Privacy and Data Security Issues
Related to Electronic Health Information Exchange
By Behavioral Health Service Systems in California

Prepared for Anasazi Software, Inc.

by

Paul Litwak

Attorney & Counselor at Law

757-431-2020, plitwak@mac.com

May 13, 2011

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Anasazi Software, Inc. is developing enhancements to the Anasazi Software System to facilitate secure "point to point" electronic health information exchange by behavioral health programs.

Anasazi will act as a "Health Information Service Provider" (HISP) and provide authentication and other technical services to support secure information exchange in accordance with the National Health Information Network – Direct communications standards.[1] Anasazi will not maintain a repository of health records or provide patient record locator services. Health records transmitted through the HISP will be encrypted. Anasazi will not store copies of the health records transmitted through its HISP. For audit purposes, the HISP will record the fact that a

[1] The Nationwide Health Information Network (NHIN) is a set of standards, services and policies that enable secure health information exchange over the Internet. It is being developed under the auspices of the Office of National Coordinator for Health Information Technology (ONC) of the US Department of Health and Human Services. See http://healthit.hhs.gov/. ONC intends for the National Health Information Network to provide an interoperable infrastructure for secure information exchange as needed for patient care and population health. The core capabilities of NHIN include:

- Ability to find and retrieve healthcare information within and between health information exchanges and other organizations;
- Ability to deliver a summarized patient record to support patient care and to support the patient's health;
- Ability to support consumer preferences regarding the exchange of his or her information, including the ability to choose not to participate in the NHIN;
- Support secure information exchange;
- Support of a common trust agreement that establishes the obligations and assurances to which all NHIN participants agree;
- Ability to match patients to their data without a national patient identifier;
- Support of harmonized standards, which have been developed by voluntary consensus standards bodies for exchange of health information among all such entities and networks.

Since 2009 the NHIN Exchange specifications have been piloted by a group of federal agencies and non-federal entities, now known as the National Health Information Network Exchange. This group includes, among others, the Department of Defense, Department of Veteran's Affairs, the Social Security Administration, Kaiser Permanente, and state health information organizations (HIOs). NHIN-Exchange now supports the exchange of summary patient records for care coordination, including the Virtual Lifetime Electronic Record (VLER), exchange of records for Social Security disability determination purposes, and reporting to the CDC. One important aspect of NHIN Exchange is the ability to identify a common patient even without a common patient identifier and to search for and exchange records about patients. Exchanges between HIOs are not limited to "direct" messages or "known participants."

The NHIN Direct Project was launched in March 2010 to specify a simple, secure, scalable, standards-based way for participants to send authenticated, encrypted health information directly to known, trusted recipients over the Internet. See http://directproject.org/. The Direct Project focuses on the technical standards and services necessary to securely push content from a sender to a receiver and not the actual content exchanged. The Sender is responsible for the collection of patient consent where appropriate. The NHIN-Direct model introduces the logical concept of a HISP, or Health Information Service Provider that provides authentication or other technical services that are required for secure data exchange. Sending and receiving entities only transmit data that has been rendered indecipherable to unauthorized individuals, including the HISP, through the combination of standard use of S/MIME (signing and encryption) and the specification of NIST-recognized strong encryption algorithms.

transmission of records occurred, including the date, time, sender, recipient, and a patient identification number (not a social security number).

The first use of the software enhancements being developed by Anasazi and the Anasazi HISP will be in California in support of the Kern County behavioral health service system. The Kern County Mental Health Department shares the nation's interest in improving coordination of physical health, behavioral health, and social services to people diagnosed with mental illness or addictions, and in the use of health information technology to link services, advance the delivery of patient centered care, improve health care quality, and reduce health costs.[2]

A critical concern for all participants in electronic health information exchange is to ensure compliance with federal and state health rivacy and data security laws. This is a particular concern for mental health and substance abuse programs, which handle sensitive information and which must comply with strict rules governing disclosure of their records.

Anasazi is a leading provider of information technology and services to the behavioral health community. Michael Morris, founder and President of Anasazi, has led efforts to ensure that information technology supports the mission of behavioral health service systems in a manner that respects the privacy rights of individuals. He commissioned this memorandum, solicited helpful feedback about earlier drafts from colleagues at the Software and Technology Vendors Association, and contributed substantially to this work.

This memorandum provides an overview of applicable United States and California law and regulations governing the disclosure of individually identifiable health information for treatment purposes by California based behavioral health providers through electronic health information exchange.[3] It describes the laws and regulations governing disclosure of health information in any form (paper or electronic), electronic health information exchange, and data security. This

---

[2] The HITECH Act (Title XIII of the American Recovery and Reinvestment Act of 2009) states the national interest in promotion of the electronic use and exchange of health information to improve health care quality, reduce medical errors, advance the delivery of patient centered care, and reduce health costs resulting from inefficiency, medical errors, inappropriate care, duplicative care, and incomplete information. It also states the national interest in ensuring that that each patient's health information is secure and protected, in accordance with applicable law. See 42 USC 300jj-11.

The Substance Abuse and Mental Health Administration (SAMHSA), along with the Health Resources Services Administration (HRSA), and the National Council for Community Behavioral Health has championed integration of physical and behavioral health services. The national interest in this issue is reflected in section 2703 of the Patient Protection and Affordable Care Act (2010), which provides enhanced federal funding for two years to encourage State Medicaid programs to create "health homes" to ensure person centered coordination of physical health, behavioral health, and social support services for people with chronic illnesses, including people with serious mental illness and people with substance abuse disorders and co-occurring asthma, diabetes, heart disease or other health conditions. One of the specifications for the health home program is the use of health information technology to link services to the extent feasible. See CMS State Medicaid Director Letter 10-024.

[3] Please note that while I have expertise in health information privacy law, I am not licensed to practice law in California. My analysis of California law may differ from that of California authorities.

memorandum does not attempt to catalog the myriad federal or state rules governing use or disclosure of health information for purposes other than treatment.

Please note that federal laws and regulations (such as HIPAA and 42 CFR Part 2) create minimum national standards for the privacy and security of health information. A State may have additional or more restrictive privacy or data security requirements. It will be necessary to supplement this analysis when the Anasazi HISP is made available in states other than California.

Anasazi is also developing software enhancements to enable the creation of Personal Health Records for individuals served by behavioral health programs. This memorandum does not address legal issues peculiar to the creation of Personal Health Records (such as limitations on disclosure of clinical laboratory results to individuals).

This memorandum refers to any entity that provides services to facilitate the electronic exchange of information among healthcare providers and which has access to individually identifiable health information as a "Health Information Exchange Organization" or "HIEO". This includes "Federated" or "Repository" model Health Information Organizations ("HIOs" or "RHIOs") that serve geographic regions, enable participating providers to identify and gain access to individual health records, and enable participants to connect to the National Health Information Network.[4] It would include an HISP that has access to individually identifiable health information.

Essential points made in this memorandum are as follows:

<u>Disclosure of Health Information for Treatment Purposes</u>

- California law creates an individual right to privacy, including the right to control disclosure of confidential information. The right to privacy is not absolute. Disclosures are permitted when authorized by law.

- Both HIPAA and the California Confidentiality of Medical Information Act permit disclosure of individually identifiable health information to treatment providers and health plans for the purposes of treatment. Individual consent is not required.

- Disclosure of mental health or HIV/AIDS records for treatment purposes without individual consent is permitted in California. There are provisions of law that restrict disclosure of outpatient mental health records for purposes other than treatment.

- Individuals in California have the right to sue for violations of the privacy rights granted by the State Constitution and the Confidentiality of Medical Information Act. Statutory remedies

[4] A "Federated Model" HIO provides record locator services and enables participating providers to identify, review, and obtain information from health records stored by other participating providers. A "Repository Model" HIO have obtains and stores copies of health records, maintains a master patient index and record locator service, and makes those records available to participating providers. "Hybrid Model" HIOs do both. An HIO may also provide HISP services. HIOs are sometimes referred to as "Health Information Exchanges" or "HIEs".

include punitive damages and payment of attorney's fees and court costs.

- Under federal law and regulations, substance abuse program records may not be disclosed for treatment purposes without a patient's written consent, except in case of medical emergency.

- With limited exceptions, patient consent is required before a federally assisted substance abuse program may provide any patient identifying information to a third party for any purpose. The required elements of a consent are set forth at 42 CFR 2.31. The consent must identify name of the patient, the program or person permitted to make the disclosure, the recipient of the record, the purpose of the disclosure, and how much and what kind of information will be disclosed. It must state that the consent may be revoked, and establish a date or event upon which it will expire.

- When substance abuse program records are disclosed with patient consent, a written notice must be sent to the recipient of the information advising the recipient that the record is protected by 42 CFR Part 2, that the recipient is obligated to follow those regulations, and that re-disclosure of the information provided is prohibited without the express permission of the patient or as permitted by 42 CFR Part 2. The form of that notice is specified at 42 CFR 2.32. The obligation of the recipient to manage information received from a substance abuse program in accordance with 42 CFR Part 2 limits the ability of primary care providers and other users of certified electronic health records to automate the process of receiving, consolidating, and making "meaningful use" of health information in the manner contemplated by the Center for Medicare and Medicaid Services and ONC.

- Substance abuse program records may be disclosed without patient consent in a medical emergency. But immediately following the disclosure, the disclosing organization must document the disclosure in the patient's record, setting forth the identity of the medical personnel and health care facility that received the record, the name of the individual making the disclosure, the date and time of disclosure, and the nature of the emergency. Health Information Exchange Organizations that support "break the glass" procedures to enable emergency disclosures without consent must be able to support this requirement.

- It seems to be premature to attempt to implement granular controls over disclosure of specific classes of data included within an individual clinical record. A "Privacy and Security Tiger Team" assembled by the Office of the National Coordinator for Health Information Technology recently examined this issue and reported that while granular consents are desirable, there is no current standard for implementation of such controls in EHR systems, and that the vast majority of individuals who are offered the opportunity to exercise granular consent control refuse the opportunity and give a general consent to disclose the entire health record.

Disclosures to and through Health Information Exchange Organizations

- The California Office of Health Information Integrity recently proposed regulations that require the affirmative consent of individuals to the electronic exchange of health information, including direct exchange (NHIN-Direct) or disclosure through an intermediary Health Information Organization. This consent to electronic information exchange is required in addition to any other required legal required authorization permitting one health care provider to disclose health records to another. The same proposed regulations require that individuals be provided with information regarding electronic health information exchange before consent is provided. They permit electronic health information exchange only for the purposes of treatment, mandatory public health reporting, and reporting compliance with the federal "Meaningful Use" rules.

- The NHIN Direct standards are based on an assumption that the sending provider will obtain patient consent to disclosure of health information. NHIN Direct transactions may bypass Health Information Exchange Organizations.

- States have established varying requirements for patient consent to disclosures of health information by providers to HIEOs. Many of these standards seem to be based on assumptions that the HIEO will operate on a Federated or Repository Model and retain individually identifiable health information. Some states permit disclosure of a patient record to an HIEO without patient consent. Others give individuals the right to "opt-in" or "opt-out" of such disclosures of their records to or through the HIEO.

- Health Information Exchange Organizations may only disclose health information to third parties as permitted by law.

- The policies and procedures used by some NHIN Exchange Participants and Health Information Exchange Organizations to obtain patient consent to disclose health information to third parties do not address the requirements of 42 CFR Part 2. This limits the ability of substance abuse programs that are subject to those regulations to participate in HIEO networks.

- Veteran's Administration records are not subject to 42 CFR Part 2. But it is worth noting that the Veteran's Administration Health System in San Diego is implementing a "Virtual Lifetime Electronic Record" and using VA Form 10-0485 to obtain patient authorization of disclosure for treatment purposes of all VA health records (including sensitive records such as treatment for alcohol or drug abuse) "to the communities that are participating in the Nationwide Health Information Network". The recipient of the record is not specified.

- In New York State, the eHealth Collaborative has established Privacy and Security Policies and Consent Forms for use by Regional Health Information Organizations and their participants. There, the individual permits a specific health care provider to receive any health information that may be available through the RHIO. This includes sensitive information such as records of mental health or substance abuse treatment, HIV status, and genetic testing results. SAMHSA has not given an opinion as to whether such a form of permission to receive health records meets the

requirements of 42 CFR 2.31, or whether it would be considered an insufficient general authorization for release of medical information.

Regulatory Environment

- Pursuant to the HITECH Act, Health Information Exchange Organizations are a business associate of the provider organizations that use the HIEO to facilitate the exchange of data. HIPAA covered entities that enter an appropriate Business Associate Agreement with the HIEO may disclose patient records to the HIEO without individual consent or authorization.

- A Health Information Exchange Organization could also be considered a "Qualified Service Organization" that provides services to federally qualified substance abuse programs. This would permit a substance abuse program that enters an appropriate Qualified Services Organization Agreement with the HIEO to disclose records to the HIEO. It would not permit the HIEO to re-disclose the record to third parties.

- The HITECH Act obligates business associates to follow the requirements of the HIPAA Security Rule and most of the requirements of the HIPAA Privacy Rule.

- Violations of HIPAA and the HITECH Act are punishable by substantial civil monetary penalties. An organization that violates the HIPAA rules as a result of "willful neglect" of its regulatory responsibilities is subject to severe penalties.

- The California Office of Health Information Integrity is empowered to enforce California health privacy and data security laws and to seek civil penalties against persons and organizations that violate those laws.

Obligations to Individuals

- HIPAA covered entities and business associates will be obligated to provide an accounting of all disclosures of protected health information.

- The HITECH Act and regulations enacted there under require HIPAA covered entities and vendors of personal health records to provide notice to affected individuals, the public and the federal government of a breach or unauthorized disclosure of non-secure protected health information. These requirements do not apply if data is encrypted. A HIPAA covered entity or business associate (including an HIEO) that does not comply with the Breach Notification Rule is subject to civil monetary penalties.

Legal Relationships

- An HIEO that participates in the National Health Information Exchange Network will be required to enter the Data Use and Reciprocal Support Agreement ("DURSA") agreement published by the National Health Information Network Cooperative ("NHIN").

- There is no required form for an HISP to HISP agreement between organizations that provide technical services to support NHIN-Direct transactions and which do not have access to individually identifiable health information.

- An HIEO should enter agreements with participating providers that include the terms of a HIPAA Business Associate Agreement and a 42 CFR Part 2 Qualified Services Organization agreement.

Development Considerations

- Health Level Seven International, Inc. (HL7) is a not-for-profit, ANSI-accredited standards developing organization. HL7 has published a draft Domain Access Model ("DAM") for Consent Directives and for Privacy Policies governing consent to disclosure of health information. This DAM is primarily a concept paper for a proposed mechanism of automating consent directives and contains some concepts, such as categorization of data, which may be instructive.

Model Consent Form

- This memorandum includes a Model Consent Form that includes the elements required by 42 CFR 2.31, the California Confidentiality of Medical Information Act, and proposed California regulations governing electronic health information exchange. The form permits electronic exchange of health information held by one identified provider to another identified provider for treatment purposes only. It does not permit disclosure of psychotherapy notes. The form is written in a manner that limits use of free text or incalculable dependencies so as to facilitate automation of the process of recording and tracking permission to disclose records.

- Please note that it would be possible to create a 42 CFR Part 2 compliant consent form that permits disclosure of a substance abuse program record to a set of identified recipients and that permits those recipients to re-disclose the information in the record to one another. This would facilitate electronic health information exchange among an identifiable and unchanging group of providers. But it would not be a practical approach to consent directive management in the context of the National Health Information Network because it is not scalable beyond limited communities of identified providers.

(Continued on Following Page)

I. HEALTH CARE PRIVACY LAW

1.1 Introduction

Privacy rights in the United States are defined by a complex patchwork of federal and state laws and regulations, court orders and administrative decisions.

While a "right to privacy" is not enumerated in the United States Constitution, the Supreme Court of the United States has found that individuals have constitutionally protected privacy interests related to health care decision-making and disclosure of health information.

Rules of evidence in United States and state courts establish privileges against disclosure of information received in confidence by physicians and other health care providers. These rules of evidence are consistent with the ethical principles of the health professions, which are described below.

The United States Congress has enacted laws for the protection of the privacy of records held by the US government, and any number of generally applicable statutes that restrict unauthorized use or disclosure of particular kinds of records, ranging from video rental records to child protection reports.

Title II of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the regulations issued there under by the US Department of Health and Human Services establish minimum national standards for health care privacy. But those standards are not universally applicable, and are superseded by federal and state laws that give individuals greater control over use and disclosure of their health information. The federal government has enacted a number of such "more stringent" statutes and regulations, particularly 42 CFR Part 2, which tightly restricts use and disclosure of records of federally assisted substance abuse treatment programs.

Each state has enacted laws and regulations governing use and disclosure of health information. These laws vary from state to state. State law often addresses subjects that are not addressed by federal law, such as protection of records of mental health treatment or records of diagnosis and treatment of HIV or AIDS. In addition, states have varying laws and procedures for consumer control of disclosures of health information to and through health information exchange organizations.

1.2 The Expectation of Privacy

In the Preamble to the Final HIPAA Privacy Rule, the Department of Health and Human Services begins a discussion entitled "The Importance of Privacy" by stating unequivocally "Privacy is a fundamental right."[5]

Legal scholars argue about the nature of a "right of privacy". But there is no doubt that we all expect clinical professionals and health care facilities to keep our personal health information confidential, to be disclosed only as permitted and as necessary.

DHHS emphasized the importance of this expectation, stating:

...[P]rivacy is necessary for the effective delivery of health care, both to individuals and to populations...[It] is a necessary foundation for delivery of high quality health care...[T]he entire health care system is built upon the willingness of individuals to share the most intimate details of their lives with their health care providers...

More than anything else, the relationship between a patient and a clinician is based on trust. The clinician must trust the patient to give full and truthful information about their health, symptoms, and medical history. The patient must trust the clinician to use that information to improve his or her health and to respect the need to keep such information private...

Individuals cannot be expected to share the most intimate details of their lives unless they have confidence that such information will not be used or shared inappropriately. Privacy violations reduce consumers' trust in the health care system and institutions that serve them. Such a loss of faith can impede the quality of the health care they receive, and can harm the financial health of health care institutions[6]

Even while stressing the importance of privacy, DHHS recognized that individuals do not have an absolute right to control the disclosure of their health information.[7] Perhaps more importantly, DHHS acknowledged that individuals often benefit from disclosure of their health information.

