Children's Data Network

HIPAA

THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)
IMPLICATIONS FOR RESEARCH WITH ADMINISTRATIVE RECORDS

USC University of Southern California

STEPHANIE CUCCARO-ALAMIN, PHD
EMILY PUTNAM-HORNSTEIN, PHD

PLEASE NOTE

Although the authors have made every effort to provide information that is timely and accurate, HIPAA provisions are subject to change. Readers should consult their University Institutional Review Board or Human Subjects Committee for guidance before working with data regulated by HIPAA.

HIPAA – LEGISLATIVE HISTORY

First introduced as the Kennedy-Kassebaum Act, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Public Law 104-191 was passed by the 104th congress and signed into law by President Bill Clinton on August 21, 1996.[1] HIPAA was designed to address two separate health care issues: the portability of health care coverage, and the growing need to protect the privacy and security of individual health information with the emergence of electronic medical records. The Act's two titles relate directly to these issues. Title I– Heath Care Access, Portability, and Renewability - ensures that individuals can maintain their health insurance when changing employers. Title II – Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform - ensures the privacy and security of patient information, improves administrative accountability and efficiency through use of electronic medical records, and directs changes to medical liability laws.

Following the passage of HIPAA, it was anticipated that Congress would pass more comprehensive health care privacy legislation. When this failed to occur, responsibility for development of HIPAA's privacy regulations fell to the U.S. Department of Health and Human Services. Three important sets of DHHS regulations now govern health information privacy and security, the most notable of these being the HIPAA Privacy Rule.[2] The Privacy Rule established national standards regarding the use and disclosure of Protected Health Information (PHI) by "covered entities" - health care providers, health plans, and health care clearinghouses.

Secondary to the Privacy Rule are the HIPAA Security Rule[3] and the Administrative Simplification Rules.[4] The Security Rule established national standards for the secure handling of Protected Health Information (PHI) defined by the Privacy Rule. The Administrative Simplification Rules established guidelines for the standardization of electronic patient health information, code sets, and employer and provider identifiers. The U.S. Department of Health & Human Services, Office for Civil Rights (OCR) administers and enforces both the Privacy Rule and the Security Rule. The Department's Centers for Medicare & Medicaid Services are responsible for the administration and enforcement of the Administrative Simplification Rules.

PRIVACY IN HEALTH CARE: CLINICAL AND RESEARCH CONTEXTS

Although the right to privacy is not explicitly enumerated in the United States constitution, American society places a high value on privacy and confidentiality and our courts have consistently upheld this "right to privacy" in many realms. In the health care context, privacy is especially significant.

As an Institute of Medicine (IOM) review states "It is difficult to think of an area more private than an individual's health or medical information. Medical records can include some of the most intimate details about a person's life."[5] Confidential communication is the foundation of the doctor/patient relationship. Proper medical diagnosis and treatment is not feasible without disclosure of private information, especially in the treatment of mental health and substance abuse.[6] In addition to promoting effective communication in the health care context, confidentiality is also important to protect patients from potential discrimination in employment and the health insurance market based on disclosures of health related information, particularly genetic information.[7]

While the importance of privacy and confidentiality in the health care setting can clearly be demonstrated, there exists a unique tension between the privacy required for effective treatment of individuals and the waivers of privacy often needed to protect the public health through practice and research.[8]

Public health practice often involves the use, and disclosure of protected (private/personal) health information. Specifically, disclosures of private information are often required for preventing or controlling disease, injury, or disability.[9] Health care providers and public health authorities are exempt from privacy regulations under several circumstances. These include: reporting suspected child or domestic abuse to authorities,[10] notification of persons at risk of contracting or spreading a communicable disease,[11] when ensuring the quality or safety of a product regulated by the FDA,[12] or for workplace medical surveillance.[13] Such exempt disclosures have long been authorized under federal and state law and were incorporated into HIPAA.

