office, *32 CFR Parts 2001 and 2003*, 37269, 28 June 2010, http://www.archives.gov/isoo/policy-documents/isoo-implementing-directive.pdf, accessed 17 November 2011.

[20] The Freedom of Information Act (FOIA) Requester Service Center for the Office of the Secretary of Defense and Joint Staff provides many released records regarding detainee treatment, including the Taguba Report, on its website, "Detainee and Other Related Documents," http://www.dod.gov/pubs/foi/operation_and_plans/Detainee/, accessed 15 September 2011.

I had considered titling this essay "From Pearl Harbor to WikiLeaks," but worried that the reference to the alleged activities of Private Bradley Manning and Julian Assange could be misleading. The leaking of classified information, either intentionally by political insiders or by individuals like Manning (whatever their motives), or the inadvertent disclosure of classified information by mistake, does not constitute declassification action. In the mind of the public, however, this is not always clear.[21] When reading in the *Washington Post* about the CIA's activities in Pakistan to capture Osama Bin Laden, one might ask why the activities of that agency fifty years ago in other countries must remain classified. Those of us in the government working in declassification must be prepared to respond to such questions. From the Pentagon Papers, Watergate, and the Church Commission, to the invasion of Iraq and the issue of "warrantless wiretapping," the expectations of the public regarding access to classified information have shifted as dramatically over the last seventy years as have the policies surrounding declassification. The access community (the Federation of American Scientists, the American Civil Liberties Union, and the National Security Archive, in particular) and the historical community understand the recent shifts in policy and are awaiting results. It is the special responsibility of the National Archives to implement the president's intention to achieve the desired result of maximum access and necessary security.

The Proprietary Nature of Private Enterprise

Sarah A. Polirer

The concept of the proprietary nature of business records can be quite a challenge for those not working in a business environment. Why do these types of records pose such a challenge? Why do these types of records seem to be least understood? Leveraging some of the key concepts surrounding proprietary records—background and definition, information types, risk management, and information classification—leads to determining the access requirement needs of a specific enterprise.

The corporate archives is an organizational repository that supports the mission of the business or corporate entity. Specifically, our job in the Cigna[22] archives is to support the business in its mission as a global health services

[21] One voice among many commenting on the WikiLeaks phenomenon is that of Mary Rose Papandrea, "The Publication of National Security Information in the Digital Age," *Journal of National Security Law and Policy* 5 (2011): 119–30.

[22] Cigna® is a registered service mark and the "Tree of Life" logo and "GO YOU" are service marks of Cigna Intellectual Property, Inc., licensed for use by Cigna Corporation and its operating subsidiaries. All products and services are provided by such operating subsidiaries and not by Cigna Corporation. Such operating subsidiaries include Connecticut General Life Insurance Company, Cigna Health and Life Insurance Company, and HMO or service company subsidiaries of Cigna Health Corporation and Cigna Dental Health, Inc.

company. Cigna carries out its mission through its employees, and we focus on meeting their needs. Although archival processes such as ethics and appraisal may be intertwined in other types of repositories, this essay focuses on the nature of proprietary records and provides a practical approach to determining external researcher access to records created in a corporate business environment. I am frequently asked, "Why isn't your archives open for researchers?" Business scholars and others may find access restrictions daunting, but they actually make good business sense as they regard the proprietary nature of the information.

According to a study done by ASIS in 2007, "75% of most organizations' value and sources of revenue creation are intangible assets, intellectual property and proprietary competitive advantages . . . and are likely to be bought, sold, disseminated, shared, licensed, or traded as part of the transaction."[23] Another study done more recently by Ocean Tomo Intellectual Capital Equity estimates the value of intangibles at around 81 percent of Standard and Poor's 500 companies' value.[24] Even in a presentation done in 2006 by Foley, Foley and Lande—quoting the Brookings Institute, et al. and John P. Hutchins from *The Corporation's Valuable Assets: IP Rights under SOX*—found "that a typical company now has up to 85% intangible assets and that the value of trade secret information held by US publicly-traded companies alone, is more than $5 trillion."[25]

These numbers alone can cause business to pause. Following on these findings and the nature of business, two concepts surface: 1) business records contain restricted materials generally defined as proprietary, and 2) the nature of a business archives positioned within a business organization.