Patients also benefit from the disclosure of such information to the health plans that pay for and can help them gain access to needed care. Health plans and health care clearinghouses rely on the provision of such information to accurately and promptly process claims for payment and for other administrative functions that directly affect a patient's ability to receive needed care, the quality of that care, and the efficiency with which it is delivered.[8]

---

[5] 65 Federal Register 82464

[6] 65 Federal Register 82467-82468

[7] "Individuals' right to privacy in information about themselves is not absolute..." 65 Federal Register 82464.

[8] 65 Federal Register 82467

1.3 Professional Ethics and Patient Privacy

The expectation of privacy described by DHS is reflected in the code of ethics of every clinical profession. For example:

The Code of Medical Ethics of the American Medical Association states:

The patient has the right to confidentiality. The physician should not reveal confidential communications or information without the consent of the patient, unless provided for by law or by the need to protect the welfare of the individual or the public interest.[9]

The need to maintain patient confidentiality is particularly important to professionals involved in delivery of mental health or substance abuse treatment services. The ethical codes of professional associations in this field reflect that concern. For example:

The American Psychiatric Association includes specific guidance regarding application of the ethical principles of the American Medical Association in psychiatric practice. A detailed statement about the obligation of psychiatrists to keep patient information confidential can be found at http://www.psych.org/apa_members/ethics_princpl.cfm.

The Code of Ethics of the National Association of Social Workers very specifically describes the obligation of social workers to protect client confidentiality. It can be found on the Internet at http://www.naswdc.org/pubs/code/standard1.htm.

The American Psychological Association Code of Ethics with regard to privacy is being reviewed, and a revised version will be published in the next year or two. The current version can be found at http://www.apa.org/ethics/code.html#Privacy.[10]

The Code of Ethics of NAADAC, the Association for Addiction Professionals, includes particularly specific and unequivocal principles regarding the professional obligation to keep patient information confidential. The NAADAC Code even includes a requirement that members use appropriate security technology to safeguard electronic communications. The

---

[9] "Fundamental Elements of the Patient-Physician Relationship", point 4, found at http://www.ama-assn.org/ama/pub/category/2510.html

[10] While the APA Code of Ethics clearly states that principle that psychologists have an obligation to keep patient information confidential, the Code allows disclosure without Consent in some circumstances. At section 5.02, the APA Code of Ethics states: "Maintaining Confidentiality. Psychologists have a primary obligation and take reasonable precautions to respect the confidentiality rights of those with whom they work or consult, recognizing that confidentiality may be established by law, institutional rules, or professional or scientific relationships." But at section 5.05 (a), the Code states: "*Psychologists disclose confidential information without the consent of the individual only as mandated by law, or where permitted by law for a valid purpose, such as (1) to provide needed professional services to the patient or the individual or organizational client, (2) to obtain appropriate professional consultations, (3) to protect the patient or client or others from harm, or (4) to obtain payment for services, in which instance disclosure is limited to the minimum that is necessary to achieve the purpose*". (Emphasis added.)

NAADAC Code can be found at http://naadac.org/ethics.htm.

1.4 Privileged Communications

The law recognizes the public interest in promoting confidential communications in clinical relationships. The rules of evidence for judicial proceedings create "testimonial privileges" that protect confidential communications between individuals and clinical professionals.

In *Jaffee v Redmond*[11], the US Supreme Court held that the Federal Rules of Evidence create a privilege that applies to communications between a patient and a clinical social worker. A police officer shot and killed a man she believed to be attacking another person with a butcher knife. The police officer received counseling from a clinical social worker to help her deal with the trauma of the event. The estate of the dead man then sued the police officer and demanded information from the social worker. The police officer objected to such testimony on the grounds that her communications with the social worker were confidential and privileged.

The Supreme Court found that the federal rules of evidence recognize that communications between patients and psychotherapists are privileged. For this reason, the social worker could not be compelled to reveal information obtained during psychotherapy sessions with the police officer. The Court said:

> *...We start with the primary assumption that there is a general duty to give what testimony one is capable of giving, and that any exemptions which may exist are distinctly exceptional...*
>
> *Like the spousal and attorney-client privileges, the psychotherapist-patient privilege is "rooted in the imperative need for confidence and trust." ... Effective psychotherapy, by contrast, depends upon an atmosphere of confidence and trust in which the patient is willing to make a frank and complete disclosure of facts, emotions, memories, and fears. Because of the sensitive nature of the problems for which individuals consult psychotherapists, disclosure of confidential communications made during counseling sessions may cause embarrassment or disgrace. For this reason, the mere possibility of disclosure may impede development of the confidential relationship necessary for successful treatment...*
>
> *The psychotherapist privilege serves the public interest by facilitating the provision of appropriate treatment for individuals suffering the effects of a mental or emotional problem. The mental health of our citizenry, no less than its physical health, is a public good of transcendent importance.*[12]

[11] 518 U.S. 1, 116 S.Ct. 1923 (1996)

[12] 116 S.Ct. 1928-1929

1.5 The US Constitutional "Right to Privacy"

The US Constitution and Supreme Court decisions that interpret the Constitution establish certain fundamental rights that individuals have relative to the government.

Supreme Court Justice Louis Brandeis is often credited with expressing the existence of a Constitutional "right to be let alone". In 1928, he wrote a dissenting opinion in a criminal case involving a warrantless search and seizure, stating:

The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men.[13]

One of the clearest expressions of the belief that there is a Constitutional right to privacy comes from *Roe v Wade*, the 1973 decision of the US Supreme Court.[14] Regardless of one's views about the wisdom of the *Roe v Wade* decision, the Court's description of the right to privacy is worth noting:

The Constitution does not explicitly mention any right of privacy. In a line of decisions, however, going back perhaps as far as [1891], the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution. In varying contexts, the Court or individual Justices have, indeed, found at least the roots of that right in the First Amendment, in the Fourth and Fifth Amendments, in the penumbras of the Bill of Rights, in the Ninth Amendment, or in the concept of liberty guaranteed by the first section of the Fourteenth Amendment. These decisions make it clear that only personal rights that can be deemed 'fundamental' or 'implicit in the concept of ordered liberty' are included in this guarantee of personal privacy.

Where certain "fundamental rights" are involved, the Supreme Court has held that regulation limiting these rights may be justified only by a "compelling state interest, and that legislative enactments must be narrowly drawn to express only the legitimate state interests at stake".[15]

The theme of balancing the individual's right to privacy against government interests is repeated again and again in Constitutional litigation. The case law can be confusing because the "right to

---

[13] Olmstead v. U.S., 48 S.Ct. 564 (1928)

[14] Roe v. Wade, 410 U.S. 113, 93 S.Ct. 705 (1973).

[15] 410 U.S. at 152-153; 93 S.Ct. at 726-727. Citations omitted. Note that there are members of the US Supreme Court who believe that the Court overstepped its bounds in Roe v Wade by reading into the Constitution a "right to privacy". Justices Scalia, Thomas, and former Chief Justice Rehnquist all believe that unless the Constitution specifically describes individual rights, States retain the power to enact laws to regulate the conduct of residents. See the dissenting opinions in Stenberg v Carhart, 530 U.S. 914, 120 S.Ct. 2597 (2000).

privacy" really describes several four different kinds of rights. And the standard used to measure the legitimacy of government's interest in intruding upon those rights varies. Broadly stated, the "right to privacy" includes:

- The right to Freedom of Expression, Association, and Religion;
- The right to freedom from Unreasonable Searches and Seizures;
- The right to make Fundamental Decisions;
- The right to control Disclosure of Personal Information. [16]

In the context of health privacy, the Constitutional question is whether an individual has the right to control disclosure of personal health information to the government. Judicial recognition of this right is based on an analysis of whether government conduct in seeking disclosure of personal information is reasonable under the circumstances.

Contrast the Supreme Court's decisions in *Whalen v Roe*[17] and *Ferguson v City of Charleston*[18]. In Whalen, the Court found that a New York law requiring pharmacies to submit information about the prescription of certain drugs to the State Department of Health did not violate the Constitutional rights of individuals whose records were disclosed. The Court said:

... Disclosures of private medical information to doctors, to hospital personnel, to insurance companies, and to public health agencies are often an essential part of modern medical practice even when the disclosure may reflect unfavorably on the character of the patient. Requiring such disclosures to representatives of the State having responsibility for the health of the community, does not automatically amount to an impermissible invasion of privacy.[19]

In *Ferguson*, the Court found that the City of Charleston had violated the Constitutional rights of individual hospital patients when it released the results of drug tests of pregnant women to criminal law enforcement authorities. The key factor for the Court was that the primary purpose for gathering the information was criminal prosecution. In other cases, the court had upheld the release of drug testing information because a "special need" of government justified the action. Examples of appropriate disclosures included drug tests of railway employees involved in train accidents and Customs Service employees seeking promotion to sensitive positions. But in *Ferguso*n, the Court said:

...The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with non-medical personnel without her consent...There are some circumstances in which state hospital employees, like other citizens, may have a duty to provide law enforcement officials with evidence of criminal conduct acquired in the course of

---

[16] Fred H. Cate, Privacy in the Information Age, Brookings Institution Press, 1997.

[17] 429 U.S. 589, 97 S.Ct. 869 (1977)

[18] 532 U.S. 67, 121 S. Ct. 1281 (2000)

[19] 97 S.Ct. at 878.

routine treatment (citing laws requiring reporting of suspected child abuse or neglect)…

In this case…the central and indispensable feature of the policy from its inception was the use of law enforcement to coerce the patients into substance abuse treatment. This fact distinguishes this case from circumstances in which physicians or psychologists, in the course of ordinary medical procedures aimed at helping the patient herself, come across information that under rules of law or ethics is subject to reporting requirements…(citing ethical codes and an Arkansas law requiring reporting where "a patient threatens to inflict bodily harm to another person or to him or herself and there is a reasonable probability that the patient may carry out the threat").[20]

1.6 Federal Privacy Statutes – Generally

Congress has enacted a number of statutes about privacy of personal information.

Some of these statutes regulate US government use and disclosure of personal information. For example, the Privacy Act of 1974, 5 USCA 552a prohibits the disclosure of personally identifiable information maintained by government agencies without the consent of the subject individual, subject to twelve codified exceptions. The Freedom of Information Act, 5 USCA 552, requires federal agencies to make government records available to the public, but it prohibits disclosure of personnel, medical, or similar files, the release of which would constitute an unwarranted invasion of personal privacy.

Other statutes apply to the general public and protect personal information that is not directly related to health care, such as records of video rentals[21], motor vehicle records[22], and financial records[23].

A few federal statutes and regulations establish standards for use or disclosure of health information. They include:

- *HIPAA*[24] and the HIPAA Privacy Rule[25], which establishes minimum national standards for privacy of health information, discussed in detail at section 1.7, below.

- The *HITECH Act*, enacted as part of the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5), extends direct application of the HIPAA Privacy and Security Rules to "business associates" of HIPAA covered entities, increases

[20] 121 S.Ct., 1288-1290

[21] Video Privacy Protection Act of 1988, 18 USCA § 2710

[22] Driver's Privacy Protection Act of 1994, 18 USCA §§ 2721 et. seq.

[23] Gramm-Leach-Bliley Act (The Financial Services Modernization Act of 1999), 15 USCA 6801 et. seq.

[24] Pub. L. No. 104-191 (42 U.S.C. § 1320d-2)

[25] 45 C.F.R. Part 160 and Subparts A and E of Part 164

penalties for HIPAA violations, and strengthens enforcement mechanisms.

- 42 U.S.C. § 290dd- 2 and 42 C.F.R. Part 2, which govern use and disclosure of records of federally assisted substance abuse programs, discussed in detail in section 1.9.

- *Medicaid Privacy Requirements*, 42 U.S.C. 1396a(a)(7), 42 C.F.R. §§ 431.300-307, which restrict the use or disclosure of information concerning Medicaid applicants and recipients to purposes directly connected with the administration of the State Medicaid Plan.

- *Genetic Information Nondiscrimination Act of 2008* (GINA), Pub. L. No. 110- 233, which prohibits discrimination by group health plans and employers on the basis of genetic information.

- The *Clinical Laboratory Improvement Amendments (CLIA) (1988),* 42 U.S.C. § 263a, 42 C.F.R. Part 493, assures quality standards for all laboratory testing to ensure the accuracy, reliability and timeliness of patient test results. Certified labs may disclose test results or reports only to those treating the patient, referring laboratories, and "authorized persons" who are empowered by State law to order laboratory tests or receive laboratory test results.

- The *Family Educational Rights and Privacy Act (FERPA)* (1974), 20 U.S.C. § 1232g, 34 C.F.R. Part 99 protects the privacy of educational records, including health records maintained by educational institutions.

A more complete listing of federal privacy statutes can be found at the website of the Office of the National Coordinator for Health Information Technology, at http://healthit.hhs.gov.[26]

1.7 HIPAA

1.7.1 Background; Applicability

"HIPAA" refers to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-91). Title II of the act includes "Administrative Simplification" provisions intended to promote efficiency in the health care system and reduce administrative costs by "encouraging the development of a health information system through the establishment of standards and requirements for the electronic maintenance and transmission of certain health information".[27]

As required by the HIPAA statute, the Secretary of Health and Human Services has enacted rules to establish national standards for a host of electronic transactions between health plans and health care providers, minimum national standards for protection of the privacy of individually identifiable health information exchanged in those transactions (the Privacy Rule), and national

[26] See also The Privacy Law Source Book 2001, by Marc Rotenberg of the Electronic Privacy Information Center. http://www.epic.org/bookstore/pls2001/

[27] PL 104-91, § 261.

standards for security of health information systems (the Security Rule).

The "covered entities" to which HIPAA applies are:

- Health Plans – This term includes any individual or group plan that provides, or pays the cost of, medical care. This specifically includes Medicare, Medicaid, health insurance programs, HMOs, employer sponsored group health plans covered by ERISA, military health programs, CHAMPUS, the Federal Employees Health Benefit Plan, and others;[28]

- Health Care Clearinghouses - broadly defined to mean organizations that process non-standard data elements of health information into standard data elements; and

- A Health Care Provider who transmits any health information in electronic form in connection with a HIPAA transaction.[29]

The HITECH Act requires "business associates" of covered entities to comply with the HIPAA Security Rule, and most provisions of the HIPAA Privacy Rule.[30] It also requires that Health Information Organizations, E-Prescribing Gateways, organizations that facilitate electronic data exchange for covered entities, and vendors of Personal Health Records that make such records available to covered entities be considered to be business associates of those covered entities.[31] The current HIPAA rules define the term "business associate" as follows:

> *A "business associate" is: (i) a person or organization that, on behalf of a covered entity or an organized health care arrangement, performs functions involving the use or disclosure of individually identifiable health information, including claims processing, data analysis, data processing or administration, utilization review, quality assurance, billing, benefit management, re-pricing, or other functions regulated by the HIPAA rules, or (ii) a person or organization (other than a member of the workforce) that provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to a covered entity or organized health care arrangement, and receives protected health information in the course of performance of those services.*[32]

The Department of Health and Human Services has issued a Notice of Proposed Rulemaking[33]

---

[28] The full statutory definition of "health plan" can be found at 42 USCA 1320d (5). This definition is incorporated into and expanded upon slightly in the HIPAA regulations, at 45 CFR 160.103.

[29] 42 USC 1320d-1(a)

[30] HITECH Act 13401 and 13404.

[31] HITECH Act 13408

[32] 45 CFR160.103. Note that health care providers that share protected health information for treatment purposes are not "business associates" because neither is performing a "business associate" function for the other. The Privacy Rule permits disclosures for treatment purposes between health care providers without a business associate agreement. See Sec. 164.502(e)(1).

[33] 75 Federal Register 40868 (July 14, 2010)

that expands the regulatory definition of "business associate" to conform to the requirements of the HITECH Act and the Patient Safety and Quality Improvement Act of 2005 (PSQIA), 42 U.S.C. 299b-21, et seq. The proposed definition reads as follows:

Business associate: (1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

(A) A function or activity involving the use or disclosure of protected health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42CFR 3.20, billing, benefit management, practice management, and repricing; or

(B) Any other function or activity regulated by this subchapter; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person

.

(2) A covered entity may be a business associate of another covered entity.

(3) Business associate includes:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) Business associate does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

Note that subsection 3(iii) provides that "business associate" includes subcontractors of other business associates. The intent of this section is to make business associates responsible for the actions of their subcontractors. Business associates will be required to enter business associate agreements with any subcontractor that will have access to protected health information. These business associate agreements must conform to the requirements of the HIPAA rules and the HITECH Act.

If Anasazi will have access to protected health information in the course of operation of the health information exchange, it will be a business associate of every covered entity (or business associate) that uses the health information exchange to transmit protected health information. The provider organizations that use the exchange are not considered to be business associates of covered entities to which they send information for treatment purposes. Even though provider-to-provider communications through the exchange will be encrypted, Anasazi will be considered to have access to protected health information if it maintains a patient locator service as part of the operation of the exchange.

1.7.2 Use and Disclosure of Protected Health Information

The HIPAA Privacy Rule establishes minimum national standards for disclosure of "protected health information" by covered entities, and by business associates acting on behalf of covered entities.

"Protected health information" refers to any "individually identifiable health information" in any form that is "... created or received by a [covered entity] and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care, or ... payment for the provision of health care to an individual".

The Privacy Rule says that covered entities may only use protected health information (internally) and disclose that information (to third parties) as permitted by the rule.[34] This simple statement is

[34] 45 CFR 164.502(a)

followed by detailed standards and implementation specifications that govern use and disclosure in various circumstances.

Unless an exception is stated in the rule, covered entities are required to obtain written permission (or "authorization") from the subject of protected health information before that information may be used or disclosed. A HIPAA compliant "authorization" must be specific and time (or event) limited. [35]

Two critical exceptions to the rule requiring authorization of disclosure permit Anasazi HIEO clients to disclose protected health information to the HIEO and permit the HIEO to transmit that information on to treatment providers without an individual authorization and without violating HIPAA. (As discussed below, these exceptions do not apply to alcohol/drug program records.)

First, covered entities may disclose PHI to a business associate and allow a business associate to create or receive PHI on its behalf, if it obtains "satisfactory assurances", in the form of a business associate agreement, that the business associate will appropriately safeguard the information.[36] The required elements of a business associate agreement are described in the regulations.[37] Anasazi routinely enters HIPAA compliant business associate agreements with its customers. This permits Anasazi clients to disclose PHI to Anasazi without the permission of individuals who are the subject of health records.