The use of private information is also often required for effective public health and other population-level and prevention-focused research and evaluation efforts. Privacy in the research context has become more complex with the advent of electronic health data.[14] While such data hold great potential for improved disease surveillance and other epidemiological research, they also involve increased risk for disclosure and harm to individuals. HIPAA's attempts to address these challenges have far reaching implications for the practice of research.[15]

PRIVACY PROTECTIONS IN RESEARCH

Prior to HIPAA, use and disclosure of personal health information in the clinical and research contexts were governed separately. Specifically, privacy in the clinical context was governed by federal and state privacy laws which protected the sanctity of the confidential doctor/patient relationship.[16] With the advent of large scale electronic record keeping in the 1970's, some information practice regulations were added to state privacy laws. Eventually federal standards were adopted with passage of the Privacy Act of 1974,[17] which regulated the collection of personal data by the federal government and its contractors. Prior to HIPAA, the federal regulation of research activities had largely been restricted to the protection of human subjects. Such regulations came about in response to unethical research practices associated with the Tuskegee Syphilis study.[18] In 1979, The Belmont Report called on the federal government to implement guidelines regarding the ethical treatment of human subjects.[19] The report became the basis for the first federal legislation governing human subject research. Known as The Common Rule (45 CFR, Part 46), this legislation contains basic regulations governing the protection of human subjects in research supported by the federal government. Human subject protections governing clinical trials for drugs and medical devices are also found in the Food and Drug Administration's (FDA) Human Subject Protection Regulations (21 CFR Parts 50 and 56).[20]

The Common Rule defines human subjects as "a living individual about whom an investigator conducting research obtains data ... or identifiable private information."[21]

The rule's primary focus is protecting research subjects from harm by mandating informed consent procedures.

Recognizing that informed consent is not always feasible, the Common Rule does provide for researchers to access private health information without informed consent through approval by an Institutional Review Board.

Approval is contingent on certain risk criteria being met—that research involves no more than minimal risk to subjects and the waiver of consent does not harm subjects. Additionally, the research must meet what is known as the "practicability standard"—that it could not feasibly be conducted without the waiver of consent. Since its passage, the Common Rule has been amended to include special protections for research on pregnant women, fetuses, and neonates (Subpart B), prisoners (Subpart C), and children (Subpart D). Over 15 federal agencies have signed on to the Common Rule.[22]

THE HIPAA PRIVACY RULE

While the Common Rule represented a significant improvement in human subject protections for research, the rule has its shortcomings. First, it applies only to federal research on living subjects; increasingly research is conducted by both non- profit and for-profit entities which are not applicable under the rule. Second, the rule lacks detailed data confidentiality requirements. Specifically, it regulates how private health information is obtained rather than how it is protected once obtained.[23] These deficiencies became apparent with the exponential growth of electronic health data and concomitant increases in risk of disclosure of personally identifiable information. HIPAA attempted to remedy these gaps.

HIPAA AND COVERED HEALTH ENTITIES

The HIPAA Privacy Rule applies to "covered entities" who conduct standard health care transactions electronically.[24] HIPAA regulates the use and disclosure of Protected Health Information (PHI) by these entities. It allows for disclosure without individual authorization as part of health care treatment, payment and operations, but also regulates when

individuals must be informed of uses and disclosures of their protected health information (PHI) and their rights to access this information.[25]

Protected Health Information (PHI) is defined as "any information, including demographic information that relates to the past, present, or future physical or mental health or condition 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".[26]

Essentially, PHI is any information that identifies an individual or that could reasonably be used to do so (i.e., name, birthdate, social security number, address, etc.). When a covered entity discloses Protected Health Information for research or other purposes, a "minimum necessary" standard applies. Specifically, the entity must make reasonable efforts to limit PHI disclosure to the minimum necessary to accomplish the purpose of the specific use or disclosure.[27]

HIPAA AND THE REGULATION OF RESEARCH

HIPAA does not regulate research activities directly - rather it does so indirectly by regulating how and when health care providers can use and disclose protected health information for research.[28] Similar to the Common Rule, HIPAA allows for the use and disclosure of private health information when individual subjects have provided consent authorization.[29]