Let's start with the second point first. Generally speaking, the main objective of business is business, to paraphrase Francis X. Blouin, Jr., describing Philip F. Mooney's article in *The Records of American Business*,[26] and also to deliver a product to the customer. The primary mission of most business or corporate archives is to support their parent companies' missions. As Marcy Goldstein

[23] ASIS Foundation, *Trends in Proprietary Information Loss Survey Report*, August 2007, 37.

[24] McAfee and SAIC, *Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency* (2011), 6, http://www.mcafee.com/apps/view-all/publications.aspx?tf=data_protection&sz=10 , accessed 9 January 2012.

[25] Inside Counsel, Foley, Foley and Lardner, LLP, "Protecting Your Proprietary Information: Making Company Employees Allies in the Fight," Web Conference Series for Corporate Counsel, 15 November 2006. In the 1970s, a typical company's market capitalization was 80 percent tangible assets and 20 percent intangible assets. Now the typical market capitalization is 15 percent tangible assets and 85 percent intangible assets according to the Brookings Institute, Aurigin Systems, Inc., and *ABF Journal*, July/August 2004. "Trade secrets are estimated to comprise 80% of the assets of 'New Economy' companies," according to John P. Hutchins, *The Corporation's Valuable Assets: IP Rights under SOX*, 859 PLI/Pat 289, March 2006. Hutchins also notes that "it has also been estimated that the value of trade secret information held by US publicly-traded companies alone is more than $5 trillion." New web set up: http://www.foley.com/news/event_detail.aspx?eventid=1064, accessed January 9, 2012.

[26] Francis X. Blouin, Jr., "Introduction: Business and American Culture: The Archival Challenge," in *The Records of American Business*, ed. James M. O'Toole (Chicago: Society of American Archivists, 1997), 7.

states in *The Records of American Business*, "Business archives are a repository of the corporate memory, preserving documents that are needed for administrative, legal, and fiscal purposes and can be used for strategic planning, advertising, public relations, research and development, and litigation support."[27] These concepts are not new. Helen Davidson and Wilbur Kurtz also expounded on the administrative use of these archives in earlier writings.[28]

Regarding my first point, proprietary information is a company asset that is a driver and lever of the success of the business; however, percentages of open and closed records will differ among businesses, as will the definition of this restriction. Note that businesses are not the only ones with proprietary information, which is also found in private companies in partnership with vendors and in universities with research sectors, especially in technology and engineering.

The word "proprietary" is used in business all the time. The word generally seems to be synonymous with "confidential." In today's world, depending on the industry, proprietary information may be confidential, but confidential information may not be proprietary. What exactly is proprietary information and why does it hamper access to materials? There is no definitive standard used to determine what is proprietary. The term "proprietary" derives from the term "proprietor" or "ownership." It is considered part of the all-encompassing term "intellectual property." Something proprietary is considered to be private property.

Black's Law Dictionary describes *proprietary* as "belonging to ownership; belonging or pertaining to a proprietary (owner) who has legal right or exclusive title to property, business, etc." Under the Uniform Trade Secrets Act, this protected information must have economic value and the company must make a reasonable effort to protect it. Further, proprietary information "in trade secret law, is information in which the owner has protectable interest." And proprietary rights are "those rights which an owner of property has by virtue of his ownership . . . title and possession and is an interest or right of one who exercises dominion over a thing or property."[29] In other words, it is commercially valuable information.

Having the term defined under federal regulation, along with the conditions that proprietary information must meet, provides companies with legal recourse if proprietary materials are leveraged and exploited for financial gain, provided safeguards are in place to stop disclosure. According to the Federal Acquisition Regulation (48 C.F.R. 27.402 Policy), proprietary information is "a property right or other valid economic interest in data

[27] Marcy G. Goldstein, "Evolving Role of In-house Business Archives: From Tradition to Flexibility," in *The Records of American Business*, 41.