Second, the Privacy Rule, as revised in 2002, allows covered entities to use and disclose protected health information for their own "treatment, payment or health care operations", and, in some cases, for the "treatment, payment or health care operations" of another health care organization. Again, the written permission of individual subjects of disclosed records is not required.

The Privacy Rule defines "treatment" to mean "the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another."[38]

"Payment" is defined very broadly to mean:

(1) The activities undertaken by:

(i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and

---

[35] 45 CFR 164.508(c)(2)

[36] 45 CFR 164.502(e)

[37] 45 CFR 164.504(e) and 164.308(b)

[38] 45 CFR 164.501

provision of benefits under the health plan; or

(ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

This includes, but is not limited to:

> *(i) Determinations of eligibility or coverage…; (ii) Risk adjusting …;(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance …, and related health care data processing; (iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; (v) Utilization review activities, including pre-certification and preauthorization of services, concurrent and retrospective review of services; and (vi) Disclosure to consumer reporting agencies … relating to collection of premiums or reimbursement…*

"Health care operations" is also broadly defined. The term includes, among other things:

> *(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;*
>
> *(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;* [39] *…*

The Privacy Rule permits use and disclosure of PHI to support treatment, payment or health care operations of third parties.

The rule permits disclosure without written authorization to support: (a) the treatment activities of another health care provider (whether or not that provider is a covered entity); (b) the payment activities of a covered entity or health care provider that receives the information; and (c) the health care operations activities of a entity that receives the information, if both entities have a relationship with the individual who is the subject of the protected health information being requested, and the disclosure is for purposes that include "…quality assessment and improvement activities, including outcomes, evaluation and development of clinical guidelines (but not generalizable research activities), population based activities relating to improving health or reducing health care costs, protocol development, case management, care coordination, contacting

[39] All definitions found at 45 CFR 164.501. Note that the July 14, 2010 Notice of Proposed Rulemaking adds the term "patient safety activities" to paragraph (1) of the definition of health care operations.

of health care providers and patients with information about treatment alternatives, and related functions that do not include treatment…".[40]

Note, however, that the rules give individuals the right to request restrictions on disclosure of their records.[41] Section 13405(a) of the HITECH Act and the proposed regulations of the Department of Health and Human Services require covered entities and business associates to honor requests to limit disclosure to payers of information about treatment when the individual pays for that treatment out of pocket. For example, an individual could consult with a primary care physician about a mental health issue, pay for that service out of pocket, and request that information about that particular consultation be kept confidential. The primary care physician would be obligated to honor that request, although it could disclose information as needed to bill a payer for other services to the patient.[42]

1.7.3 The Minimum Necessary Standard

At 45 CFR 164.502 (b), the Privacy Rule establishes the "Minimum Necessary" standard. The Rule requires that when "using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request".

But the Minimum Necessary Standard does not apply to:

- Disclosures to or requests by a health care provider for treatment;
- Disclosures made to the individual;

---

[40] 45 CFR 164.506(c)

[41] 45 CFR 164.522(a)(1)

[42] In its discussion of this provision, DHHS notes the challenge of tracking required restrictions on disclosure of portions of a health record. This discussion is interesting in light of the requirements of 42 CFR Part 2, which restricts re-disclosure of records received from substance abuse programs. Note the following comments by DHHS:

"… Additionally, we request comment on the obligation of covered health care providers that know of a restriction to inform other health care providers downstream of such restriction. For example, a provider has been treating an individual for an infection for several months pursuant to the individual's requested restriction that none of the protected health information relating to the treatment of the infection be disclosed to the individual's health plan. If the individual requests that the provider send a copy of his medical records to another health care provider for treatment, what, if any, obligation should the original provider have to notify the recipient provider (including a pharmacy filling the individual's prescription) that the individual has placed a restriction upon much of the protected health information in the medical record? We request comment on whether a restriction placed upon certain protected health information should apply to, and the feasibility of it continuing to attach to, such information as it moves downstream, or if the restriction should no longer apply until the individual visits the new provider for treatment or services, requests a restriction, and pays out of pocket for the treatment. In addition, we request comment on the extent to which technical capabilities exist that would facilitate notification among providers of restrictions on the disclosure of protected health information, how widely these technologies are currently utilized, and any limitations in the technology that would require additional manual or other procedures to provide notification of restrictions…" (75 Federal Register 40900, July 14, 2010)

- Disclosures at the request of the individual pursuant to an Authorization;
- Disclosures made to DHHS related to enforcement of or compliance with HIPAA;
- Uses or disclosures that are required by law.

Implementation specifications for the minimum necessary standard are described at 45 CFR 164.514 (d). The rule requires covered entities to establish policies and procedures to comply with the minimum necessary standard.

A covered entity must control internal use of protected health information by establishing policies and procedures that identify:

"Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and

For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access."

The covered entity must then make a reasonable effort to limit the access to protected health information based on the duties of members of its workforce and information needed to enable staff to carry out their responsibilities.[43] Note that this requirement dovetails with the Security Rule, which requires covered entities to establish role based access controls for information systems.

For any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.[44]

Section 13405(b) of the HITECH Act incorporates the minimum necessary standard for disclosure of protected health information into law. Covered entities and business associates must limit the use, disclosure or request of protected health information to the extent practicable to either the limited data set (as defined in 45 CFR 164.514(e)(2)) or, if needed by such entity, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request, respectively. The legislative history of this provision indicates that Congress did not intend to override the exceptions to the minimum necessary rule described at 45 CFR 164.502(b). Those exceptions permit full disclosure of PHI for purposes of treatment, disclosures to individuals, and disclosures pursuant to an authorization. The covered entity or business associate that discloses protected health information is empowered to determine the "minimum necessary" to accomplish the purpose of disclosure. The Act requires the Secretary of Health and Human Services to issue guidance on what constitutes "minimum necessary" for purposes of the Privacy Rule within 18 months and to take into consideration the use and disclosure of information necessary to improve

[43] 45 CFR 164.514 (d)(2)

[44] 45 CFR 164.514 (d)(3)

patient outcomes and to detect, prevent and manage chronic disease.[45]

The HITECH Act creates financial incentives for eligible professionals (EPs), eligible hospitals, and critical access hospitals (CAHs) participating in Medicare and Medicaid programs that adopt and demonstrate meaningful use of certified electronic health record (EHR) technology. In July of 2010, the Center for Medicare and Medicaid Services (CMS) enacted final rules that specify the initial criteria EPs, eligible hospitals, and CAHs must meet in order to qualify for an incentive payment; calculation of the incentive payment amounts; payment adjustments under Medicare for covered professional services and inpatient hospital services provided by EPs, eligible hospitals and CAHs failing to demonstrate meaningful use of certified EHR technology; and other program participation requirements.[46] At the same time, the Office of the National Coordinator for Health Information Technology (ONC) issued a final rule that specifies the Secretary's adoption of an initial set of standards, implementation, specifications, and certification criteria for electronic health records.[47] ONC also issued a separate final rule on the establishment of certification programs for health information technology. (These rules are collectively referred to hereafter as the "Meaningful Use Rules".)

Among other things, the Meaningful Use Rules require professionals and hospitals to use qualified electronic health records to electronically transmit to other providers and electronically receive from other providers and organizations and display in human readable format a patient's summary record, including, at a minimum, diagnostic test results, problem list, medication list, and medication allergy list in accordance with the standard (and applicable implementation specifications) specified in 170.205(a)(1) [CCD] or 170.205 (a)(2) [CDR].[48]

The Meaningful Use Rules do not address privacy issues. But they clearly describe DHHS requirements for the minimum set of information to be electronically exchanged by provider organizations for purposes of treatment and care coordination. I think that it is safe to conclude that a health information exchange protocol based on the CCD standard adopted in the Meaningful Use rule will be consistent with the "minimum necessary" requirements of the HIPAA Privacy Rule and the HITECH Act.

1.7.4 Psychotherapy Notes

Psychotherapy notes are the only health record that is subject to a special standard under the HIPAA Privacy Rule. Psychotherapy notes may not be disclosed without an individual's specific authorization.

---

[45] HITECH Act § 13405(b)

[46] 42 CFR Part 495

[47] 45 CFR Part 170

[48] *45 CFR 170.304(i)*. The reference is to HL7 Clinical Document Architecture (CDA) Release 2, Continuity of Care Document (CCD).

The term "psychotherapy notes" is narrowly defined.[49] It includes personal notes kept in any form by a mental health professional to record or analyze individual, group or family counseling sessions, and kept separate from the rest of the individual's medical record. Diagnosis, functional status, treatment plan, symptoms, prognosis, progress notes, medications, treatment encounters, and clinical tests are all excluded from the definition of "psychotherapy notes" – HIPAA permits use and disclosure of such information without individual authorization as necessary for purposes of treatment, payment, or healthcare operations.

Psychotherapy notes may be disclosed without an individual's permission: (i) to DHHS when required for enforcement of the Privacy Rule; (ii) when required by law; (iii) when needed for regulatory oversight of the provider who created the notes; (iv) to a coroner or medical examiner; or (v) when needed to avert a serious and imminent threat to health or safety.[50]

A covered entity that receives psychotherapy notes must adhere to the terms of the Privacy Rule. It must obtain an authorization for any further use or disclosure.

The Privacy Rule exempts psychotherapy notes from the category of records that must be disclosed upon demand to the individuals who are the subject of a medical record.[51]

1.7.5 HIPAA vs. Other Privacy Standards

The HIPAA statute and the HIPAA Privacy Rule create minimum national standards for the use and disclosure of "protected health information" by HIPAA covered entities and business associates. State or federal privacy laws that grant individuals greater privacy rights continue to apply. Those that are less favorable to individuals are superseded by HIPAA. This means that it is necessary to compare the HIPAA Privacy Rule, other applicable federal law or rules, and state law to determine which provisions grant individuals greater privacy rights. The "more stringent" requirements apply in any situation.

The Privacy Rule defines "more stringent" to mean:

> *"...(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted by HIPAA...*
>
> *(2) With respect to the rights of an individual who is the subject of the individually identifiable health information of access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable; provided that, nothing in this subchapter may be construed to preempt any State law to the extent that it authorizes or prohibits disclosure of protected health information about a minor to a parent, guardian, or person acting in loco parentis of such*

[49] 45 CFR 164.501

[50] 45 CFR 164.508(a)(2)

[51] 45 CFR 164.524(a)(1)(i)

minor.

(3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.

(4) With respect to the form or substance of an authorization or consent for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the authorization or consent, as applicable.

1.7.6 The Security Rule

Both the HIPAA statute and the final Security Rule require covered entities to:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule.
- Ensure compliance by its workforce.[52]

DHHS first proposed the HIPAA Security Rule on August 12, 1998. The final rule was published in the Federal Register on February 20, 2003. The Security Rule creates standards and implementation specifications for *administrative*, *physical and technical safeguards* to protect the confidentiality, integrity, and availability of electronic protected health information. The rules are found at 45 CFR Part 164, Subpart C.

Section 13401 of the HITECH Act extends the direct application of the Security Rule to business associates of covered entities. As a result, both covered entities and business associates must establish security management processes and procedures to prevent, detect, contain, and correct security violations[53] and maintain the administrative, physical and technical safeguards of protected health information that is stored or transmitted electronically, as required by the rule. A business associate that violates these standards is subject the same civil and criminal penalties that could be applied to covered entities. Previously, business associates had contractual obligations to covered entities, but were not subject to civil enforcement actions by the Department of Health and Human Services or criminal prosecution for violation of the HIPAA standards.

[52] 42 USC 1320d-2(d)(2); 45 CFR 164.306(a)

[53] 45 CFR 164.308(a)

A discussion of the specific requirements of the Security Rule would be lengthy and beyond the scope of this memorandum. But to give a sense of the scope of the rule, the tables that follow list the Security Rule standards and implementation specifications for administrative, physical and technical safeguards of electronic protected health information.

The administrative safeguards include nine standards and twenty-one "required" or "addressable" implementation specifications.[54] They are presented in the table that follows.

45 CFR §	**Standard**	**Implementation Specification Required = R, Addressable = A**	
164.308(a)(1)	Security Management Process	Risk Analysis Risk Management Sanction Policy Information System Activity Review	R R R R
164.308(a)(2)	Assigned Security Responsibility	None	R
164.308(a)(3)	Workforce Security	Authorization and/or Supervision Workforce Clearance Procedure Termination Procedures	A A A
164.308(a)(4)	Information Access Management	Isolate Healthcare Clearinghouse Access Authorization Access Establishment and Modification	R A A
164.308(a)(5)	Security Awareness and Training	Security Reminders Protection from Malicious Software Log-in Monitoring Password Management	A A A A
164.308(a)(6)	Security Incident Procedures	Response and Reporting	R

[54] An "addressable" implementation specification is one that the covered entity or business associate must consider in its risk analysis, and implement if the safeguard is reasonably necessary to ensure the confidentiality, integrity and availability of electronic protected health information. Compliance with "required" implementation specifications is mandatory .

164.308(a)(7)	Contingency Plan	Data Backup Plan Disaster Recovery Plan Emergency Mode Operation Plan Testing and Revision Procedure Applications and Data Criticality Analysis	R R R A A
164.308(a)(8)	Evaluation	None	R

45 CFR 164.310 requires covered entities to establish physical safeguards of electronic protected health information. The final rule describes physical safeguards as "security measures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."[55] The standards and implementation specifications for physical safeguards are presented in the table that follows.

45 CFR §	Standard	Implementation Specification Required = R, Addressable = A	
164.310(a)	Facility Access Controls	Contingency operations Facility security plan Access control/validation procedures Maintenance records	A A A A
164.310(b)	Workstation Use	None	R
164.310(c)	Workstation Security	None	R
164.310(d)	Device and Media Controls	Disposal Media Re-use Accountability Data backup and storage	R R A A

45 CFR 164.312 establishes standards and implementation specifications relating to technical security of information systems that contain electronic protected health information. The standards are access control, audit controls, integrity, and transmission security. Within these standards are a number of implementation specifications.

[55] 45 CFR 164.304

45 CFR §	Standard	Implementation Specification Required = R, Addressable = A	
164.312(a)	Access Control	Unique user identification Emergency access procedure Automatic logoff Encryption and decryption Remote Access Wireless networks	R R A A
164.312(b)	Audit Controls	None	R
164.312(c)	Integrity	Mechanism to authenticate ePHI	A
164.312(d)	Person/Entity Authentication	None	R
164.312(e)	Transmission Security	Integrity controls Encryption	A A

1.7.7 HIPAA Enforcement

The HIPAA statute allows both civil and criminal penalties to be imposed for violation of the privacy and data security requirements quoted above. The original civil monetary penalties were fairly modest.

The HITECH Act included a number of provisions to strengthen enforcement of the HIPAA Rules. As noted above, the Act made business associates of covered entities directly responsible for compliance with the Privacy and Security Rules.

The HITECH Act substantially increased civil monetary penalties for HIPAA violations. In determining the amount of a penalty for a violation, the Secretary of Health and Human Services is required to base her determination on the nature and extent of the violation and the nature and extent of the harm resulting from such violation. She is required by the HITECH Act to investigate any case in which it appears that a violation of the HIPAA standards is the result of willful neglect by a covered entity or business associate, and required to seek civil monetary penalties in such cases.

The minimum and maximum penalties for violations of the HIPAA requirements are displayed in the table that follows.

Civil Monetary Penalties for HIPAA Violations	
Circumstance of Violation	Minimum and Maximum Penalties
Violation in which it is established that the person did not know (and by exercising reasonable diligence would not have known) that such person violated the HIPAA standard.	*Minimum Penalty*: $100/violation; Not more than $25,000/calendar year for same violation. *Maximum Penalty*: $50,000/violation; Not more than $1,500,000/calendar year for same violation.
Violation due to reasonable cause and not due to willful neglect.	*Minimum Penalty*: $1,000/violation; Not more than $100,000/calendar year for same violation. *Maximum Penalty*: $50,000/violation; Not more than $1,500,000/calendar year for same violation.
Violation was due to willful neglect and is corrected.	*Minimum Penalty*: $10,000/violation; Not more than $250,000/calendar year for same violation. *Maximum Penalty*: $50,000/violation; Not more than $1,500,000/calendar year for same violation.
Violation was due to willful neglect and is not corrected.	*Minimum Penalty*: $50,000/violation; Not more than $1,500,000/calendar year for same violation.

Note, however, that no penalty may be imposed if the failure to comply is due to reasonable cause, and not willful neglect, and the failure to comply is corrected within thirty (30) days of the date that the person knew or should have known that the failure occurred.[56]

DHHS enacted standards and procedures for enforcement of the HIPAA rules in February 2009. These rules were further amended to conform to the HITECH Act through an Interim Final Rule enacted in October 2009. (See 45 CFR Part 160, Subparts C and D.) In its July 14, 2010 Notice of Proposed Rule Making, DHHS proposes new definitions of the terms "reasonable cause" and

[56] 42 U.S.C. 1320d-5(b)

"willful neglect". They propose that "reasonable cause" mean:

"An act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect."

Willful neglect is defined, at 45 CFR 160.401, to mean the "conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated." The term not only presumes actual or constructive knowledge on the part of the covered entity or business associate that a violation is virtually certain to occur but also encompasses a conscious intent or degree of recklessness with regard to its compliance obligations. Thus, the failure to make a good faith effort to implement a compliance program would be considered reckless indifference and "willful neglect". In those circumstances, DHHS is required to investigate reports of non-compliance and required to seek civil monetary penalties.

Please note that HIPAA does not create a "private right of action" that would allow individuals to sue in federal court for violation of those privacy standards.

1.8 Substance Abuse Program Records

1.8.1 Background

42 USC 290dd-2(a) provides that:

Records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any program or activity relating to substance abuse education, prevention, training, treatment, rehabilitation, or research, which is conducted, regulated, or directly or indirectly assisted by any department or agency of the United States shall … be confidential and be disclosed only for the purposes and under the circumstances expressly authorized under subsection (b) of this section.

Subsection (b) permits disclosures with the consent of the patient. Disclosures without consent are permitted in cases of medical emergency, to qualified personnel for purposes of audits or program evaluations, and pursuant to a court order.