Recognizing the impracticality of obtaining consent authorizations from all individual subjects, particularly in research involving electronic health data, the Privacy Rule also permits the use and disclosure of PHI by covered entities without individual authorization for research purposes under limited circumstances.[30]

Specifically, the rule outlines four circumstances under which a waiver of the individual authorization (consent) may be granted. These include: (1) when an Institutional Review Board (IRB) or Privacy Board Approval has been obtained,[31] (2) in the context of the preparation of a research protocol where no data are removed from a covered entity,[32] (3) when the research involves the protected health information of decedents,[33] and (4) through De-identified Data Sets and Limited Data Sets with a Data Use Agreement.[34]

1. INSTITUTIONAL REVIEW BOARD (IRB) OR PRIVACY BOARD APPROVAL: **Three important criteria must be satisfied for an IRB or Privacy Board to approve an authorization waiver under the Privacy Rule. First, the research must involve no more than minimal risk to the privacy of individuals. To meet minimum risk standards researchers must show adequate plans for the protection of protected health information (PHI) from improper use and disclosure, plans for the destruction of identifiers consistent with conducting research (unless there is proper justification), as well as assurances against information re-disclosure to a third party. There are also two practicability standards which must be met—that the research could not practicably be conducted without the waiver and that the research could not be practicably carried out without the protected health information.**

2. PREPARATION FOR RESEARCH: **An authorization waiver may also be granted when the use or disclosure of PHI is exclusively for the preparation of a research protocol (for example, the recruitment of subjects) and no protected information will be removed from the premises of the covered entity.**

3. RESEARCH ON DECEDENTS: **A third scenario in which waivers may be granted is when the use or disclosure of PHI is exclusively for research on confirmed decedents.**

4. DE-IDENTIFIED AND LIMITED DATASETS: **Finally, PHI can also be released without individual authorization through the creation of either a de-identified data set or a limited data set with a data use agreement. Under the Common Rule, data are considered de-identified and available without a waiver if the researcher did not have direct access to key codes for re-identification. HIPAA's Privacy Rule outlines a stricter de-identification standard. Two methods of de-identification are allowable - Expert Determination and the Safe Harbor Method. Expert determination involves determination by a scientific/statistical expert that the risk of individual identification is small. The Safe Harbor Method involves the removal of 18 specific PHI identifiers to de-identify the data set (see Appendix A). Once de-identified, the data are no longer subject to the privacy rule. PHI can also be released through the creation of a limited data set and establishment of a data use agreement. Limited data sets may include information such as dates, city, state, and ZIP codes, and other unique identifying codes or characteristics. All data use agreements must include limits on use and disclosure for data recipients and subcontractors, as well as safeguards to pre-event re-identification of individuals.**

HIPAA stipulates an individual's right to accounting of disclosures of protected health information by covered entities.[35] Research disclosures for which individual consent was received or for a limited data set are exempted from this provision. For larger research studies (50 or more subjects) for which a waiver authorization has been granted, the Privacy Rule allows for simplified disclosures accounting.[36] Specifically, the covered entity can provide a list of all studies for which the patient's protected health information may have been disclosed along with the researcher's name and contact information. This accounting provision does not apply to limited data set disclosure.[37]

THE SECURITY RULE

The HIPAA Security Rule establishes national standards to protect "individually identifiable information a covered entity creates, receives, uses, or maintains in electronic form".[38] It does not apply to oral or written records. The Security Rule requires that covered entities implement appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and availability of electronic protected health information (e-PHI).[39] Covered entities must actively protect against (reasonable anticipated) threats to data security or integrity, unauthorized use and disclosures, and ensure compliance among their employees with these procedures.[40]

Required administrative procedures include established security management processes, data security personnel, personnel training, and ongoing procedural evaluation. Physical safeguards required by the rule include secure facility access and computer workstation and device security systems. The technical safeguards mandated by the rule include a permission control system that allows only authorized personnel access to electronic protected health information as well as system of audit controls to monitor this activity. Additionally, covered entities must have integrity controls to prevent damage or destruction of e- PHI, and finally transmission security procedures to ensure secure transmission of PHI over electronic networks. The Security Rule stipulates that covered entities must routinely review and modify their security procedures to ensure continual protection of electronic health information in an ever evolving technological environment.[41]

THE ADMINISTRATIVE SIMPLIFICATION RULES

The HIPAA Privacy and Security Rule was incorporated into the existing Administrative Simplification Rules in 2009 (45 CFR §160, §162, §164). The Administrative Simplification Rules also include transaction and code set standards, identifier standards, enforcement rules and breach notification rules. These rules are administered and enforced by the Centers for Medicare & Medicaid Services.