[28] Helen L. Davidson, "The Indispensability of Business Archives," *American Archivist* 30 (October 1967): 593–97, and Wilbur Kurtz, "Business Archives in the Corporate Function," *ARMA Quarterly* 4 (April 1970): 5–11.

[29] *Black's Law Dictionary,* 6th ed., s.v. "proprietary" (St. Paul, Minn.: West Publishing, 1994), 1220.

resulting from private investment. Protection of such data from unauthorized use and disclosure is necessary to prevent the compromise of such property right or economic interest."[30]

It wasn't until 1996, under the Economic Espionage Act (18 U.S.C. 1831–39), that trade secrets were further defined and given protection under federal law along with patents, creative works, and copyright. Additionally, thirty-nine states have laws that give remedy under theft. A significant body of case law now exists regarding remedy. State laws further define trade secrets and theft conditions and the reasonable actions companies may take to protect them.[31] The law defines

> trade secrets as all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if: the owner thereof has taken reasonable measures to keep such information secret, and; the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by the public.[32]

By their nature, business records exist to support the economic viability of the business, because proprietary information gives a company a competitive advantage in the marketplace. To be competitive in a market-based system, businesses need to protect those intangible assets that derive economic value.

Business Flow and Examples of Proprietary Information

To understand this definition it is necessary to understand the nature of business. Competitive advantage is the key to growth in the marketplace. Business evolves around having a product, methods of sales and marketing, methods of recording transactions, methods of delivering the product to the customer, and methods of reporting. Other factors in business include regulatory compliance and business protection laws. These business basics generate the following types of information: financial; prereleased; marketing and advertising; market-share and planning; research and development; technical specifications;

[30] Federal Acquisition Regulation, Title 48, Part 27 Patents, Data, and Copyrights (48 CFR 27.402 Policy), available at http://law.justia.com/cfr/title48/48-1.0.1.5.26.4.1.3.html, accessed 12 November 2011.

[31] David P. Bianco, "Reference for Business", *Encyclopedia of Business, 2nd ed.*, available at http://www.referenceforbusiness.com/encyclopedia/Pro-Res/Proprietary-Information.htm, accessed 20 June 2011,.

[32] "Proprietary Information and Trade Secrets," Wright State University, available at http://www.wright.edu/rsp/Security/S2unclas/Propriet.htm, accessed, 20 June 2011.

sales and product specifications, including demographics and customer-related information (HIPAA related); strategic business planning; legal and compliance, including mergers, acquisitions, divestiture materials, and minute books; IT; human resources, including personnel; and patents, trademarks, trade secrets, and copyrights.

Type of Risks

In today's global, electronic world, all types of business information are subject to threats, both deliberate and inadvertent, and at a more rapid pace than ever before. Losses are quickly felt and can be longer lasting. Risks can include misappropriation of information, infringement of rights, and counterfeiting. The methods used to breach information vary: inadvertent actions from internal sources; exploitations from partners, vendors, or customers; and deliberate open attacks.

These compromises or breaches of information can result in losses to reputation, image, goodwill, competitive advantage, core technology, and profitability. Specifically these risks can

> stifle an organization's competitive/economic advantage, erode an asset's value and future profitability, result in the loss of competitive advantage, devalue image and goodwill, reduce return and profitability, result in the loss of core business technologies, weaken economic and/or strategic advantages, increase vulnerability to potential terrorist and extremist threats, facilitate product counterfeiting or loss of prototype information, or undermine a transaction.[33]

Reducing Risk of Loss

Companies seek to reduce the risk of losing proprietary information by setting up policies and procedures to protect it. Doing so protects the viability of the business and enables it to seek legal recourse. Given a more global economy, an explosion of technology, and the speed in which information can be accessed and disseminated, the loss of proprietary information can quickly prove fatal for a business. Thus, minimizing the risk of loss is extremely important, although risk needs to be balanced with transparency and access.