Note that the statute does not apply to records maintained by the Veteran's Administration or the Armed Forces of the United States.[57]

[57] 42 USC 290dd-2(e)

1.8.2 Applicability of 42 CFR Part 2 – Definition of Federally Assisted Substance Abuse Program

42 CFR Part 2 is the set of federal regulations enacted pursuant to 42 USC 290dd-2 and its predecessor statutes. The rules were enacted in 1987.

42 CFR Part 2 imposes restrictions on the disclosure and use of alcohol and drug abuse patient records which are maintained in connection with the performance of any federally assisted alcohol or drug abuse program.[58] A "program" includes:

Any individual or entity (other than a general medical care facility) that holds itself out as providing, and provides alcohol or drug abuse diagnosis, treatment or referral for treatment;

An identified unit within a general medical care facility that holds itself out as providing, and provides alcohol or drug abuse diagnosis, treatment or referral for treatment; or

Medical personnel or other staff in a general medical care facility whose primary function is the provision of alcohol or drug abuse diagnosis, treatment or referral for treatment and who are identified as such providers[59].

Almost all alcohol and drug programs are considered to be "federally assisted" and subject to the regulations. This includes: programs conducted directly or under contract to any department or agency of the United States (with the exception of the Veteran's Administration and the Armed Forces, which are exempt from 42 USC 290dd-2); programs that are licensed, certified, registered or otherwise authorized by any department or agency of the United States, including Medicare providers, operators of methadone maintenance programs, and people or organizations that are registered to dispense a controlled substance (to the extent that the controlled substance is used to treat alcohol or drug abuse); programs that receive any form of federal financial assistance for any purpose, including state or local government programs that receive general revenue sharing from the federal government; and tax-exempt organizations.[60]

The applicability of 42 CFR Part 2 is explained at section 2.12(e).

... These regulations cover any information (including information on referral and intake) about alcohol and drug abuse patients obtained by a program ... if the program is federally assisted ... Coverage includes, but is not limited to, those treatment or rehabilitation programs, employee assistance programs, programs within general hospitals, school-based programs, and private practitioners who hold themselves out as providing, and provide alcohol or drug abuse diagnosis, treatment, or referral for treatment. However, these regulations would not apply, for example, to emergency room personnel who refer a patient to the intensive care unit for an apparent overdose, unless the primary function of such personnel is the provision of alcohol

[58] 42 CFR 2.3(a).

[59] 42 CFR 2.11

[60] 42 CFR 2.12(b)

or drug abuse diagnosis, treatment or referral and they are identified as providing such services or the emergency room has promoted itself to the community as a provider of such services.[61]

It is important to note that individually identifiable health information generated by primary care physicians, psychiatric hospitals, health plans, pharmacies, and the mental health units of community mental health centers is not subject to 42 CFR Part 2, even though the content of the information may indicate that the subject of the record has a substance abuse disorder. These services do not "hold themselves out" as providers or alcohol or drug abuse treatment and do not meet the definition of a "program" for purposes of 42 CFR Part 2. The protections of 42 CFR Part 2 attach to information based on the source of the information, not its content.

The Substance Abuse and Mental Health Services Administration (SAMHSA, along with the Office of National Coordinator for Health Information Technology, recently issued a paper entitled *Frequently Asked Questions, Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE) (June 2010).* The discussion following FAQ question 2 suggests that physicians may become subject to the requirements of 42 CFR Part 2 simply by prescribing a controlled substance.

…Clinicians who use a controlled substance (e.g., benzodiazepines, methadone or buprenorphine) for detoxification or maintenance treatment of a substance use disorder require a federal DEA registration and become subject to Part 2 through the DEA license. In contrast, a physician who does not use a controlled substance for treatment, such as Naltrexone, and does not otherwise meet the definition of a Part 2 program is not subject to Part 2.

This statement generated concern in the clinical community about the privacy rules that must be followed by prescribers of controlled substances. The American Psychiatric Association, American Association of Addiction Medicine and others presented their concerns to SAMHSA at a public hearing in Washington DC on August 4, 2010. During this meeting, SAMHSA leadership said that they did not intend to expand application of 42 CFR Part 2 to physicians that do not "hold themselves out" as substance abuse treatment specialists.

1.8.3 Applicability of 42 CFR Part 2 – Definitions

42 CFR Part 2 restricts "disclosure" of any alcohol or drug abuse program "patient" "record". 42 CFR 2.11 defines the terms used in this sentence.

A "patient" is any individual who has applied for or been given diagnosis or treatment for alcohol or drug abuse at a federally assisted program.

A "record" includes any information, whether recorded or not, relating to a patient that is received or acquired by a federally assisted alcohol or drug program.

[61] See Center for Legal Advocacy v. Earnest, 320 F.3d 1107 (10th Cir., 2003).

Disclose or disclosure means "a communication of patient indentifying information, the affirmative verification of another person's communication of patient identifying information, or the communication of any information from the record of a patient who has been identified".

Thus, a person or organization that is required to follow 42 CFR Part 2 is prohibited from disclosing any information at all that would identify an individual as a patient at an alcohol or drug abuse program or any part of the patient's record, except as permitted by the rule. Unconditional compliance is required.[62] A Health Information Exchange Organization that maintains a patient locator service that informs third parties of an association between an identifiable person and a patient record maintained by an alcohol or drug abuse program without the consent of the patient would violate 42 CFR Part 2.

1.8.4 Applicability of 42 CFR Part 2 – Recipient of Substance Abuse Program Record

The restrictions on disclosure set forth in 42 CFR Part 2 apply to:

> *Third party payers with regard to records disclosed to them by federally assisted alcohol or drug abuse programs;*
>
> *Entities having direct administrative control over substance abuse programs; and*
>
> *Persons who receive patient records directly from a federally assisted alcohol or drug abuse program and who are notified of the restrictions on redisclosure of the records in accordance with §2.32 of these regulations.*[63]

The notice requirements of 42 CFR 2.32 are described at section 1.8.7. They apply when a disclosure of a substance abuse program record is made with the written consent of the patient. They do not apply when information is disclosed without the patient's consent, such as in cases of medical emergency. So a hospital that receives substance abuse program information in an emergency on a "break the glass" basis will not be restricted by 42 CFR Part 2 from re-disclosing that information. But if it receives the same information pursuant to a patient's consent, the re-disclosure restrictions will apply.[64]

Healthcare providers that wish to use certified electronic health records in compliance with the "Meaningful Use" rules must have the ability to send and receive health information including Continuity of Care Documents, problem lists, laboratory results, medication lists, and medication allergies[65] and must use that information to improve the quality and appropriateness of treatment.

---

[62] 42 CFR 2.13(b)

[63] 42 CFR 2.12(d)(2)

[64] This is one of the weaknesses of a regulatory scheme that bases privacy protections on the source of a record and not its content. It is not whether clear

[65] See 45 CFR 170.205 and 170.207

But when the source of that information is a substance abuse program, a health care provider that is not subject to 42 CFR Part 2, such as a primary care physician, cannot automatically incorporate that data into its electronic health record without risking non-compliance with the 42 CFR Part 2 restrictions on re-disclosure. The recipient might be forced to create a separate file to ensure compliance. This could limit the utility of electronic health information exchange and therefore inhibit efforts to coordinate physical health and addiction treatment services.

1.8.5 42 CFR Part 2 – Consent Requirements Prior to Disclosure of Record

Except in the case of a medical emergency, 42 CFR Part 2 requires the written permission of a patient for disclosure of patient identifying information or any portion of a substance abuse program record information for the purposes of treatment, payment or healthcare operations. This includes disclosures made through a health information organization.

1.8.6 42 CFR Part 2 – Required Form of Consent

The patient's permission must be given using a "consent" form described at 42 CFR 2.31. The elements of this form are very similar to those required for a HIPAA compliant "authorization" of disclosure.

The required elements of a written Consent to disclose alcohol/drug program records include:

- The specific name or general designation of the program or person permitted to make the disclosure;
- The name or title of the individual or the name of the organization to which disclosure is to be made;
- The name of the patient;
- The purpose of the disclosure;
- How much and what kind of information is to be disclosed;
- The signature of the patient and, when applicable, the person authorized by law to give consent for a minor, incompetent or deceased patient;
- The date on which the consent is signed;
- A statement that the consent is subject to revocation at any time except to the extent that the program or person which is to make the disclosure has already acted in reliance on it;
- The date, event, or condition upon which the consent will expire if not revoked before. This date, event, or condition must insure that the consent will last no longer than reasonably necessary to serve the purpose for which it is given.

The *Frequently Asked Questions* paper published by SAMHSA and ONC provides useful guidance regarding the consumer consent requirements for disclosure of information to and through a health information exchange. Among other things, SAMHSA and ONC confirm that:

- Under Part 2, a single consent form can authorize a disclosure of information about a patient to one recipient, such as an HIO, and simultaneously authorize that recipient to re-disclose that information to an additional entity or entities (such as other HIO affiliated health care providers identified in the consent form), provided that the purpose for the disclosure is the same.

- A Part 2 consent form can authorize an exchange of information between multiple parties named in the consent form. The key is to make sure the consent form authorizes each party to disclose to the other ones the information specified and for the purpose specified, in the consent. The consent must identify the specific parties who are permitted to receive information about the patient. A form permitting disclosure to "all HIO members" would not comply with 42 CFR 2.31.

- Part 2 does not require programs (or recipients named in the consent) to have a patient's "original" signed consent form in their possession to make disclosures. As long as the program or recipient of the consent acts with reasonable caution, it may accept a facsimile or a photocopy of a consent form.

- An electronically signed consent form is allowable, provided that an electronic signature is valid under applicable law.

- Under a Part 2 patient consent, information may be disclosed multiple times, as long as the consent has not yet expired and the entities to whom the information is to be disclosed, the nature of the information, and the purpose for the disclosure specified in the consent form are still the same. A separate consent form does not need to be obtained each time a disclosure of Part 2 records is made.

- A Part 2 consent form must list the date, event, or condition upon which the consent will expire, if not revoked before. It is not sufficient under Part 2 for a consent form to state that disclosures will be permitted until consent is revoked. It is, however, permissible for a consent form to specify the event or condition that will result in revocation, such as having its expiration date be "upon my death."

1.8.7 Notice Requirement

A written notice must accompany alcohol/drug program records that are disclosed with the patient's consent. 42 CFR 2.32 requires that each disclosure made with the patient's written consent must be accompanied by the following written statement:

> *"This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient."*

This notice is not required when the disclosure is made without the patient's consent, such as a disclosure in a medical emergency.

1.8.8 Minors

42 CFR § 2.14 provides that if a minor patient has the right under state law to seek treatment at a federally assisted substance abuse program, the minor must give the required consent to disclosure of records of his or her treatment. Parental consent for a disclosure is required in addition to the minor's only if the Part 2 program is required by state law to obtain parental consent before providing alcohol or drug treatment to the minor.

1.8.9 Disclosures Without Consent – When Permitted

The restrictions on disclosure of substance abuse program records described in 42 CFR Part 2 do not apply in certain circumstances. Consent is not required for disclosures:

- Within a substance abuse program;
- Between a substance program and an entity that has direct administrative control over the program;
- To Qualified Services Organizations;
- To report crimes on the premises of the program or against program personnel;
- To report suspected child abuse or neglect[66];
- In response to medical emergencies[67];
- As part of an authorized research program[68], or

[66] All above listed disclosures are permitted by 42 CFR 2.12.

[67] 42 CFR 2.51

[68] 42 CFR 2.52

- To federal, state or local government agencies, peer review organizations and other authorized organizations that conduct audit or evaluation activities.[69]

1.8.10 Disclosure Without Consent in Medical Emergencies

42 CFR 2.51(a) permits disclosure of patient identifying information to "medical personnel who have a need for information about a patient for the purposes of treating a condition which poses an immediate threat to the health of any individual which requires immediate medical intervention". 42 CFR 2.51(c) requires that when such a disclosure is made, the Part 2 program must document the disclosure in the patient's records, setting forth in writing: (1) the name of the medical personnel to whom the disclosure was made and their affiliation with any health care facility; (2) the name of the individual making the disclosure; (3) the date and time of the disclosure; and (4) the nature of the emergency.

The SAMHSA and ONC Frequently Asked Questions document addresses a number of questions regarding disclosures in medical emergencies through health information organizations. They confirm the following:

- Any health care provider who is treating a patient can make a determination that a medical emergency exists. It is not necessary for the Part 2 program to make that determination. "Thus, any treating provider who determines that a condition which poses an immediate threat to the health of an individual exists can make the decision to "break the glass" (the term used when a health care provider, in the case of an emergency, gets access to a patient's records without the patient's consent) and gain access to Part 2 records. This includes HIO affiliated health care providers treating an individual in a medical emergency who might seek access to records about a patient that are held in, or made available through, an HIO".[70]

- The treating provider must record the name and affiliation of the medical personnel receiving the information, the name of the individual making the disclosure, the date and time of the disclosure, and the nature of the emergency and convey that information to the Part 2 provider to enable the Part 2 provider to comply with 42 CFR 2.51(c). Automated electronic systems may be used to generate information necessary for a provider to make a determination of a medical emergency, to enable provider entry of emergency information, and/or to generate a report documenting the emergency.

- A Health Information Organization system may make clinical decision support functions (such as showing a patient's medications to clinicians when they write prescriptions, automatically ordering medications, and/or alerting clinicians about potential drug interactions) available to HIO affiliated health care providers in a medical emergency. In circumstances not involving a medical emergency, the system could not disclose any Part 2 data to the treating physician in the absence of consent. The system could only tell the provider that a specific consent must be

[69] 42 CFR 2.53

[70] FAQ #26

obtained, and it must be set up so that such a notice would not reveal the existence of protected Part 2 information.

- Part 2 information disclosed in a medical emergency may be re-disclosed without obtaining patient consent. Medical personnel treating a patient for a medical emergency who are HIO affiliated providers may download and include in their own records the information they obtained in treating the emergency, and may then re-disclose that information to others without obtaining patient consent.

1.8.11 Qualified Service Organizations

42 CFR 2.12(c)(4) permits substance abuse programs to disclose patient records to "qualified service organization" that provides services to the program and enters an agreement in which acknowledges the applicability of and agrees to follow 42 CFR Part 2 with regard to disclosure of alcohol/drug records.[71]

A "qualified service organization" is defined at 42 CFR 2.11 to mean a person which:

> *(a) Provides services to a program, such as data processing, bill collecting, dosage preparation, laboratory analyses, or legal, medical, accounting, or other professional services, or services to prevent or treat child abuse or neglect, including training on nutrition and child care and individual and group therapy, and*
>
> *(b) Has entered into a written agreement with a program under which that person:*
>
> *(1) Acknowledges that in receiving, storing, processing or otherwise dealing with any patient records from the programs, it is fully bound by these regulations; and*
>
> *(2) If necessary, will resist in judicial proceedings any efforts to obtain access to patient records except as permitted by these regulations.*

Note the similarity between the definitions of "business associate" under HIPAA and "qualified service organization" under 42 CFR Part 2 and the common requirement of an agreement between the disclosing organization and the organization that provides services to the discloser. Anasazi may enter a single agreement with users of the health information exchange that includes the required elements of both a HIPAA Business Associate Agreement and a 42 CFR Part 2 Qualified Service Organization Agreement.

In the recent Frequently Asked Questions, SAMHSA and ONC state explicitly that a Qualified Service Organization Agreement may be used to facilitate communication between a Part 2 program and an HIO. Once a QSOA is in place, Part 2 permits the program to freely communicate information from patients' records to the HIO as long as it is limited to that information needed by the HIO to provide services to the program. The HIO may also

[71] 42 CFR 2.13(d)

communicate with the Part 2 program and share information it receives from the program back with the program. Patient consent is not needed to authorize such communications between the HIO and Part 2 program when a QSOA is in place between the two.

However, information protected by Part 2 may only be made available through the health information organization to third parties if the patient signs a Part 2-compliant consent form or a medical emergency exists.

1.8.12 Disclosures in Legal Proceedings

42 CFR Part 2 Subpart E establishes procedures and standards for issuance of court orders permitting disclosure of substance abuse program records in civil proceedings and in criminal investigations. The holder of the record must be given notice of an application for the court order and an opportunity to be heard in response to the application. The standards for issuance of court orders are set forth in the regulations at 42 CFR 2.64 (non-criminal proceedings), 2.65 (criminal investigations) and 2.66 (investigations of the holder of the record). 42 USC 290dd-2(c) and 42 CFR 2.12(d) bar the use of substance abuse program records as evidence to investigate or prosecute patients in criminal proceedings.

1.8.13 Enforcement of 42 CFR Part 2

Under 42 USC 290dd-2(f), any person who violates that statute or 42 CFR Part 2 may be fined not more than $500 for a first offense, and not more than $5,000 for each subsequent offense. Violation of the statute is a crime. Neither the statute nor the regulations create civil monetary penalties or describe procedures for SAMHSA or DHHS enforcement of 42 CFR Part 2. There is no "private right of action" that would allow individuals to sue for damages based on a violation of the provisions of 42 USC 290dd-2 or 42 CFR Part 2.

1.9 State Laws – Generally

Most states have statutes that require healthcare providers to protect the confidentiality of certain kinds of health information, such as AIDS/HIV, mental health or substance abuse treatment records. Some states have enacted statutes that grant individuals the right of access to medical records. But the law varies from state to state. As described by the 1999 Health Care Privacy Project Survey of State Health Privacy Statutes,

> *Nearly all states have laws that impose condition-specific privacy requirements, most often to shield people with mental illness, communicable disease, cancer, and other sensitive, stigmatized diseases from broad disclosures…The protections tend to attach to the information at the point of collection, before the information is disclosed. These requirements may, for example, require a provider, hospital or laboratory to obtain a particular kind of authorization from the patient or more stringently restrict disclosure.*

For more information about state health privacy laws, see The State of Health Privacy – An Uneven Terrain, A Comprehensive Survey of State Health Privacy Statutes (1999), by Joy Pritts,

JD, Janlori Goldman, JD, Zoe Hudson, Aimee Berenson, JD, and Elizabeth Hadley, JD, prepared for the Georgetown University Health Care Privacy Project. See, also the Report from the Health Information Protection Taskforce to the State Alliance for E-Health, National Governor's Association, 2007; Harmonizing State Privacy Law Collaborative Final Report, Health Information Security and Privacy Collaboration (HISPC), March 2009; and Report on State Law Requirements for Patient Permission to Disclose Health Information, Health Information Security and Privacy Collaboration (HISPC), August 2009.