With the transaction and code set standards, as well as the identifier standards, HHS mandated the consistency of electronic patient health information. The transaction code sets are data content and format standards for health care data transactions.[42] They include: mandated code standards for physicians procedures (CPT-4), diagnosis and hospital inpatient procedures (ICD- 9),[43] items/supplies and non-physician services (HCPCS), National Drug Codes (NDC), and codes for Dental procedures (CDT).[44] HHS also adopted standards for unique identifiers for employers and providers, which must also be used in all transactions. The employer identified is the Employer Identification Number (EIN), issued by the Internal Revenue Service (IRS).[45] The National Provider Identifier (NPI) is a unique 10-digit number used to identify all covered entities (health care providers and all health plans and health care clearinghouses).[46]

The Administrative and Simplification Rules also include The HIPAA Enforcement Rule (45 CFR §160 Subparts C, D, E) and The HIPAA Breach Notification Rule, (45 CFR §164.400-414). The Enforcement Rule provides for civil penalties for HIPAA violations.[47] The Breach Notification Rule requires covered entities and their business associates to provide notification following a breach of unsecured protected health information.[48] The rules regarding HIPAA breaches were strengthened in 2009 with the passage of The Health Information Technology for Economic and Clinical Health (HITECH) Act (Public Law 111-5)[49] The act which served to promote use of health information technology, also included provisions that improved the civil and criminal enforcement of the HIPAA rules (Section 13401). HITECH defined different levels of infractions and

imposed stricter monetary penalties for electronic data breaches (Section 13402).[50]

By standardizing data content and formats as well as promoting safer and more secure electronic transmission, HIPAA's Administrative Simplification Rules have enhanced the quality of health care data available for research.

RECENT HIPAA MODIFICATIONS

Recently HHS further streamlined the HIPAA regulations with release of Ombibus HIPAA Rule Making: The Final Rule in January 2013. These updates modify HIPAA regulations to respond to technological and industry changes since its original passage. The final rule strengthened privacy protection by modifying HIPAA rules to make health care business associates liable for compliance, strengthened limits on the sale of health information and its use and disclosure for marketing and fundraising, expanded individual's rights to copies of their electronic PHI, modified notice of privacy practices for covered entities, modified the individual authorization (compound) and other requirements to facilitate research, and enhanced the existing HITECH rules for noncompliance. The final rule also adopted HITECH's higher civil penalties for HIPAA violations, modified breach notification procedures to be more objective, and significantly strengthened privacy protections against the use of genetic information for underwriting purposes. From a research perspective, the rule changes were beneficial as they streamlined the individual authorization process for the use and disclosure of personal health information for research purposes. Specifically, it allows for the use of compound authorizations for research, aligning HIPAA practices with The Common Rule[51]

RESEARCH IN THE HIPAA ERA

HIPAA attempts to balance an individual's right to privacy and confidentiality of their health information with public needs for research and knowledge advancement.[52] Importantly, it extends individual privacy protections to research not previously covered under the Common Rule. Additionally, HIPAA's privacy protections are flexible to respond to the ever evolving technological environment.

Technology has revolutionized health care delivery systems by improving both efficiency and communication. These data also hold great potential for improved disease surveillance and other epidemiological research.[53]

Although it cannot replace traditional experimental research, information based research has many advantages. It is often faster and less expensive than traditional research. Additionally, because it utilizes large amounts of data it can often find unexpected differences or control for factors that one cannot account for in more classical designs.[54] With this potential, however comes responsibility for both covered entities and researchers to safeguard patient's protected health information from unauthorized disclosures. While researchers have long operated with a mandate to protect human subjects, HIPAA regulations effectively legislate such best practice with electronic data. Figure 1 illustrates the general commonalities and differences between the waiver of authorization/consent between HIPAA and The Common Rule.