The business archives plays a role in this ever-changing business structure. The archives needs to be responsive to information changes and document them as they relate to an organization's business records, and it needs to be available as a resource to aid in the development of employees and the support

[33] ASIS Foundation, *Trends in Proprietary Information Loss Survey Report*, 31–32.

of new business structures. Anne Van Camp's 1982 essay, "Access Policies for Corporate Archives," addresses some of these basic points and identifies basic records information access categories: open, restricted, and closed.[34] These categories can be further expanded to include a classification scheme based on records' sensitivity. The level of classification can be further refined to tease out issues such as information handling and use to minimize and eliminate any improper access that would adversely impact the business.

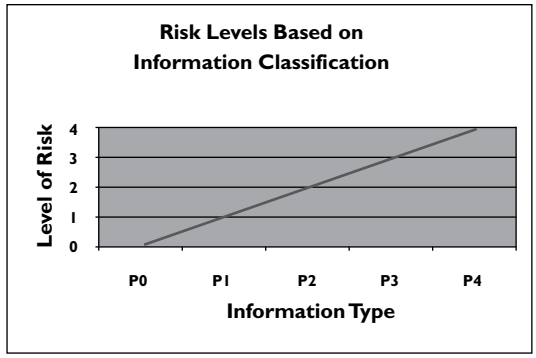
Records Classification

A due diligence process should be established for records classification, information ranking, and determining level of risk tolerance in a business archives. The due diligence process for records classification includes identifying the information, quantifying the information's value, performing a cost-benefit analysis, reviewing requirements, assessing vulnerability to threats, assessing its impact of loss of disclosure, identifying existing and planned security controls, determining information rank, and prioritizing risk of loss. The next step is to identify proprietary information on a sliding scale based on its sensitivity. For instance, proprietary information can be further classified from highly sensitive, to restricted, to confidential. An additional category would be nonproprietary, or public. Following classification, the final step is to determine the best methods for practically handling each level of information. Matrix schemes coordinate the levels of restriction with options for handling information, such as use, access, storage, and disposal (see the matrix illustrated in Figure 1).

Archives Role in Access

For corporate and business archivists, the challenge is to leverage a due diligence process that vets the potential researcher to determine the exact nature of the research intended and then to determine the relative nature of proprietary information that may or may not be involved in the research. The due diligence process at my organization includes interviewing the potential researcher to determine the research topic, determining whether the collection meets the researcher's needs, and asking the researcher to complete a written application. Upon receipt, the application is forwarded, along with collection material findings based on the application request and the archivist's recommendations, to the Legal and Public Affairs Department (L&PA). Upon return

[34] Anne Van Camp, "Access Policies for Corporate Archives," *American Archivist* 45 (Summer 1982): 296–98.



Information Handling

Format / Activity	P4	P3	P2	P1	P0
Access Requirements –internal	Approval by	Approval by	Approval by	Approval by	No approval needed
Access Requirements –external	Approval by	Approval by	Approval by	Approval by	Approval by
Faxing / e-mail	Password Protected Recipient Mailbox or Attended Receipt	Password Protected Recipient Mailbox or Attended Receipt	Approval by	No Restrictions	No Restrictions
Copying	Permission	Permission	Approval by	No Restrictions	No Restrictions
Labeling	Label Any Media, and Confidentiality Stamp plus Internal Labels	No Label Required Only Confidentiality Stamp	No Label Required Only Confidentiality Stamp	No Label Required Only Confidentiality Stamp	Release Date Plus Classification
Release to Third Parties	Approval, Non-Disclosure Agreement, or Duly Executed Contract Protects Confidentiality	Approval, Non-Disclosure Agreement, or Duly Executed Contract Protects Confidentiality	Non-Disclosure Agreement, or Duly Executed Contract Protects Confidentiality	Non-Disclosure Agreement, or Duly Executed Contract Protects Confidentiality	No Restrictions