Differences between state privacy laws must be resolved when transmitting health information across state lines. See the Final Report of the Interstate Disclosure and Patient Consent Requirements Collaborative to the Office of National Coordinator for Health Information Technology, March 2009.

1.10 California Law Governing Disclosures for Treatment Purposes

1.10.1 California State Constitution

Article 1, Section 1 of the California State Constitution reads:

> *§ 1. Inalienable rights*
>
> *All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.*

The Supreme Court of California has held that this provision of the State Constitution creates a right to privacy that can be legally enforced against both government and private sector organizations. In *Hill vs. NCAA*,[72] the Court held that a plaintiff may prevail in a cause of action alleging a violation of the constitutional right to privacy if he/she establishes each of the following: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy.

> *Legally recognized privacy interests are generally of two classes: (1) interests in precluding the dissemination or misuse of sensitive and confidential information ("informational privacy"); and (2) interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference ("autonomy privacy").*
>
> *... Even when a legally cognizable privacy interest is present, other factors may affect a person's reasonable expectation of privacy. ... [C]ustoms, practices, and physical settings surrounding particular activities may create or inhibit reasonable expectations of privacy ... A "reasonable" expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms. ... Finally, the presence or absence of opportunities to consent voluntarily to activities impacting privacy*

[72] 7 Cal. 4th 1; 865 P.2d 633 (1994)

interests obviously affects the expectations of the participant...

Actionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right. Thus, the extent and gravity of the invasion is an indispensable consideration in assessing an alleged invasion of privacy.

The diverse and somewhat amorphous character of the privacy right necessarily requires that privacy interests be specifically identified and carefully compared with competing or countervailing privacy and nonprivacy interests in a "balancing test." The comparison and balancing of diverse interests is central to the privacy jurisprudence of both common and constitutional law.

... Invasion of a privacy interest is not a violation of the state constitutional right to privacy if the invasion is justified by a competing interest. Legitimate interests derive from the legally authorized and socially beneficial activities of government and private entities. Their relative importance is determined by their proximity to the central functions of a particular public or private enterprise. Conduct alleged to be an invasion of privacy is to be evaluated based on the extent to which it furthers legitimate and important competing interests.

Confronted with a defense based on countervailing interests, the plaintiff may undertake the burden of demonstrating the availability and use of protective measures, safeguards, and alternatives to defendant's conduct that would minimize the intrusion on privacy interests. ... For example, if intrusion is limited and confidential information is carefully shielded from disclosure except to those who have a legitimate need to know, privacy concerns are assuaged. On the other hand, if sensitive information is gathered and feasible safeguards are slipshod or nonexistent, or if defendant's legitimate objectives can be readily accomplished by alternative means having little or no impact on privacy interests, the prospect of actionable invasion of privacy is enhanced.

The Hill case upheld the right of the NCAA to conduct drug tests of student athletes. The court noted that plaintiffs had no right to participate in intercollegiate athletic competition, that plaintiffs' reasonable expectation of privacy were diminished by notice and consent elements of defendant's testing program, and that the NCAA had a legitimate interest in maintaining the integrity of intercollegiate athletic competition and in protecting the health and safety of student athletes.

Other California cases have resulted in findings for the plaintiff, particularly when a clinical professional makes an unauthorized disclosure of confidential information in a manner that violates the California Confidentiality of Medical Information Act (CMIA), Cal. Civ. Code § 56 et seq., which is discussed below.[73]

[73] See, *Pettus v Cole*, 49 CalApp4th 402, 57 Cal Rptr 2d 46 (1996), *Urbaniak v. Newton* (1991) 226 Cal.App.3d 1128, 1138 (1991) and *Garrett v. Young,* 109 Cal App 4th 1393 (2003).

1.10.2 Confidentiality of Medical Information Act

The California Confidentiality of Medical Information Act is very similar to the HIPAA Privacy Rule in that it permits disclosures of individually identifiable medical information without patient authorization for purposes of treatment and payment of benefit claims.

Section 56.10(a) of the California Civil Code states the general rule that:

> *(a) No provider of health care, health care service plan, or contractor shall disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization, except as provided in subdivision (b) or (c).*

Subdivision (b) lists nine circumstances under which disclosure of medical information may be compelled, including various kinds of legal proceedings, disclosures to coroners, and disclosures to the patient. Unlike 42 CFR Part 2, there is no requirement that the holder of the record resist efforts to compel disclosure in legal proceedings.

Subdivision (c) of section 56.10 permits, but does not require, a provider of health care or a health care service plan to disclose medical information without an authorization in twenty-one different circumstances.

Subdivision (c)(1) permits disclosure of information for treatment purposes without an authorization.

> *(1) The information may be disclosed to providers of health care, health care service plans, contractors, or other health care professionals or facilities for purposes of diagnosis or treatment of the patient. This includes, in an emergency situation, the communication of patient information by radio transmission or other means between emergency medical personnel at the scene of an emergency, or in an emergency medical transport vehicle, and emergency medical personnel at a health facility…*

56.10(c) also permits disclosures for billing and payment purposes and disclosures to persons or entities that provide billing, claims management or other administrative services to providers and health plans. (The statute does not require agreements equivalent to a HIPAA Business Associate Agreement or a 42 CFR Part 2 Qualified Service Organization Agreement.) Other permitted disclosures are similar to the disclosures for health care operations that are permitted by HIPAA.

1.10.3 Mental Health Records

California has several provisions of law that are designed to protect the confidentiality of information about mental health treatment.

The Evidence Code creates a "psychotherapist-patient" privilege[74] that allows a patient to refuse to disclose and to prevent disclosure of a confidential communication between patient and psychotherapist.

The Confidentiality of Medical Information Act establishes a higher standard for release of information about outpatient psychotherapy treatment for purposes other than treatment or when necessary to prevent a serious and imminent threat of harm to a third party. Information may be released to a provider of health care or a health services plan for treatment purposes without consent, as permitted by Civil Code §56.10(c)(1).

But if medical information is to be disclosed for other purposes permitted by §56.10(c) and that information "*specifically relates to the patient's participation in outpatient treatment with a psychotherapist*", the requestor must submit a signed written request to the patient and to the holder of the record that includes all of the following:

> *(1) The specific information relating to a patient's participation in outpatient treatment with a psychotherapist being requested and its specific intended use or uses.*
>
> *(2) The length of time during which the information will be kept before being destroyed or disposed of. A person or entity may extend that timeframe, provided that the person or entity notifies the provider, plan, or contractor of the extension. Any notification of an extension shall include the specific reason for the extension, the intended use or uses of the information during the extended time, and the expected date of the destruction of the information.*
>
> *(3) A statement that the information will not be used for any purpose other than its intended use.*
>
> *(4) A statement that the person or entity requesting the information will destroy the information and all copies in the person's or entity's possession or control, will cause it to be destroyed, or will return the information and all copies of it before or immediately after the length of time specified in paragraph (2) has expired.*[75]

The person or entity requesting the information about outpatient psychotherapy must submit a copy of the written request to the patient within 30 days of receipt of the information requested, unless the patient has signed a written waiver in the form of a letter signed and submitted by the patient to the provider of health care or health care service plan waiving notification. Note that the statute does not require an authorization prior to the release of information.

---

[74] Evidence Code §§ 1010-1027.

[75] Civil Code §56.104

The statute does not define what medical information "*specifically relates to the patient's participation in outpatient treatment with a psychotherapist*". It is not clear whether this refers to psychotherapy notes, or to any information that would indicate that a person is receiving outpatient treatment from a psychotherapist. The legislative history indicates that the California legislature was concerned about the need to prevent unnecessary disclosures to managed care companies for purposes other than treatment or payment.[76] I have found no case law or regulations that interpret section 56.104.

Section 5328 of the California Welfare and Institutions Code requires that all information and records obtained in the course of providing inpatient mental health, community mental health, or developmental disabilities services be kept confidential. Such information and records may only be disclosed as permitted by the statute. Section 5328 permits disclosure without written authorization to qualified treatment providers for purposes of treatment or referral for treatment. It goes on to list a number of other circumstances in which disclosures are permitted, including disclosures for payment purposes and disclosures to county mental health directors. The list of permitted disclosures is very similar to that found in the Confidentiality of Medical Information Act.

---

[76] Stats 1999 ch. 527, section 1 provides:

The Legislature finds and declares the following:

(a) Privacy is a fundamental right of Californians.

(b) Mental health treatment, in order to be effective, depends upon open communication based on the patient's trust in the practitioner.

(c) A relationship of trust can only be established if the patient is confident that access to his or her personal information will be limited and that the information will be protected to the fullest extent possible.

(d) In recognition of the fundamental importance of maintaining this relationship with patients, mental health practitioners are bound by professional codes of ethics and laws designed to protect sensitive information.

(e) As managed care has expanded in recent years, mental health professionals have been forced to choose between their obligation to protect the confidentiality of patient information and the demands of insurers and health care service plans that operate the health care system to obtain that information for administrative purposes other than authorization of treatment and payment of services.

(f) The inclusion of recognizable patient identification information in medical records obtained by health care service plans or insurers exposes sensitive identifying information about the patient, thereby jeopardizing the patient's privacy.

(g) Laws providing for the confidentiality of medical information should protect patients from the unlawful disclosure of their most personal information.

(h) Informed consent is appropriately given by the patient's signature on an authorization to release information that clearly and specifically states the information requested, the purpose for the request, the identity of those who will have access to the information, the date the authorization was signed, and an expiration date.

(i) Patients should not forfeit their right to confidentiality of their personal information to insurers or health care service plans for purposes other than those purposes authorized by law.

1.10.4 HIV/AIDS Records

California law protects the confidentiality of public health records of reports of HIV infection or AIDS as well as research records relating to HIV or AIDS. Such records may not be disclosed, are not discoverable, and may not be used in legal proceedings.[77] The law requires health care providers and clinical laboratories to report positive HIV results to public health authorities.

But I have found nothing in California law that creates a separate standard for disclosure of HIV/AIDS related information for treatment purposes. The Confidentiality of Medical Information Act governs such disclosures.

1.10.5 Disclosure Pursuant to an Authorization

As noted above, an authorization is not ordinarily required by California law prior to disclosure of medical information for treatment purposes. But in circumstances in which an authorization is required, it must be in proper form. The specifications for a legally valid authorization are set forth in section 56.11 of the Civil Code:

> *An authorization for the release of medical information by a provider of health care, health care service plan, pharmaceutical company, or contractor shall be valid if it:*
>
> *(a) Is handwritten by the person who signs it or is in a typeface no smaller than 14-point type.*
>
> *(b) Is clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization.*
>
> *(c) Is signed and dated by one of the following:*
>
> *(1) The patient. A patient who is a minor may only sign an authorization for the release of medical information obtained by a provider of health care, health care service plan, pharmaceutical company, or contractor in the course of furnishing services to which the minor could lawfully have consented...*
>
> *(2) The legal representative of the patient, if the patient is a minor or an incompetent...*
>
> *(3) The spouse of the patient or the person financially responsible for the patient, where the medical information is being sought for the sole purpose of processing an application for health insurance or for enrollment in a nonprofit hospital plan, a health care service plan, or an employee benefit plan, and where the patient is to be an enrolled spouse or dependent under the policy or plan.*
>
> *(4) The beneficiary or personal representative of a deceased patient.*
>
> *(d) States the specific uses and limitations on the types of medical information to be disclosed.*
>
> *(e) States the name or functions of the provider of health care, health care service plan, pharmaceutical company, or contractor that may disclose the medical information.*
>
> *(f) States the name or functions of the persons or entities authorized to receive the medical information.*
>
> *(g) States the specific uses and limitations on the use of the medical information by the persons or*

[77] Health and Safety Code §§121025 and 121075 et. seq.

entities authorized to receive the medical information.

(h) States a specific date after which the provider of health care, health care service plan, pharmaceutical company, or contractor is no longer authorized to disclose the medical information.

(i) Advises the person signing the authorization of the right to receive a copy of the authorization.

A recipient of medical information pursuant to an authorization may not further disclose that medical information except in accordance with a new authorization that meets the requirements of Section 56.11, or as specifically required or permitted by other provisions of law.[78]

A provider of health care, health care service plan, or contractor that discloses medical information pursuant to a required authorization must communicate to the person or entity to which it discloses the medical information any limitations in the authorization regarding the use of the medical information.[79]

An authorization may be cancelled or modified at any time, effective as of the date of receipt of the modification or cancellation.[80]

1.10.6 Genetic Information

Section 57.17 of the Civil Code requires that health service plans obtain an authorization before disclosing genetic test results contained in an applicant's or enrollees medical records. The statute does not apply to health care providers. Persons who negligently or willfully disclose the results of a test for a genetic characteristic without an authorization are subject to civil penalties of $1,000 or $5,000 per disclosure and criminal prosecution for a misdemeanor, with a fine of up to $10,000. In addition, the person whose records are disclosed may bring a civil action for damages, including damages for economic, bodily or emotional harm caused by the disclosure.

1.10.7 Data Security

The California Confidentiality of Medical Information Act provides that:

Every provider of health care, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical records shall do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical records shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36.[81]

---

[78] Civil Code §56.13

[79] Civil Code §56.14

[80] Civil Code §56.15

[81] Civil Code § 56.101

In addition, section 13303(a) of the Health and Safety Code requires that:

> *(a) Every provider of health care shall establish and implement appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's medical information. Every provider of health care shall reasonably safeguard confidential medical information from any unauthorized access or unlawful access, use, or disclosure.*

1.10.8 Enforcement of California's Health Privacy and Data Security Laws

In 2008, the State of California enacted legislation to establish within the Health and Human Services Agency the Office of Health Information Integrity (OHII) to "ensure the enforcement of state law mandating the confidentiality of medical information and to impose administrative fines for the unauthorized use of medical information".[82]

Section 130202 of the Health and Safety Code empowers OHII, "upon a referral from the State Department of Public Health, to assess an administrative fine against any person or any provider of health care, whether licensed or unlicensed, for any violation … in an amount as provided in Section 56.36 of the Civil Code. All administrative fines assessed by OHII will be deposited in a special account known as the Internal Health Information Integrity Quality Improvement Account. Monies in the account are to be used to support the work of OHII".[83]

Section 56.36 of the Civil Code creates criminal and civil penalties for violation of the Confidentiality of Medical Information Act (CMIA), and gives individuals affected by a violation of the Act the right to sue for damages.

Any violation that results in economic loss or personal injury is punishable as a misdemeanor.

A number of officials of State and local government are empowered to bring civil actions in the name of the people of California to assess and recover civil penalties for violations of CMIA. This includes the Office of Health Information Integrity, the State Attorney General, state licensing authorities, a District Attorney, County Counsel, City Attorneys of large cities, and city prosecutors.

Individuals have the right to bring a civil action against any person or entity that releases confidential information or records in violation of CMIA. Section 56.36 specifies the remedies listed below. The same penalties may be assessed in a case commenced by a public official on behalf of the State. They are as follows:

---

[82] Stats 2008, chapter 602

[83] Health and Safety Code § 13204

Violation	Damages and Penalties
Negligent disclosure of medical information	*Nominal damages of one thousand dollars ($1,000), regardless of whether or not plaintiff suffered or was threatened with actual damages; and/or* *The amount of actual damages, if any, sustained by the patient.* **+** *An administrative fine or civil penalty not to exceed two thousand five hundred dollars ($2,500) per violation.*
Unauthorized disclosure of medical information causing economic loss or personal injury	*Damages to be paid to plaintiff = compensatory damages + punitive damages not to exceed $3,000 + attorneys' fees not to exceed $1,000 + the costs of litigation.*[84]
Knowingly and willfully obtaining, disclosing, or using medical information	*$25,000 administrative fine or civil penalty per violation if violator is not a health care professional.* *If a health care professional: $2500 for 1st violation, $10,000 for 2nd violation, $25,000/violation thereafter.*
Knowingly and willfully obtaining, disclosing, or using medical information for financial gain	*Administrative fine or civil penalty not to exceed two hundred fifty thousand dollars ($250,000) per violation plus disgorgement of any proceeds or other consideration obtained as a result of the violation if not a health care professional.* *If a health care professional: administrative fine or civil penalty up to $5000 for 1st violation, $25,000 for 2nd violation, $250,000/violation thereafter plus disgorgement of proceeds from violation.*
Knowing and willful obtaining, disclosing or using medical information without written authorization by a person or entity that is not permitted to receive medical information pursuant to the Confidentiality of Medical Information Act	*Civil penalty not to exceed $250,000 per violation.*

[84] Civil Code § 56.35

Section 56.36 (d) identifies the factors to be considered when assessing administrative fines or civil penalties.

> *(d) In assessing the amount of an administrative fine or civil penalty pursuant to subdivision (c), the Office of Health Information Integrity, licensing agency, or certifying board or court shall consider any one or more of the relevant circumstances presented by any of the parties to the case including, but not limited to, the following:*
>
> *(1) Whether the defendant has made a reasonable, good faith attempt to comply with this part.*
> *(2) The nature and seriousness of the misconduct.*
> *(3) The harm to the patient, enrollee, or subscriber.*
> *(4) The number of violations.*
> *(5) The persistence of the misconduct.*
> *(6) The length of time over which the misconduct occurred.*
> *(7) The willfulness of the defendant's misconduct.*
> *(8) The defendant's assets, liabilities, and net worth.*

Note that individuals have the right to bring suit to redress a violation of their privacy rights. The facts of each case drive the outcome of private lawsuits in which plaintiffs seek compensation for damages suffered as a result of an alleged violation of their privacy rights under the Confidentiality of Medical Information Act and the State Constitution. The cases turn on whether the plaintiff had a reasonable expectation of privacy under the law and whether the defendant's actions were within the scope of use or disclosure of confidential information permitted by the statute.