Some researchers argue that some HIPAA provisions unnecessarily constrain their ability to conduct effective research.[55] The National Research Council conducted a review of surveys of researchers regarding HIPAA's impact on research.[56] Regarding information based health research, researchers argue that it is expensive and time consuming to obtain IRB approval. Additionally, it can be difficult to conduct meaningful research with limited data sets and that once de-identified, data are often too limited to provide important demographic variables of interest. De-identified data also restrict researchers from conducting potentially important data linkages. Some also feel that HIPAA's disclosure provisions are confusing and often difficult to abide by. Health researchers continue to advocate for changes to the HIPAA privacy laws. Although HIPAA has increased obstacles to research using protected health information, these are by no means insurmountable. First, HIPAA covers only health data used or disclosed by covered entities. A large amount of administrative data for epidemiological and population based studies is not covered by HIPAA. Among others, these include Vital Statistics Data/Birth and Death Records, Child Maltreatment Data, Educational Data, Wage Data, Crime and Arrest Data, Adult Protective Services data, DMV Records and Census Data.

All are governed by either federal or state statutes and are not subject to HIPAA rules.

Secondly, when identifiable health information is required for research, HIPAA authorization waivers can be obtained through IRB and privacy board approval. Though this process can be time consuming, it is necessary to properly protect patient privacy and confidentiality.

Ultimately, HIPAA exists to provide reasonable protections for individuals against improper use and disclosure of their protected health information. Though HIPAA impacts research that utilizes health data, the constraints it imposes are not prohibitive for researchers and are critical to ensuring data privacy and confidentiality in the era of electronic health information.

AUTHORS

Stephanie Cuccaro-Alamin, PhD
Emily Putnam-Hornstein, PhD

ACKNOWLEDGEMENTS

This brief was published by The Children's Data Network, a university, agency, and community collaborative focused on the integration and application of data to inform programs and policies for children and their families. The Children's Data Network is funded by First 5 LA and the Conrad N. Hilton Foundation, housed at USC's School of Social Work, and includes a partnership with the California Child Welfare Indicators Project at UC Berkeley.

FOR MORE DETAILED GUIDANCE ON HIPAA, PLEASE CONSULT:

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Health Information Privacy
http://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html

HIPAA PRIVACY RULE AND PUBLIC HEALTH

Guidance from CDC and the U.S. Department of Health and Human Services
http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm

NATIONAL INSTITUTES OF HEALTH

Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule
https://privacyruleandresearch.nih.gov/pdf/HIPAA_Booklet_4-14-2003.pdf

APPENDIX A

Under the HIPAA Privacy Rule "identifiers" include the following:

1. Names
2. Geographic subdivisions smaller than a state (except the first three digits of a zip code if the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000).
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, and date of death and all ages over 89 and all elements of dates (including year) indicative of such age (except that such ages and elements may be aggregated into a single category of age 90 or older)
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code (excluding a random identifier code for the subject that is not related to or derived from any existing identifier)

SOURCE: U.S. Department of Health and Human Services. Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html#protected