FIGURE 1. This information is based upon comparison of multiple data risk classification charts used by organizations and then determination of their risk and protection levels. The author further extrapolated similar trends and provided a template that can be used to model data classification and risks. Sources include National Institute of Standards and Technology, Standards for Security Categorization of Federal Information and Information Systems (February 2004), http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf, accessed 12 November 2011; Stanford University, *Secure Computing*, "Stanford Data Classification Guidelines," http://www.stanford.edu/group/security/securecomputing/dataclass_chart.html, accessed 12 November 2011; and Shannon Buckley, "Data Classification," *Internal Auditor* (March 2011), http://www.theiia.org/intAuditor/itaudit/2011-articles/data-classification/, accessed 12 November 2011.

from L&PA, the researcher is notified appropriately and the materials will be prepared as necessary.

By leveraging information classification schemes and processes, and working through records identification, classification, and risk evaluations, the business archivist can determine how best to handle access requirements and balance openness with business and legal requirements. As an extension of the business, the intersection of company proprietary information and researchers' access needs puts the corporate or business archives in a unique position of balancing these two forces.

HIPAA and Beyond: Privacy and Confidentiality Legislative and Ethical Issues within Health Sciences Special Collections

Judith A. Wiener

The inherent nature of the materials found within health sciences special collections provides obvious challenges to the dual archival responsibilities of providing access to records, while maintaining the privacy of those whose lives the records reflect. Materials such as doctors' journals, hospital registers, and medical images provide unique historical resources that are of significant importance to researchers in a multitude of disciplines. At the same time, providing access to such materials brings forth ethical and legislative concerns that have changed dramatically over time.

Staff members at the Medical Heritage Center[35] at the Ohio State University Health Sciences Library are well aware of the daily challenges provided by medical archives. The center was established in 1997 as a partnership between the Ohio State University (OSU) and the Columbus Medical Association, which is the city's main physician professional organization. The focus of the center is to collect, preserve, and promote the rich health sciences legacy of central Ohio, and it does so by maintaining a collection of rare books, artifacts, and archival collections that enhance this mission. The center is under the reporting line of the OSU Health Sciences Library, but also has an advisory board comprising members from OSU, the Columbus Medical Association, and the community at large.

Unlike the Ohio State University Archives, which holds the official records of the public university, the Medical Heritage Center's archival collection policy centers more on personal papers and the health sciences organizations of the region not affiliated with the university, as well as pre-OSU medical school records. The center, therefore, is not bound by the public records mandates that govern the University Archives in providing open access, but is committed

[35] For more information, see The Ohio State University, Medical Sciences Library, "Medical Heritage," http://hsl.osu.edu/mhc, accessed 14 November 2011.

to the general mission of an academic institution to provide as much access to holdings as possible for researchers.

Carefully balanced with this mission of access, however, is the Medical Heritage Center's organizational situation as part of an academic medical center that must meet the regulations set forth by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). As part of a campus with a medical center, the Ohio State University was declared a hybrid institution under that law, meaning certain areas must comply with HIPAA regulations while others are not bound by its reach. This mix of ethical, professional, and legislative responsibilities in terms of protecting privacy makes the Medical Heritage Center the perfect microcosm of the various issues facing medical and health sciences special collections today.

The purpose of this essay is to briefly explore the evolution of privacy issues in medical records and to discuss their impact on both the archival profession and the historical record. It is important to note that this essay is not intended as legal advice. Rather, it seeks to provide for practitioners a background survey of the challenges that health sciences archival professionals have faced historically and currently as they walk the tightrope between providing access to valuable resources and protecting individual privacy.

The Origin of Privacy Standards in Medical Records

Tracing the evolution of privacy in medical records is indeed a winding road. Historically speaking, medical records have always contained sensitive information and patients generally trusted that this information would be used and shared responsibly by their physicians long before the enactment of federal privacy legislation.[36] Traditionally, the physician's professional code of ethics, and not legislation, was the main protector of patient privacy. As a professional ethical standard, the Hippocratic Oath documented early on the physician's duty to preserve the confidence of his or her patients and was understood and upheld by the physician or designated record's trustee.[37] It is not the nature of the records themselves, but the advent of technology and the possibility of widespread privacy breaches made possible by widespread access to digital record systems that led to today's legislative reality.[38]

[36] Barbara L. Craig, "Confidences in Medical and Health Care Records from an Archives Perspective," in *Privacy and Confidentiality Perspectives*, ed. Menzi L. Behrnd-Klodt and Peter J. Wosh (Chicago: Society of American Archivists, 2005), 246–47.