Even when a disclosure of medical information is permitted, the Courts will examine the circumstances to be sure that the disclosure was within the scope authorized by statute or authorized by the plaintiff. Consider, for example, *Pettus v. Cole*[85] a 1996 decision of the California Court of Appeals. In the *Pettus* case, an employee sought a leave from work due to a disabling stress-related condition and was examined by a psychiatrist. The psychiatrist not only reported to the employer about whether or not the employee suffered a disabling stress-related condition, but also, without the consent of the employee, disclosed to the employer that the employee's problems were the result of alcoholism. The California Court of Appeals found that the disclosure of the employee's alcoholism gave rise to a claim under the Confidentiality of Medical Information Act and the Privacy Clause of California Constitution, saying:

> *"[I]t is important to note that even the permissive disclosure exceptions do not always allow full disclosure of all medical information. The exceptions recognize that in some circumstances a legitimate need for access to medical information may conflict with an individual's interest in keeping that*

[85] (1996, Cal App 1st Dist) 49 Cal App 4th 402, 57 Cal Rptr 2d 46, 1996 Cal App LEXIS 858, rehearing denied (1996, Cal App 1st Dist) 50 Cal App 4th 328B, 1996 Cal App LEXIS 975, review denied (1996, Cal) 1996 Cal LEXIS 7258

information confidential, and attempt to strike a balance. Thus, under some of the exceptions described in [Civil Code] section 56.10, subdivision (c)(1) through (14) the Legislature established parameters within which disclosure is permissible and allowed disclosure of only that information which is necessary to achieve the legitimate purpose addressed by the particular exception."[86]

This is consistent with the standards of both HIPAA and 42 CFR Part 2 that disclosures of confidential medical information should be limited to that which is necessary to accomplish the purposes of the disclosure.

[Continued on following page}

[86] See also, California Consumer Health Care Council v. Kaiser Foundation Health Plan, Inc., 142 Cal. App. 4th 21; 47 Cal. Rptr. 3d 593; 2006

1.11 Disclosures to Health Information Exchange Organizations

1.11.1 Generally

As the United States moves towards establishment of health information exchanges, each state is confronted with the question of whether or not to require consumer consent to the disclosure of information to the exchange and the type of consent required, if any. Most analyses of this issue are based on an assumption that the HIE will be a repository model, meaning that providers will send patient health records to the exchange, which will hold the record and disclose it to other participating providers upon request.

Melissa Goldstein, JD of the Department of Health Policy of George Washington University has written an excellent white paper about this issue, which was published by the Office of National Coordinator for Health Information Technology on March 23, 2010. The white paper begins by noting the complexity of the problem:

> *The current landscape of possible consent models is varied, and the factors involved in choosing among them are complex. States and other entities engaged in facilitating the exchange of electronic health information are struggling with a host of challenges, chief among them the establishment of policies and procedures for patient participation in their exchange efforts. While some have adopted policies enabling patients to exercise individual choice, others have prioritized the needs and concerns of other key stakeholders, such as providers and payers…*
>
> *Core consent options (abbreviated) for electronic exchange include the following:*
>
> · *No consent. Health information of patients is automatically included—patients cannot opt out;*
>
> · *Opt-out. Default is for health information of patients to be included automatically, but the patient can opt out completely;*
>
> · *Opt-out with exceptions. Default is for health information of patients to be included, but the patient can opt out completely or allow only select data to be included;*
>
> · *Opt-in. Default is that no patient health information is included; patients must actively express consent to be included, but if they do so then their information must be all in or all out; and*
>
> · *Opt-in with restrictions. Default is that no patient health information is made available, but the patient may allow a subset of select data to be included.*
>
> *As these definitions illustrate, a range of consent models can be applied in different contexts of electronic exchange in the U.S., and it is possible for there to be further permutations depending on the level of choice granularity allowed. There is also considerable variation in the type of information exchanged, ranging from the more basic (e.g., lab results) to the more mature and complex (e.g., a wide array of health information).*

The consent model selected for electronic exchange, as well as the determination of which types of health information to exchange, affects many stakeholders (e.g., patients, providers, and payers). These decisions also have consequences for national policy goals, such as improving the quality of healthcare, promoting public health, engaging patients in their health care, and ensuring the privacy and security of personal health information. This discussion requires not only an appreciation of the sometimes competing interests of various stakeholders, but also consideration of the interests of the individual relative to those of society as a whole.

Provider and patient participation in electronic exchange have been identified as key challenges–both patient and provider participation are desired to facilitate better care delivery and advance other societal goals (e.g., improved public health), as well as to ensure the viability and utility of the exchange. To enhance patient participation, numerous electronic exchanges have employed one or more of the following tactics:

- *Active engagement of patients in the development of the exchange entity;*
- *Vigorous marketing of exchange efforts through effective channels;*
- *Initial and ongoing education (largely from providers) about the effort; and*
- *Adoption of an opt-out or no-consent model, in concert with tight restrictions on data access and / or use, including stringent penalties for misuse.*

In addition, these electronic exchanges have employed the following methods of ensuring adequate provider participation:

- *Minimization of administrative burdens, sometimes coupled with financial or other incentives;*
- *Maximization of value (i.e., access to as much useful information as possible, as often as is needed); and*
- *Provision of key infrastructure and service components (e.g., a record locator service or consent management tool).*

Other issues of particular significance with regard to progress (or lack thereof) toward the greater proliferation of electronic exchange include:

- *Numerous and sometimes inconsistent federal and state laws regarding patient consent generally, and disclosure of sensitive information specifically;*
- *Provider workflow challenges associated with obtaining and managing consent;*
- *The lack of (or difficulty in achieving) technical and procedural capacity to segment and manage data in the manners desired by various constituents;*
- *The concern that existing security and privacy provisions are inadequate; and*
- *The need to balance multiple and often conflicting stakeholder interests to ensure adequate participation.*

At present, the evidence from emerging electronic exchanges is insufficient to determine the consequences associated with policy decisions that allow for greater or lesser levels of patient choice with regard to the

electronic exchange of their data. There are early signs that consent models at both ends of the spectrum can generate sufficient patient and provider participation to achieve the critical mass necessary for system function and the realization of key goals. However, in any consent model the role of other factors, such as the accompanying level of dedicated human and financial resources, policy development, and other necessary supports, must also be considered. Due to the complexity of issues involved in selecting and applying a particular consent model, appropriate guidance in the form of higher-level principles or recommendations is critical to moving forward… While this document represents a starting point for discussion related to consent, it is imperative that future deliberations are informed by further research regarding the effectiveness and impact of various consent options, consideration of the broader policy landscape, and assessment of the needs of those most affected by the consent decision. Until the time when we are confident that we can protect health information in a systematic and thorough way, prudent use of the mechanism of consent appears to be one of the most reliable ways to pursue that goal.

1.11.2 California.

In 2010, California was awarded $38.8 million dollars under the HITECH Act to support electronic health information exchange development in the State.[87] As a condition of the federal grant, the State is required to develop privacy and security rules appropriate for the electronic exchange of individual health information. In response to this requirement, the State has enacted a law authorizing the Director of the California Office of Health Information Integrity (CalOHII) to establish and administer demonstration projects to determine how best to protect privacy in accordance with State and Federal laws while enabling electronic health information exchange.[88]

The California legislature declared its findings and the intent of this law as follows:

(a) There is a need to enhance California's ability to obtain and use federal funding, as awarded in the State Cooperative Grant Agreement for health information exchange, for the establishment of statewide health information exchange infrastructure in California. The California Health and Human Services Agency is authorized by the Legislature, under Section 130255, to use those federal funds to achieve that purpose.

(b) Health information exchange has the potential to significantly improve the quality of treatment and care, reduce unnecessary health care costs, and increase administrative efficiencies within the health care system. The application of health information exchange technology to manage health information will also have a significant impact on consumers, health care facilities, and licensed health care providers.

---

[87] ONC supports state and regional level efforts to achieve health information exchange through grants authorized by the HITECH Act (Title XIII of the American Recovery and Reinvestment Act of 2009), and seeks to align state efforts with the national health IT agenda through a number of initiatives, including the Health Information Security and Privacy Collaboration (HISPC). Adoption and "meaningful use" of health information technology by physicians and hospitals is supported by incentive payments available under the Medicare or Medicaid programs.

[88] Stat. 2010 Ch. 227, codified at California Health and Safety Code § 130275 et seq.

(c) Current laws may not adequately protect privacy, or may impose obstacles to the exchange of vital health information, as required by the State Cooperative Grant Agreement for health information exchange and other federal health information funding programs.

(d) It is the intent of the Legislature to authorize the Office of Health Information Integrity within the California Health and Human Services Agency to establish and administer demonstration projects funded by federal grants and other sources. It is the intent of the Legislature that the demonstration projects do all of the following:

(1) Identify barriers to implementing health information exchanges.

(2) Test potential security and privacy policies for the safe and secure exchange of health information, including, but not limited to, issues related to access to, and storage of, individual health information.

(3) Identify and address differences between state and federal laws regarding privacy of health information.[89]

The statute authorizes CalOHII to approve up to four demonstration projects annually. Health care entities or governmental authorities are permitted to submit applications to be approved as demonstration project participants. CalOHII is permitted to approve demonstration projects to test (among other things):

(1) Policies and practices related to patient consent, informing, and notification.

(2) New technologies and applications that enable the transmission of protected health information, while increasing privacy protections by ensuring only required health data is transmitted for purposes and uses consistent with state and federal law.

(3) Implementation issues, if any, encountered by small solo health care providers as a result of exchanging electronic health information.

The Director of CalOHII is also authorized to:

[A]dopt regulations to ensure all approved health information exchange service participants and demonstration project participants follow rules, and work within parameters, as defined by the office, that are consistent for the exchange of information.[90]

CalOHII published proposed regulations on March 1, 2011. As of May 5, 2011, final regulations had not been published. CalOHII made some interesting comments about the challenge of

[89] CA Health and Safety Code § 130275

[90] CA Health and Safety Code § 130277

protecting privacy in electronic health information exchange in an Initial Statement of Reasons for the Proposed Regulations.

> *CalOHII has the general authority to enforce State laws mandating the confidentiality of medical information. These projects will test policies and rules to better inform the State and health care stakeholders while the HIEO infrastructure is being defined over the next several years. By allowing for various HIEO demonstration projects, it will be possible to determine how best to protect privacy in accordance with State and Federal laws while enabling electronic health information exchange…*
>
> *CalOHII concluded, in its work with Phase I, II and III in Health Information Security and Privacy Collaboration (HISPC) and in the work of the California Privacy and Security Advisory Board (CalPSAB) that health care stakeholders do not agree on the lawfully permitted disclosures and uses of health information. This problem is long standing and intrinsic in the structure of the applicable laws, due in part to:*
>
> - *the potential preemptions of State laws by HIPAA,*
> - *a lack of clarity in the laws in both the Federal and State arenas, and*
> - *the permitted flexibility in implementation of security safeguards under HIPAA…*
>
> *Evolving patient-centric provider configurations and reimbursement methodology need to be supported by robust, interoperable health record systems. Privacy concerns arise because of the liquidity of the information and the lack of transparency in the sharing of that information. The need to foster innovation and experimentation in health information exchange should not be hamstrung by too stringent, proscriptive regulation in this developing area. But in order to foster trust amongst patients, providers, and other health care entities, and to allow for the expansion of health information exchange, rules are needed to protect privacy and to set a baseline for security. Development currently is stymied by the lack of clarity on privacy and security issues. The field cannot develop further until privacy and security issues are resolved, but no progress will be made if the privacy and security solutions are too specific, are based upon obsolete technology, or are inadequate to stop inappropriate business practices that are undetectable because of the lack of transparency and oversight.*
>
> *These privacy and security requirements for HIE are being created in an iterative fashion, applicable for a limited time frame, and are based upon the real use of individual health information (IHI). The goal of the demonstration projects is to increase transparency and knowledge of the use of IHI and from this knowledge build a set of requirements for HIE that can evolve as the technology evolves. Through the CalPSAB process, consensus was reached on:*
>
> - *Core principles of fair information practices;*
> - *An initial limited scope of health information exchange, with the goal to develop further capacity with a growth in understanding the privacy and security implications;*
> - *The need for affirmative consent during this development phase; and*
> - *That more work was needed to better define what were appropriate secondary uses of IHI.*
>
> *There is a need for a flexible approach to protecting privacy while enabling innovation in HIE. These regulations, and future amendments, are intended to provide a ground floor of policy to promote for*

further development and deployment of privacy enhancing technologies to ensure compliance with State and Federal laws mandating the confidentiality of individual health information.

The Proposed Regulations require HIE Demonstration Project Applicants to provide CalOHII with copies of their Notice of Privacy Practices, Data Use Agreements, and consumer complaint mechanisms and related educational materials. If an Applicant is approved, it must disclose each participant's business associates and trading partners, the types of data shared and the purpose of disclosure of that data to the business associate or trading partner, and whether those partners are permitted further use or disclose the information.

The Proposed Regulations would apply to any health information exchange, including exchanges through a RHIO and "Direct Exchange" through "(1) A direct connection between the electronic health record systems of health care providers; or (2) From a health care provider or entity to another health care provider or entity utilizing national or state standards, services, and policies including but not limited to the standards, services and policies of the Direct Project of the National Health Information Network".[91] In its explanation of the Proposed Regulations, CalOHII says:

...[T]he differences between having IHI exchanged through an HIO and a direct exchange are not significant. The risk of overly broad and unnecessary disclosures and the potential questionable secondary uses and unauthorized access are the same. The only difference is the additional link through a third party intermediary ...

The Proposed Regulations permit "individual health information" to be exchanged or accessed through an HIO or a direct exchange only for the purposes of "(1) Treatment (2) Reporting to Public Health Officials for immunizations, bio-surveillance and mandated reporting. (3) Quality reporting for meaningful use to Centers for Medicare and Medicaid Services and the California Department of Health Care Services."[92] The term "Treatment" is very broadly defined to mean:

[T]he provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers related to a patient; or the referral of a patient for health care from one health care provider to another.[93]

Before requesting an individual or an individual's personal representative to permit the electronic exchange of health information, an entity shall provide a notice describing:

(A) Electronic exchange of health information;

(B) Uses of data exchanged using electronic health information exchange;

[91] Proposed regulation section 126020(g).

[92] Proposed regulation section 126050

[93] Proposed regulation section 126020(t)

(C) Benefits and risks associated with electronic health information exchange, including the exchange of sensitive health information, such as HIV status, mental health records, reproductive health records, drug and alcohol treatment records, and genetic information which could be inferred or embedded in information that is made available in the exchange;

(D) Consent requirements for electronic health information exchange;

(E) Specific exceptions to the consent requirements for electronic health information exchange for mandated public health reporting;

(F) Specific exceptions to the consent requirements for electronic health information exchange in emergency situations;

(G) Process for revoking consent, including a contact name, phone number, email address, and website; and

(H) When the revocation of consent is effective[94].

Most importantly, the Proposed Regulations require that before an individual's health information is electronically exchanged an entity must obtain "written affirmative consent documenting the individual's or the individual's personal representative's choice to electronically exchange the individual's individual health information."[95] The consent must be revocable. There is no requirement of a time limit or expiration event for the consent.

The consent to electronic health information exchange must be obtained in addition to other legally required authorizations to disclose health information. The Proposed Regulation does not address the issues of whether the consent to disclose information electronically can be given once, and remain in effect for all future exchanges until revoked, or whether the permission for electronic exchange can be combined with other permissions to disclose health information.

The Proposed Regulation permits electronic exchange of health information without consent in a medical emergency and for mandated public health reporting.

Finally, the Proposed Regulation requires participants in HIE Demonstration Programs to meet data security requirements that are very similar to those set forth in the HIPAA Security Rule.[96]

1.11.3 Disclosure of Alcohol/Drug Program Records through an HIEO

The *Frequently Asked Questions - Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIEO)* document published by SAMHSA provide some clarification regarding the disclosure of alcohol/drug program records through an HIEO.

---

[94] Proposed regulation section 126060(a)

[95] Proposed regulation section 126060(b)

[96] Proposed regulation section 126070

Ordinarily, patient consent is required for disclosure of substance abuse program records to or through an HIEO. However, if the substance abuse program and the HIEO enter a Qualified Services Organization Agreement, the substance abuse program will be permitted to disclose patient records to the HIEO without patient consent. But further disclosures by the HIEO to third parties will be subject to 42 CFR Part 2, which means that patient consent will be required for disclosures to the third party through the HIEO.

In medical emergencies, it is permissible to "break the glass" and disclose patient information to a treating clinical provider as needed. It is necessary for the treating clinical provider to document that an emergency existed, the nature of the emergency, and to whom the information is disclosed. This information must be entered in the medical record maintained by the originating substance abuse program. The FAQs do not describe the mechanism to be used to transfer information from the treating provider to the originating provider.

1.11.4 DURSA

In November 2009, the National Health Information Network Cooperative published the Data Use and Reciprocal Support Agreement (DURSA), a comprehensive agreement that would govern the exchange of health data through the National Health Information Network (NHIN). The DURSA is a multi-party agreement, a single agreement that establishes the rules of engagement and obligations to which all NHIN Participants agree and that all NHIN Participants sign as a condition of joining the community. The "Participants" are NHIN approved Health Information Exchanges, Integrated Delivery Systems, States and federal government agencies. The DURSA Participants in turn enter agreements with "Participant Users" of the National Health Information Network (including health care providers), obligating Participant Users to follow the DURSA terms and conditions with regard to the exchange of health information through the NHIN.

The DURSA does not override applicable privacy laws, including HIPAA, more stringent state laws and 42 CFR Part 2. It establishes a process for authentication of the identity of "Recipients" of health information, transmission of requests for information about individual patients ("Message Content"), and responding to such requests. Requesting Recipients are required to represent that they are requesting information for a "Permitted Purpose" (treatment, payment, health care operations, public health activities, quality improvement required to meet meaningful use standards), and transmitting a copy of the Authorization (Consent) if that is the sole legal basis for the Permitted Purpose. The Responding Participant is required to respond to all authenticated messages that seek "Message Content" for treatment purposes. The Responding Participant is also required to ensure that any requirements of applicable law, including obtaining consent or authorization for disclosure, have been met before making the Message Content available for exchange through the NHIN.

Note that DURSA does not set technical standards for the completion of transactions such as requests for information, acknowledgement of receipt of requests, or transmission of requested data. Nor does it establish a standard form for recording a valid consent to release health information.

The DURSA is necessary for any HIEO that wishes to participate in the National Health Information Exchange Network.

The provisions of DURSA are summarized in the following overview published by the Office of the National Coordinator for Health Information Technology at www.hhs.gov/healthit/nhin on November 30, 2009.