REPORT END NOTES

[1] Full text of the law can be found at:
https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/Downloads/HIPAALaw.pdf
[2] 45 CFR §160 and §164 (Subparts A and E)-Final Privacy Rule, December 2000, later modified in August 2002.
[3] 45 CFR §160 and §164 (Subparts A and E)-Final Security Rule, February 2003.
[4] The Administrative Simplification Compliance Act (ASCA)
https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/downloads/ASCALaw.pdf
[5] Pritts, J.L. (2008). The Importance and Value of Protecting the Privacy of Health Information: The Roles of the HIPAA Privacy Rule and the Common Rule in Health Research. Washington, D.C. National Academy of Sciences, p. 5.
http://www.iom.edu/~/media/Files/Activity%20Files/Research/HIPAAandResearch/PrittsPrivacyFinalDraftweb.ashx
[6] ibid, p.4.
[7] ibid, p.4.
[8] Guidance from CDC and the U.S. Department of Health and Human Services* Section - The Privacy Rule and Public Health Research
http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm
[9] 45 CFR §164.512(b)
[10] 45 CFR §164.512(b)(1)(ii)
[11] 45 CFR §164.512(b)(1)(iv)
[12] 45 CFR §164.512(b)(1)(iii)
[13] 45 CFR §164.512(b)(1)(v)
[14] Guidance from CDC and the U.S. Department of Health and Human Services* Section - The Privacy Rule and Public Health Research.
http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm
[15] Department of Health and Human Services. Protecting personal health information in research --- understanding the HIPAA Privacy Rule. Department of Health and Human Services. Washington, D.C.: 2003. http://privacyruleandresearch.nih.gov/pr_02.asp
[16] Magnussen, R. (2004). The Changing Legal and Conceptual Shape of Health Care Privacy. The Journal of Law, Medicine, and Ethics, 681.
[17] 45 CFR §2555 and 5 U.S.C. § 552a
[18] U.S. Public Health Service (1932-1972). Tuskegee Study of Untreated Syphilis in the Negro Male.
http://www.cdc.gov/tuskegee/timeline.htm
[19] National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (1979). Belmont report: ethical principles and guidelines for the protection of human subjects of research Department of Health, Education and Welfare. Available at
http://www.med.umich.edu/irbmed/ethics/belmont/BELMONTR.HTM
[20] http://www.fda.gov/ScienceResearch/SpecialTopics/RunningClinicalTrials/default.htm
[21] 46 CFR §102(f)
[22] See http://www.hhs.gov/ohrp/humansubjects/commonrule/ for a list of Federal Agencies who have signed on to the Common Rule.
[23] Pritts, J.L. (2008).
[24] DHHS provides a quick decision tool for determining if an entity is covered under HIPAA. See
http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf
[25] 45 CFR §164
[26] 45 CFR §164
[27] 45 CFR §164.502(b), §164.514(d)
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/minimumnecessary.html
[28] Pritts, J.L. (2008).
[29] HIPAA does contain special provisions related to individual authorization for release of personal health information for research. Consent forms can: have no expiration date; be combined with consent for participation forms; be compound authorizations for conditioned parts of a study; and apply to future research purposes.

[30] 45 CFR §164.502(d) and §164.514(a)-(c).
[31] 45 CFR §164.512(i)(1)(i)
[32] 45 CFR §164.512(i)(1)(ii)
[33] 45 CFR §164.512(i)(1)(iii).
[34] 45 CFR §164.512(i)(1)(e)
[35] 45 CFR §164.528
[36] 45 CFR §164.528 (b)
[36] 45 CFR §164.514 (b (1&2)
[36] 45 CFR §164.514 (b (1&2)
[36] 45 CFR §164.514 (e)
[36] 45 CFR §164.528
[37] http://privacyruleandresearch.nih.gov/research_repositories.asp
[38] http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html
[39] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html
[40] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html
[41] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html
[42] http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/TransactionCodeSetsStands/index.html?redirect=/TransactionCodeSetsStands/02_TransactionsandCodeSetsRegulations.asp#TopOfPage
[43] ICD-10 - Scheduled for release October 1, 2014.
[44] http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/TransactionCodeSetsStands/CodeSets.html
[45] http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/EmployerIdentifierStand/index.html
[46] http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/NationalProvIdentStand/index.html
[47] http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/privacyrule/finalenforcementrule06.pdf
[48] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/
[49] 42 USC §17931 - http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf
[50] 42 USC §17932 - http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf
[51] http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
[52] http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/research/research.pdf p, 1.
[53] National Research Council. Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. Washington, DC: The National Academies Press, 2009, .p 130.
[54] ibid, p. 118
[55] ibid
[56] ibid