[37] History of Medicine Division, National Library of Medicine,"Greek Medicine: The Hippocratic Oath," http://www.nlm.nih.gov/hmd/greek/greek_oath.html, accessed 31 July 2011.

[38] Susan C. Lawrence, "Access Anxiety: HIPAA and Historical Research," *Journal of the History of Medicine and Allied Sciences* 62 (2007): 426.

The Legal Origin of Confidentiality and Privacy Concerns

Prior to 1890, the legal focus in regard to medical records was on protecting the confidence of the physician-patient relationship. Although often commonly used as synonyms, the terms "confidentiality" and "privacy" are not interchangeable from a legal standpoint. Confidentiality specifically refers to a breach of confidence at any level, within a relationship of trust, while privacy alludes to the public revelation of information that should be held in secret. Therefore, it is possible to break one's confidential relationship—for example a physician sharing a patient's condition with her husband—without violating privacy, as this information was not shared with the world at large. Before 1890, any legal action against a physician for violating this professional expectation was brought forth as a breach of confidence.[39]

In 1890, however, the right to privacy came into the forefront after Samuel D. Warren and Louis D. Brandeis wrote their groundbreaking article, "The Right to Privacy," in the *Harvard Law Review*. They argued that the law should protect citizens' privacy rights in the larger world as well as the confidences held between two individuals. Interestingly enough, one of their major arguments for the extension of privacy was the expanding usage of photographic technology. The ability for a photographer to take someone's image and publish it on a mass basis without his or her knowledge called for greater state protection in the authors' minds.[40] After the article was published, states began to quickly establish privacy laws. Today the regulations in HIPAA trump many state confidentiality and privacy laws in the area of health care records. It is important to note, though, that these laws are still very much in effect for those institutions not covered under HIPAA's reach and may provide additional causes for action in some cases.

Congress passed HIPAA in 1996, and it has changed the landscape in health sciences archives. It sets these special collections apart from other sorts of institutions in terms of privacy and confidentiality diligence. The act was founded out of both good intentions and concern for the expanding use of technology. It was intended to facilitate the transfer of health information electronically while addressing concerns over confidentiality and privacy breaches made possible by the new technology, as well as to provide more security for workers who changed jobs and faced the threat of not being able to secure health insurance because of pre-existing conditions. Although Congress passed the act, it did not spell out the specifics of the law, including its administrative regulations and

[39] Judith A. Wiener and Anne T. Gilliland, "Balancing between Two Goods: Health Insurance Portability and Accountability Act and Ethical Compliancy Considerations," *Journal of the Medical Library Association* 99 (2011): 15–16.

[40] Samuel D. Warren and Louis D. Brandeis, "Right to Privacy," *Harvard Law Review* 4 (1890): 193–220.

penalties. This task was left to the secretary of Health and Human Services, who enacted the Privacy Rule to codify the act's regulations.[41]

Of particular note and concern to those professionals working with medical archives is that the rule, which went into effect on 14 April 2003, has no grandfather clause. The rule covers all information in perpetuity, without consideration for the death of an individual or the age of the records. The only considerations for determining whether or not HIPAA covers a record, then, is where the record resided when the rule took effect and if that institution was a covered or noncovered entity. The lack of an age limit on records is another patient protection. Concerns that ancestral diseases could be discovered and prevent the extension of health coverage to descendants led to the exclusion of a date limitation in the final rule and the applicability of the law to medical archives.[42]