> *As part of ongoing work on the Nationwide Health Information Network ("NHIN") Trial Implementations – Option Year 1, a large, multi-stakeholder team was assembled to develop a comprehensive agreement that would govern the exchange of health data across a diverse set of public and private entities. This agreement – the Data Use and Reciprocal Support Agreement ("DURSA") – is a comprehensive, multi-party trust agreement that will be signed by all entities who wish to exchange data on a nationwide basis ("Participants"). The DURSA provides the legal framework governing participation in nationwide information exchange by requiring the signatories to abide by a common set of terms and conditions that establish the Participants' obligations and the trust fabric to support the privacy, confidentiality and security of the health data that is exchanged.*
>
> *Key terms and conditions of the DURSA are summarized below. This summary is not all inclusive nor does it attempt to address all of the intricacies in the DURSA that have been memorialized in carefully crafted contract language. Instead, it is offered as a basic overview of the DURSA to help facilitate review of the agreement.*
>
> • ***Multi-Party Agreement.*** *The DURSA must accommodate and account for a variety of Participants so that it can successfully serve as a multi-party agreement among all Participants. This multi-party agreement is critical to avoid the need for each Participant to enter into "point-to-point" agreements with each other Participant, which becomes exceedingly difficult, costly and inefficient as the number of Participants increases.*
>
> • ***Participants in Production****. The DURSA expressly assumes that each Participant is in "production" and, as a result, already has in place trust agreements with or written policies applicable to its end users. These end user trust agreements and policies support the trust framework memorialized in the DURSA.*
>
> • ***Privacy and Security Obligations****. To the extent that each Participant has existing privacy and security obligations under applicable law (e.g. HIPAA or other state or federal privacy and security statutes and regulations), the Participant is required to continue complying with these obligations. Participants, which are neither HIPAA covered entities, HIPAA business associates nor governmental agencies, are obligated to comply with specified HIPAA Privacy and Security Rules as a contractual standard of performance.*[97]

[97] While the DURSA requires participants to respect applicable privacy laws, it does not specify procedures for compliance with laws that are more stringent than HIPAA, such as 42 CFR Part 2.

• *Requests for Data Based on Permitted Purposes*. *Participant's end users may only request information through the NHIN for "Permitted Purposes," which include treatment, limited purposes related to payment, limited health care operations with respect to the patient that is the subject of the request, specific public health activities, quality reporting for "meaningful use" and disclosures based on an authorization from the individual.*

• *Duty to Respond*. *Participants that allow their respective end users to seek data through the NHIN for treatment purposes have a duty to respond to requests for data for treatment purposes. This duty to respond means that the Participant will send a standardized response to the requesting Participant, which may or may not include the actual data requested. Participants are permitted, but not required, to respond to all other (non-treatment) requests. The DURSA does not require a Participant to disclose data when such a disclosure would violate applicable law or conflict with any restrictions an individual may have placed on the data in accordance with the HIPAA Privacy Rule.*

• *Future Use of Data Received Through the NHIN*. *Once the Participant or Participant's end user receives data from a responding Participant (i.e. a copy of the responding Participant's records), the recipient may incorporate that data into its records and retain that information in accordance with the recipient's record retention policies and procedures. The recipient can re-use and re-disclose that data in accordance with all applicable law and the agreements between a Participant and its end users.*

• *Duties of Requesting and Responding Participants*. *Each Participant has certain duties when acting as a requesting or responding Participant.*

o *When responding to a request for data, Participants will apply their local policies to determine whether and how to respond to the request. This concept is called the "autonomy principle" because each Participant can apply its own local policies before requesting data from other Participants or releasing data to other Participants.*

o *It is the responsibility of the responding Participant – the one disclosing the data – to make sure that it has met all legal requirements before disclosing the data, including, but not limited to, obtaining any consent or authorization that is required by law applicable to the responding Participant. This policy is essential for nationwide health information exchange given the number of different state laws, Federal statutes and local policies related to consent or authorization to exchange data for treatment purposes. To effectively enable the exchange of health information in a manner that protects the privacy, confidentiality and security of the data, the DURSA adopts the HIPAA Privacy and Security Rules as minimum requirements.*

o *Under HIPAA, data can be exchanged for treatment purposes without obtaining a separate consent or authorization. Under some state laws and other Federal laws, however, patient consent or authorization is required to exchange data for treatment. Responding Participants who are subject to these more restrictive laws will be required to obtain those consents or authorizations that they deem necessary under their applicable laws before sending data through the NHIN. As the DURSA is written, the responsibility for obtaining this consent or authorization will not fall to the requesting*

Participant, usually a healthcare provider, because there is simply no way for the requesting healthcare provider to keep track of the rapidly changing laws and regulations in every state. It is unlikely that even patients will know what specific consent forms may be required for data exchange by their local Health Information Exchange {Orgaanization] (HIEO). Requiring the requesting Participant to obtain a consent or authorization that complies with the responding Participant's applicable law would create an undue burden on requesting Participants. Essentially, this would require the requesting Participant to track the laws of all 50 states and federal laws beyond HIPAA and have consent or authorization forms that meet each individual state's requirements. Instead, it is more reasonable to expect each responding Participant to remain current on the legal requirements to which it is subject and take steps to comply with those laws.

o When a request is based on a purpose for which authorization is required under HIPAA (e.g. for SSA benefits determination), the requesting Participant must send a copy of the authorization with the request for data. As described in the bullet above, requesting Participants are not obligated to send a copy of an authorization or consent when requesting data for treatment purposes.

• *NHIN Coordinating Committee. The NHIN Coordinating Committee will be responsible for accomplishing the necessary planning, consensus building, and consistent approaches to developing, implementing and operating the NHIN, including playing a key role in NHIN breach notification; dispute resolution; Participant membership, suspension and termination; NHIN operating policies and procedures; and, will inform the Technical Committee when proposed changes for interface specifications have a material impact on Participants.*

• *NHIN Technical Committee. The NHIN Technical Committee will be responsible for determining priorities for the NHIN and creating and adopting specifications and test approaches. The NHIN Technical Committee will work closely with the NHIN Coordinating Committee to assess the impact that changes to the specifications and test approaches may have on Participants.*

• *Breach Notification. Participants are required to promptly notify the NHIN Coordinating Committee and other impacted Participants of breaches which involve the unauthorized disclosure of data through the NHIN, take steps to mitigate the breach and implement corrective action plans to prevent such breaches from occurring in the future. Suspected breaches must be reported within one (1) hour of discovering information that leads the Participant to believe that a breach may have occurred. As soon as reasonably practicable, but no later than twenty-four (24) hours, Participants must notify affected Participants and the NHIN Coordinating Committee This process is not intended to address any obligations for notifying consumers of breaches, but simply establishes an obligation for Participants to notify each other when breaches occur to facilitate an appropriate response.*

• *Mandatory Non-Binding Dispute Resolution. Because the disputes that may arise between Participants will be relatively complex and unique, the Participants will agree to participate in a mandatory, non-binding dispute resolution process.*

• *Allocation of Liability Risk. With respect to liability, the DURSA memorializes the Participant's understanding that each Participant is responsible for its own acts or omissions.*

• ***Applicable Law***. *The DURSA reaffirms each Participant's obligation to comply with "Applicable Law." As defined in the DURSA, "Applicable Law" is the law of the jurisdiction in which the Participant operates. For non-Federal Participants, this means the law in the state(s) in which the Participant operates and any applicable Federal law. For Federal Participants, this means applicable Federal law.*

Note that regulations proposed by the California Office of Health Information Integrity for HIEO Demonstration Programs require participating organizations to enter "Trading Partner Agreements" relating to the exchange of information in electronic transactions. The proposed regulations do not specify the terms of such an agreement.

1.12 Rights of Individuals

As noted earlier, the HITECH Act specifically designates health information organizations as business associates of the covered entities with which they contract. As a business associate, the HIO/HIEO will be required to comply with the HIPAA Security Rule and most of the provisions of the HIPAA Privacy Rule. It will also be required to cooperate with the covered entities in responding to requests by individuals for the exercise of rights granted by the HIPAA Rules and by the HITECH Act.

1.12.1 Right to Accounting of Disclosures

The current HIPAA Privacy Rule, at 45 CFR 164.528, requires covered entities, upon request, to give individuals an accounting of any disclosure of the individual's protected health information in the 6 years preceding the request. There are a number of exceptions to this rule, the most significant of which is that no accounting is required for disclosures of PHI for purposes of treatment, payment or health care operations. Section 13405(c) of the HITECH Act revises this rule when the disclosure is through an electronic health record. A covered entity that uses an electronic health record will be also obligated to maintain a record and provide an accounting of disclosures for purposes of treatment, payment and health care operations during the 3 years preceding the request.

The Act requires DHHS to issue regulations on what information must be collected about each disclosure for purposes of treatment, payment or health care operations, taking into consideration the interests of individuals and the administrative burden on covered entities. This subject was not addressed in the DHHS July 14, 2010 Notice of Proposed Rulemaking that proposed modifications to the HIPAA rules. Presumably, this is because the new accounting requirement does not take effect until January 1, 2014, unless the covered entity adopts the EHR after January 1, 2009, in which case the requirement becomes effective after January 1, 2011.

The Act describes the process to be followed in response to a request for an accounting. It allows a covered entity to either: (1) providing an accounting of disclosures by the covered entity and its business associates, or (2) provide an accounting of disclosures by the covered entity, and provide a

list of all business associates acting on behalf of the covered entity, including contact information for the business associate. The Act then requires a business associate included on a list provided by the covered entity to provide an accounting of disclosures for purposes of treatment, payment or health care operations directly to an individual upon request.

1.12.2 Right to Request Restriction on Disclosures

Section 13405(a) of the HITECH Act requires a covered entity to honor the request of an individual that PHI not be disclosed to a health plan if the disclosure is for purposes of payment or health care operations (and not for purposes of treatment) and if the health care provider has been paid out of pocket in full. This provision became effective February 17, 2010. In its July 14, 2010 Notice of Proposed Rulemaking, DHHS proposes amendments to 45 CFR 164.522 to implement this requirement.[98] Note that the NPRM says that DHHS enforcement of new regulations required by the HITECH Act will not begin until 180 days after the final regulation becomes effective.

1.12.3 Access to Information in Electronic Format

45 CFR 164.524 gives individuals the right to request a copy of protected health information maintained by a covered entity. Section 13405(e) of the HITECH Act requires covered entities that have electronic health records to provide that information in electronic format upon request. It limits the fees that may be charged for preparation of the record to the labor costs incurred by the covered entity in responding the request. The July 14, 2010 NPRM proposes amendments to 45 CFR 164.524 to implement this rule. The covered entity must provide the record in the format requested by the individual if it is readily producible in that format, or if not in readable electronic form (such as a PDF file) or other form as may be agreed upon by the individual and the covered entity.

Note that the final rule governing Medicare and Medicaid incentive payments to eligible professionals and eligible hospitals that make meaningful use of electronic health records includes as a core requirement that patients are provided with an electronic copy of their health information (including diagnostic test results, problem list, medication lists, medication allergies) within three business days of a patient's request. It includes a "menu set" standard that patients be allowed electronic access to their health information (through a secure web portal or otherwise) within four days of entry of information into the EHR.[99]

[Continued on following page.]

[98] 75 Federal Register 40923

[99] 42 CFR 495.6

1.13 Breach Notification

1.13.1 Introduction

The HITECH Act requires covered entities to notify affected individuals, the media, and the Secretary of Health and Human Services without unreasonable delay and no later than 60 days after discovery of a breach of unsecured protected health information. Business Associates are required to provide such notice to covered entities.[100] Failure to comply with these requirements can result in civil enforcement actions by the Department of Health and Human Services or State Attorneys General, including substantial civil monetary penalties.

The Act also requires Vendors of Personal Health Records and related entities to notify affected individuals, the media, and the Federal Trade Commission (FTC) in the event of a breach of security of "PHR Identifiable Information". Third parties that provide services to PHR Vendors or related entities to support the offering of personal health records or related services are required to notify the PHR Vendor or related entity of a breach. Failure to comply with the requirements of the Act and the implementing regulations enacted by the FTC can result in an enforcement action by the FTC on the grounds that the vendor is engaged in an unfair or deceptive trade practice.[101]

The Department of Health and Human Services and the Federal Trade Commission have each issued interim final regulations to implement the breach notification requirements of the Act.

A PHR vendor that is a business associate of a covered entity and also offers personal health records to the public is obligated to comply with both the DHHS and the FTC rules. DHHS and the FTC consulted with one another to avoid conflicting regulatory requirements in such cases. While the regulatory standards of the two sets of rules are nearly the same, they are not identical.

1.13.2 Reporting of Security Breaches – HIPAA Covered Entities and Business Associates

The HITECH Act requires HIPAA covered entities and business associates to provide notice of a "breach" of "unsecured protected health information". These are defined terms. It is important to study them carefully because notice is not required if a "breach" has not occurred or if the protected health information was secured in accordance with federal standards.

The term ''unsecured protected health information'' means protected health information that is not secured through the use of a technology or methodology specified in guidance published by the Secretary of Health and Human Services.[102] In the absence of such guidance, the term means "protected health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and is

[100] HITECH Act §13402

[101] HITECH Act §13407

[102] HITECH Act § 13402(h)(1)(A)

developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute".[103]

The Secretary was required to issue guidance about technologies and methods to secure protected health information within sixty days of enactment of the Act, and did so in April 2009.[104] She is required to update that guidance annually. [105] The guidance was updated and republished in the Interim Final Rule.[106] The Secretary's guidance states that PHI is rendered unusable, unreadable or indecipherable to unauthorized individuals if one or more of the following applies:

(a) Electronic Personal Health Information is encrypted using an algorithmic process as specified in the HIPAA Security Rule.[107] The confidential process or encryption key required for decryption must be stored on a device or at a location separate from the encrypted data. Encryption processes tested and approved by the National Institute of Standards and Technology (NIST) are judged to meet this standard. They are as follows:

- Data at Rest: NIST Special Publication 800-111 – Guide for Storage Encryption Technologies for End User Devices

Note that the DHHS Rule says that NIST is developing security guidelines for enterprise level storage devices, and that such guidelines will be considered updates to this DHHS guidance when they are available.

- Data in Motion: NIST Special Publication 800-52 Guidelines for Selection and Use of Transport Layer Security (TLS) Implementations, or
- NIST Special Publication 800-77 Guide to IPSec VPNs, or
- NIST Special Publication 800-113 Guide to SSL VPNs, or
- Federal Information Processing Standards (FIPS) 140—2 validated

(b) The media on which the protected health information is stored or recorded have been destroyed in one of the following ways:

Paper, film or other hard copy media have been shredded or destroyed such that PHI cannot be read or otherwise reconstructed. Redaction is specifically excluded as a means of data destruction.

---

[103] HITECH Act § 13402(h)(1)(B)

[104] 74 Federal Register 19006, April 27, 2009

[105] HITECH Act § 13402(h)(2)

[106] 74 Federal Register 42742

[107] 45 CFR 164.304

Electronic media have been cleared, purged or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitation*.

Definition of Breach

The term "breach" is defined at HITECH Act §13400(1) to mean "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information".

In the Interim Final Rule, the Department of Health and Human Services interpreted this section to mean that a breach occurs when there is a use or disclosure of unsecured PHI that is not permitted by the HIPAA Privacy Rule that "poses a significant risk of financial, reputational, or other harm to the individual".[108] Addition of this harm threshold is intended to ensure consistency of the HIPAA breach notification requirement with State breach notification laws and the obligations of Federal agencies pursuant to OMB Memorandum M-07-16.[109]

To determine if an impermissible use or disclosure of PHI constitutes a breach, covered entities and business associates will need to conduct a risk assessment to determine if there is a significant risk of harm to the individual. This is a fact specific analysis, considering the nature of the information disclosed, the recipient of the information, whether the information or data was returned and other factors. For example, unauthorized disclosure of the fact that an individual was a patient of a general hospital, without diagnostic information, might not pose a significant risk of harm. But disclosure that the individual was treated for a psychiatric condition would create such a significant risk of harm to the individual's reputation. Loss of a laptop computer with unencrypted patient records would create a risk of harm, but if the computer is returned and it is determined that the records were not accessed, that risk would not be significant.

The covered entity or business associate has the burden of proving that an unauthorized use or disclosure of PHI did not create a substantial risk of harm to individuals.[110] For this reason, it is important to document the risk assessment.

The DHHS Rule includes a narrow exception for unauthorized disclosures of "limited data sets". The HIPAA Privacy Rule permits covered entities and business associates to enter data use agreements that allow the business associate to use protected health information to create a limited data set for use for research and other purposes. A limited data set is created by removing the 16 direct identifiers of individuals that are listed at 45 CFR 164.514(e), including name, address, social security number, account numbers, etc. This does not amount to complete de-identification of the protected health information, which requires removal of 22 possible identifiers (See 45 CFR

[108] 45 CFR 164.402(1)(i)

[109] 74 Federal Register 42744

[110] 45 CFR 164.414

164.514(b)). The DHHS Rule states that if a limited data set excludes direct identifiers and also excludes date of birth and zip code, then loss of that data would not constitute a "breach" because it would not compromise the security and privacy of the protected health information.[111] Otherwise, unauthorized access to, use, or disclosure of a limited data set should trigger a risk assessment, as described above.

The HITECH Act lists three exceptions to the term ''breach'' that encompass situations in which there is unintentional acquisition, access or use of PHI by individuals acting on behalf of a covered entity.[112] With slight modifications, these standards are repeated in the DHHS Rule at 45 CFR 164.402. The term "breach" does not include an unintentional acquisition, access, or use of protected health information by a member of the workforce or person acting under the authority of a covered entity or business associate if made in good faith and within the scope of authority and there is no further use or disclosure in a manner not permitted by the Privacy Rule. Nor does it include inadvertent disclosures to another person authorized to access PHI at the covered entity, business associate, or organized health care arrangement, again provided that there is no further unauthorized use or disclosure of PHI. Finally, it excludes unauthorized disclosures to third parties when there is a good faith belief that the person to whom the disclosure was made would not reasonably have been able to retain the information.