Professional Ethical Considerations

Although HIPAA may often be the eight-hundred-pound gorilla in the room, professional ethical standards also mandate that archivists consider privacy issues. The ethical codes of the Society of American Archivists (SAA), the Association of Canadian Archivists (ACA), and the International Council on Archives (ICA) all dictate that the privacy of the individuals reflected within archival materials should be protected and weighed against the professional duty to provide access to materials.[43]

Ethical responsibilities to donors and those individuals reflected inadvertently within collections should be considered as well. The core values of archivists, as established by SAA, note the need to uphold donor expectations as expressed in donor contracts when providing access to records.[44] Although it is in the archival institution's best interest to limit restrictions as much as possible when accepting a collection, it is important to be sensitive to the privacy concerns of donors, particularly in relation to medical information. For example, in the past, the revelation of a teen pregnancy or substance abuse may have brought shame upon an individual and would have been a closely guarded family secret. A donor may have then requested that this or similar health information be access restricted.

[41] Lawrence, "Access Anxiety," 426–27.

[42] Lawrence, "Access Anxiety," 437–38.

[43] Society of American Archivists, *Code of Ethics for Archivists*, http://www.archivists.org/governance/handbook/app_ethics.asp, accessed 31 July 2011; Association of Canadian Archivists, *Code of Ethics*, http://www.archivists.ca/content/code-ethics, accessed 27 July 2011; International Council on Archives, "Reference Documents," *ICA Code of Ethics* http://www.ica.org/5555/reference-documents/ica-code-of-ethics.html, accessed 31 July 2011.

[44] Society of American Archivists, "Cores Value of Archivists," http://www2.archivists.org/statements/core-values-of-archivists, accessed 31 July 2011.

Reformatting for digitization and wider access than a reading room may pose a challenge for donor relations as well. A donor who was comfortable with transferring materials to an institution with a specific mission and researcher population may not have intended for the materials to be widely distributed on the Web. It is also important to note that donors may not be legally able to release for access all information included within a collection, especially if it contains the personal health information of others.[45]

Impact and Implications

It is easy to speculate how the current privacy legislation, which places a timeless restriction on materials, causes concern for the stewards of medical historical materials and was met with strong opposition by archivists working in these areas. It has made an indelible mark on the core archival responsibilities, such as collecting, processing, researcher accessibility, reference work, and digitization projects. It has also caused significant fear on the part of the archival profession and the research community about the legitimacy and fullness of the historical record.

In spite of all of these valid concerns, archivists who currently oversee health care special collections have come up with solutions for balancing privacy concerns with access demands and have created resources to share their experiences with others.[46] In conjunction with the legal advice of their institutions, they have developed policies and procedures for balancing these two seemingly contradictory professional responsibilities. These solutions differ from institution to institution and depend on a variety of contextual factors, such as whether the institution is a covered or noncovered entity under HIPAA, the risk-aversion level of the parent institution, and the nature of the records. These work-around efforts include the establishment of privacy boards to facilitate donor access, redaction of personally identifying information from publically available material, and placing time limits on the availability of sensitive material when appropriate.[47]

The Medical Heritage Center staff is currently working on the center's collection policies in conjunction with the Ohio State University Medical Center's privacy officer. Anecdotally, we have found that some of the guidelines for collection access that have resulted from HIPAA have been beneficial when

[45] Digital Library of Georgia, "Securing Permission to Digitize and Display Collections Online," http://dlg.galileo.usg.edu/AboutDLG/DisplayPermission.html?Welcome, accessed 31 July 2011.

[46] Science, Technology, and Health Care Roundtable and Archivists and Librarians in the History of the Health Sciences, "HIPAA Resource Page," http://www.library.vcu.edu/tml/speccoll/hipaa.html, accessed 31 July 2011.

[47] Wiener and Gilliland, "Balancing between Two Goods," 19–21.

establishing procedures that allow for access. For example, the Robert M. Zollinger, MD, Collection contains records with patient data that resulted from the groundbreaking research he and Dr. Edwin Ellison conducted in the process of their discovery of Zollinger-Ellison syndrome. Prior to the establishment of the Medical Heritage Center, the records were maintained by and access provided through Zollinger's office and the OSU Department of Surgery, as was the long-established, physician-protected tradition. Once the records were transferred to the archives with the entire collection, they were recognized for their historic value but sealed out of concern and lack of knowledge about how to best provide access. Under HIPAA and with the establishment of best practices, an access policy in accordance with the law and organizational policies was developed. It is the staff's hope that, as in this circumstance, the center can continue to carefully strike a balance between privacy and access.

Although room exists for future study of its impact on the historical record, the doom and gloom concerns that surrounded HIPAA's passage in 1996 appear largely not to have materialized. Special collections in the health sciences have not been shredded, sealed, or trashed en masse, and ingenuity and hard work have enabled archivists in these settings to continue to preserve and provide access to materials, albeit in different ways than in the past. Archivists working in these areas have also been active in advocating for changes to HIPAA that would make access to historical records less restrictive under the law. At the time of this writing, it appears some attention is being given to limiting HIPAA's impact on historical records.[48]

It is interesting to note that societal expectations and norms in regard to privacy concerns continue to shift and evolve and, perhaps, have never been more varied or less clear-cut. Social media sites like Facebook, Patients Like Me, and Caring Bridge have made it very easy for patients to share their personal medical information openly or with select individuals. The same individuals reading a Facebook feed, however, would be unable to call a hospital to obtain the most basic information about a patient. Thus, we live in a time where legislation has dictated very limited access to medical records based on technological concerns at the same time that technology has encouraged the public to share private information openly with others. How this information will be documented, preserved, and shared within the historical record in this environment has yet to be determined. One can be confident, however, that as in the past, archivists will be on the cutting edge of creating solutions to meet these ever-evolving challenges.

[48] Department of Health and Human Services, Office of the Secretary, *Federal Register, Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act. Proposed Rules* (14 July 2010), http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/nprmhitech.pdf, accessed 31 July 2011.

Conclusion

Charlene Nichols

In spite of the different and evolving access restrictions placed upon records in government, business, and medical archival settings, common threads can be found within the professional experiences of all three authors. Each archival professional has an abiding desire to ensure records are being collected and preserved, to acknowledge the value of their holdings to their institutions and to society in general, and to provide the most appropriate access possible to these collections. Carefully balanced with these desires, however, is the need to adhere to classified, propriety, and privacy restrictions on access that protect both individuals and institutions. In each case, these authors offer perspective, experience, and solutions to walk the fine line between access and restrictions in archival settings.

* * *

About the authors:

William C. Carpenter is a program analyst at the Information Security Oversight Office at the National Archives and Records Administration in Washington, D.C., where he works primarily with issues regarding declassification policy and with the Interagency Security Classification Appeals Panel. Before joining that office in 2007 he was an archivist specializing in declassification at the National Archives and in the Department of Defense. He has a PhD in history from George Mason University.

Charlene Nichols, CA, has been an archivist at the Jet Propulsion Laboratory in Pasadena, California, in the library, archives and records section since 2007. She has processed thousands of historic documents, including the records of the SEASAT project, the first space mission to use radar imaging to observe Earth's oceans. She received her MLS in 2007 and was certified by the Academy of Certified Archivists in 2010.

Sarah A. Polirer, CA, is currently the manager of Corporate Research at Cigna. She has been a practicing archivist for more than 20 years, the last 10 with Cigna. She received her MSLS from Simmons College in 1990 and became a Certified Archivist in 1991. Her career also includes government and university archival work.

Judith A. Wiener, MA, MLIS, is an assistant professor and the assistant director for collections and outreach at The Ohio State University Health Sciences

Library. One of her main responsibilities is serving as the head curator of the organization's Medical Heritage Center. She earned a BA in History at Wheeling Jesuit University, a MA in History with a concentration in public history at Wright State University, and a MLIS from Kent State University. She is currently a steering committee member for the Science, Technology, and Health Care Roundtable of SAA, the vice president of the Society of Ohio Archivists, and the president of the Ohio Academy of Medical History.