Notification of Individuals

A covered entity is required to notify each individual whose unsecured protected health information has been, or is reasonably believed to have been accessed, acquired, used or disclosed as a result of a breach without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.[113]

A breach is considered "discovered" as of the first day in which the breach is known, or with reasonable diligence would have been known, by a member of the workforce or agent of the covered entity other than the person who committed the breach.[114] "Because the covered entity or business associate is liable for failing to provide notice of a breach when it did not know – but with reasonable diligence would have known – of a breach, it is important for such entities to implement reasonable systems for discovery of breaches." Because knowledge of breach is attributed to the covered entity or business associate when it is known, or should have been known to a member of the workforce or agent, "it is important to ensure that workforce members are adequately trained and aware of the importance of timely reporting of privacy and security incidents and the consequences of failing to do so".[115] Note that when an agency relationship exists, the date of discovery is the date that the agent knew or should have known of the breach.

---

[111] 45 CFR 164.402

[112] HITECH Act § 13400(1)(B)(ii)

[113] HITECH Act § 13402, 45 CFR 164.404

[114] 45 CFR 164.404(a)(2)

[115] DHHS explanation of 45 CFR 164.404(a)(2), 74 Federal Register 42749

This is an issue that should be considered by covered entities in structuring business associate agreements and service agreements.

DHHS expects covered entities to make individual notifications as soon as reasonably possible. It assumes that covered entities will promptly investigate a suspected breach and take a reasonable time to investigate the circumstances surrounding the breach in order to collect and develop the information required to be included in the notice to affected individuals.[116] Once it has that information, notice must be provided without further delay. 60 days is the outer limit for provision of notice.

The notice must be written in plain language, and include the following elements, to the extent possible:

- A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known;

- A description of the types of unsecured protected health information that were involved in the breach (such as whether name, address, social security or account numbers, diagnosis, etc);

- Steps individuals should take to protect themselves from potential harm resulting from the breach;

- A brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

- Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an email address, Web site, or postal address.[117]

- Notification of individuals must be provided in writing by first class mail to the last known address of the individual, or, if the individual agrees to electronic notice, by electronic mail. It may be provided in one or more mailings as information becomes available.[118]

- If the covered entity knows that the individual is deceased and has the address of the next of kin or personal representative, it may send notice to that person. It is not necessary to provide substitute notice when an individual is deceased and the covered entity does not have contact information for the next of kin or personal representative.[119]

- If there is insufficient or out of date contact information that precludes written notice to one

[116] 45 CFR 164.404(b), explained at 74 Federal Register 42749

[117] 45 CFR 164.404(c)

[118] 45 CFR 164.404(d)(1)(i)

[119] 45 CFR 164.404(d)(1)(ii)

or more individuals, a substitute form of notice must be provided.[120] If there is insufficient information for fewer than 10 people, notice may be by telephone or other alternate form of notice.

- If there is insufficient information for 10 or more people, then the substitute notice must be in the form of a conspicuous posting on the home page of the covered entity's web site, or conspicuous notice in major print or broadcast media in geographic area where the individuals affected by the breach likely reside. The notice must include a toll-free number that remains active for at least 90 days where an individual can learn whether his or her information was included in the breach.[121] DHHS' regulatory impact statement anticipates that creation and staffing of the toll-free number to answer questions about breaches will be the most significant cost of compliance with the new rule.[122]

- In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured PHI, the covered entity may provide information to individuals by telephone or other means.

Notification to the Media

In the event of a breach affecting more than 500 individuals served by a covered entity who are residents of the same State or jurisdiction, notice must be provided to prominent media outlets serving that State or jurisdiction. It must be provided within the same timeline and include the same content as the notice to be provided to individuals.[123] Written notice to individuals is required even if notice to the media is also required. If substitute notice to more than 10 people is necessary, the notice to the media will satisfy the substitute notice requirement only if it includes all of the information required for the substitute notice, including the toll-free number.

The term "prominent media outlets" is not defined, but DHHS commentary says that it includes print or broadcast media serving the State or jurisdiction, sufficient to reach affected residents within the jurisdiction. For example, if all affected residents live a one city, notice to a local newspaper or local broadcast media would be sufficient. If affected residents are spread across media markets, multiple notices may be required. DHHS anticipates that notices will be provided in the form of press releases.

The DHHS commentary explains that the 500 individuals threshold for media notice links the number of affected individuals to a specific State and a specific covered entity. If a covered entity suffers a breach that affects 400 individuals in one State and 300 in another State, then notice to the media is not required. Similarly, if a business associate suffers a breach that affects more than

---

[120] 45 CFR 164.404(d)(2)

[121] HITECH Act § 13402(e)(1)(B), 45 CFR 164.404(d)(2)(ii)

[122] 74 Federal Register 42764

[123] HITECH Act § 13402(e)(2), 45 CFR 164.406

500 people in a single State, but fewer than 500 of those people are associated with a single covered entity, notice to the media is not required. [124]

Notification to the Secretary of Health and Human Services

Covered entities must notify the Secretary of Health and Human Services of breaches of unsecured protected health information. If a breach is with respect to 500 or more individuals, notice must be provided at the same time as notice is provided to individuals. The content of the notice is the same as that required for individual notice. Unlike media notification, the residence of the affected individuals doesn't matter. If 500 or more people are affected, notice must be given the Secretary without unreasonable delay and in no event later than 60 days after discovery of the breach.[125]

For breaches involving less than 500 individuals, the covered entity may maintain a log or other documentation of such breaches. Within 60 days after the end of any calendar year, the covered entity is required to submit to the Secretary a notice of the breaches that occurred during that year.[126]

DHHS intends to post instructions on its web site for submission of the required notices. As required by the section 13402(e)(4) of the HITECH Act, DHHS will publish on its web site a list of covered entities that submit reports of breaches involving more than 500 individuals.

Notification of Covered Entity by Business Associate

A business associate is required to notify each covered entity whose unsecured protected health information has been, or is reasonably believed to have been accessed, acquired, used or disclosed as a result of a breach without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.[127]

Notice must be provided only to those covered entities whose unsecured protected health information has been breached. It is not necessary to notify other covered entities served by the business associate. If the business associate is unsure about the scope of the breach, it would be required to notify all of the covered entities that could be affected.

The standard for determining when a breach is discovered are the same for business associates as for covered entities. A breach is considered discovered on the first day that a member of the

---

[124] 74 Federal Register 42752

[125] HITECH Act §13402(e)(3), 45 CFR 164.408(a). Note that the statute requires notice to the Secretary to be given "immediately". DHHS interpreted this requirement to mean that notice must be provided at the same time as notice is given to individuals.

[126] 45 CFR 164.408(b)

[127] HITECH Act §13402(b), 45 CFR 164.410

workforce or an agent of a business associate knew, or through the exercise of reasonable diligence should have known that a breach occurred.

Note that when a business associate is acting as an agent for a covered entity, the time period within which the covered entity must provide notice to individuals, the media and/or the Secretary begins when the business associate is considered to have discovered the breach. If an independent contractor relationship exists, the covered entity is considered to have discovered the breach when it receives notice from the business associate. The federal common law of agency is applied for purposes of determining whether an agency relationship exists. For example, a business associate authorized to act on behalf of a health plan in operation of a case management program would be considered to be an agent of the plan. But if the business associate is simply analyzing data and providing reports to the health plan, an agency relationship would not exist.

The timeframe for reporting breaches to the covered entity is the same as that which is applied for covered entity reports to individuals. The business associate must notify the covered entity without unreasonable delay and in any event no later than 60 days after discovery of the breach.[128]

The notice from the business associate to the covered entity must, if feasible, identify each individual who may be affected by the breach. The notice from the business associate to the covered entity must provide any other available information that the covered entity is required to provide in its notice to individuals affected by the breach. Additional information must be provided to the covered entity as it is discovered, even if that occurs after notice is provided to individuals.[129]

Business associates are not required by the rule to provide notice of breaches to individuals, the media, or the Secretary.

In its discussion of the new rule, DHHS took great pains to note that covered entities and business associates are free to structure business associate agreements in any manner they see fit, as long as the agreements meet the requirements of the HIPAA Privacy and Security Rules.[130] Business associate agreements can set specific time periods within which a business associate must provide notice to covered entities. A covered entity and a business associate are free to agree that in the event of a breach of unsecured protected health information maintained by the business associate, the business associate will act on behalf of the covered entity and provide all notices to individuals, the media, and the Secretary that the covered entity is required to provide.[131]

---

[128] 45 CFR 164.410(b)

[129] 45 CFR 164.410(c)

[130] 45 CFR 164.504(e)(2)(ii)(C) and 45 CFR 164.314(a)(2)(i)(C)

[131] 74 Federal Register 42754

Delay of Notification at the Request of a Law Enforcement Official

The HITECH Act and the DHHS Rule provide that if a law enforcement official determines that a notification of breach would impede a criminal investigation or cause damage to national security, the notification is to be delayed. If a covered entity or business associate a receives written statement from a law enforcement official requesting a delay for this reason, the breach notice is to be delayed for the time period specified by the law enforcement official. If the law enforcement official's request is communicated orally, but not in writing, the covered entity or business associate is required to document the request, and delay the required notice for thirty days. The time periods for compliance with the DHHS Notification Rule are tolled during the period that notice is delayed.[132]

Administrative Requirements

DHHS is requiring covered entities to comply with the administrative requirements of 45 CFR 164.530 with respect to the breach notification requirements. Covered entities will be required to amend their policies and procedures to incorporate the breach notification requirements, train workforce members, and have sanctions for failure to follow the requirements. In addition, they will be required to permit individuals to file complaints about these policies or a failure to comply with them and refrain from intimidating or retaliatory actions against individuals who do file complaints.[133]

Burden of Proof

Section 13402(d)(2) of the HITECH Act provides that following an impermissible use or disclosure of unsecured protected health information, the covered entity or business associate has the burden of demonstrating that all notifications were made as required, including evidence demonstrating the necessity of any delay. The DHHS rule restates this requirement at 45 CFR 164.414(b).

In the event of an impermissible use or disclosure of protected health information, it will be necessary to document that all required notifications were made. It will also be necessary to document any risk analysis that results in a determination by the covered entity or business associate that, despite the unauthorized use or disclosure of PHI, there was no "breach" of "unsecured protected health information" and notification is not required. It will also be necessary to document the reasons for any delay in making required notifications.

In an enforcement proceeding, covered entities and business associates have the burden of presenting evidence as well as the burden of persuasion to prove that all notifications were made as required.

---

[132] HITECH Act §13402(g), 45 CFR 164.412

[133] 45 CFR 164.414(a)

1.13.3 Reporting of Security Breaches – Vendors of Personal Health Records

Section 13407 of the HITECH Act is entitled: "Temporary Breach Notification Requirement for Vendors of Personal Health Records and Other Non-HIPAA Covered Entities". This section establishes requirements for notification of individuals, the media and the federal government in the event of a breach of unsecured individually identifiable health information in a personal health record. Enforcement is by the Federal Trade Commission rather than the Department of Health and Human Services.

The first thing to notice is use of the word "temporary" in the title of section 13407. The Act also requires the Department of Health and Human Services, in consultation with the Federal Trade Commission to conduct a study and issue a report to Congress by February 17, 2010 with recommendations as to which federal agency should have responsibility for oversight of PHR vendors and related organizations.[134] A "sunset" provision says that if Congress enacts new legislation establishing requirements for notification in the case of a breach of security that apply to entities that are not covered entities or business associates, section 13407 shall not apply to breaches of security discovered on or after the effective date of regulations implementing such legislation.[135] It would not be a surprise for DHHS to recommend and for Congress to enact a law that makes HIPAA applicable to organizations that maintain personal health records, even if those organizations are not covered entities or business associates of covered entities. In that event the DHHS rules described above would be applied. In the meantime, section 13407 is in force and the Federal Trade Commission rules must be followed where applicable.

Applicability

Section 13407 and the Federal Trade Commission rules apply to:

Vendors of personal health records, defined to mean an entity, other than a HIPAA covered entity or an entity to the extent that it acts as a business associate of a HIPAA covered entity that offers or maintains a "personal health record".[136]

"*PHR related entities*", defined to mean an entity, other than a HIPAA covered entity or an entity to the extent that it acts as a business associate of a HIPAA covered entity, that:

- Offers products or services through the website of a vendor of personal health records;
- Offers products or services through the websites of covered entities that offer individuals personal health records; or
- Accesses information in a personal health record or sends information to a personal health record.

[134] HITECH Act §13424(b)

[135] HITECH Act §13407(g)(2)

[136] HITECH Act §13400(18)

Third party service providers, defined to mean an entity that (i) provides services to a vendor of personal health records in connection with the offering of the personal health record or to a PHR related entity in connection with a product or service offered by that entity, and (ii) accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses unsecured PHR identifiable information as a result of such services.[137]

Notification Obligation - Generally

Upon discovery of a *breach of security* of *unsecured PHR identifiable health information* in a *personal health record*, a vendor of personal health records is obligated to notify each affected individual who is a citizen or resident of the United States and the Federal Trade Commission. PHR related vendors have the same obligation following the discovery of a breach of security of unsecured PHR identifiable information they have obtained.[138] Third party service providers are required to notify the appropriate vendor of personal health records or PHR related entity upon discover of a breach of security of PHR identifiable information in their possession.[139]

Personal Health Records, PHR Identifiable Information

The Act defines the term "*personal health record*" to mean an *electronic* record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.[140] Unlike the DHHS rules, which apply to unsecured protected health information in any form, the FTC rules only apply to electronic records of PHR identifiable health information.

"*PHR identifiable health information*" is defined in the Act and the FTC Rule to mean individually identifiable health information that is provided by or on behalf of the individual and that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.[141]

"*Individually identifiable health information*" has the same meaning as it does under HIPAA. It is 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 that identifies the individual or that can be used to identify the individual.[142]

---

[137] 16 CFR 318.2(d)

[138] HITECH Act §13407(a)

[139] HITECH Act §13407(b)

[140] HITECH Act §13400(11) (emphasis supplied), 16 CFR 318.2(d)

[141] HITECH Act §13407(f)(2), 16 CFR 164.318.2(e)

[142] 42 USC 1320d(6)

Unsecured PHR Identifiable Information

"*Unsecured PHR identifiable health information*" means PHR identifiable health information that is not protected through the use of a technology or methodology specified in guidance issued by the Secretary of Health and Human Services pursuant to section 13402(h)(2) of the HITECH Act.[143]

The Department of Health and Human Services has issued guidance as required by the Act. That guidance refers to the data security guidelines of National Institute for Standards and Technology. The specific guidelines are listed in the discussion of "Unsecured Protected Health Information", above.

Breach of Security

The HITECH Act defines the term "*breach of security*" to mean, with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information without the authorization of the individual.[144]

The Federal Trade Commission rule expands on this definition by adding…"Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information."

In its explanation of the Health Breach Notification Rule, the FTC gives examples of unauthorized acquisition of information, including the theft of a laptop containing unsecured records, unauthorized downloading or transfer of records by an employee, and the electronic break-in and copying of records by a hacker. It describes as a rebuttable presumption its requirement that *acquisition* will be presumed if there is unauthorized *access* to unsecured PHR information, explaining that the presumption was intended to address the difficulty of determining whether access to data (i.e., the opportunity to view the data) did or did not lead to acquisition (i.e., the actual viewing or reading of the data). In the example of the lost laptop, the presumption of acquisition could be rebutted if the laptop is returned and a forensic analysis demonstrates that the files with unsecured PHR identifiable health information were not opened.[145]

In case of inadvertent access to PHR identifiable health information by an employee, no breach notification is required if (1) the employee follows company policies by reporting such access to his or her supervisory and affirming that he or she did not read or share the data, and (2) the company conducts a reasonable investigation to corroborate the employee's version of events.[146]

---

[143] HITECH Act §13407(f)(3)

[144] HITECH Act §13407(f)(1)

[145] 74 Federal Register 42966

[146] 74 Federal Register 42967

There are very significant differences between the definition of "breach" in the DHHS rule and the definition of "breach of security" in the FTC rule. The DHHS rule requires notification of a breach when there is an authorized use or disclosure of unsecured PHI that "poses a significant risk of financial, reputational, or other harm to the individual". The FTC refused to incorporate the requirement of a risk of harm to an individual into its definition of breach of security. Without commenting on the DHHS rule, the FTC said: "Because health information is so sensitive, the Commission believes the standard for notification must give companies the appropriate incentive to implement policies to safeguard such highly sensitive information".[147]

In addition, the DHHS rule allows exceptions to the breach notification requirement in some cases of unintentional use or disclosure of unsecured protected health information. Those exceptions are not applied in the FTC rule. This is partly the result of loose drafting. The term "breach" is defined at section 13400 of the Act and includes the exceptions applied by DHHS. It is used in section 13402, which is implemented by DHHS. It is not used in section 13407, which has a vague definition of "breach of security" that does not list the exceptions. The FTC is responsible for implementation of section 13407. It was free to write a regulation that expanded the definition of "breach of security" so that it more closely conformed to the "breach" definition applied elsewhere in the Act. But it did not to do so, choosing instead to set a quick trigger of the notice requirement.

The Commission noted that a breach of security means acquisition of unsecured PHI identifiable health information *without authorization of the individual*. PHR websites obtain such authorization through click-through agreements to the site's terms of use and privacy policies, prompting this comment:

The Commission believes that an entity's use of information to enhance individuals' experience with their PHR would be within the scope of the individuals' authorization, as long as such use is consistent with the entity's disclosures and individuals' reasonable expectations. Such authorized uses could include communication of information to the consumer, data processing, or Web design, either in-house or through the use of service providers. Beyond such uses, the Commission expects that vendors of personal health records and PHR related entities would limit the sharing of consumers' information, unless the consumers exercise meaningful choice in consenting to such sharing. Buried disclosures in lengthy privacy policies do not satisfy the standard of "meaningful choice".[148]

Notification of Individuals

The FTC requirements for the timeliness, content and method of notification of a breach of unsecured PHR identifiable information by PHR vendors, PHR related entities, and third party service providers are nearly identical to those applied to HIPAA covered entities and business

[147] 74 Federal Register 42966

[148] 74 Federal Register 42967

associates under the DHHS rules. There are a few small differences, which are noted below.

PHR vendors and PHR related entities are required to notify each individual who is a citizen or resident of the United States whose unsecured PHR identifiable information was acquired by an unauthorized person as a result of a breach of security.[149] Notice must be provided without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.[150]

A breach is considered "discovered" as of the first day in which the breach is known, or reasonably should have been known, by a member of the workforce or agent of the vendor of personal health records, PHR related entity, or third party service provider, other than the person who committed the breach.[151]

The notice must be written in plain language, and include the following elements, to the extent possible:

- A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known;
- A description of the types of unsecured PHR identifiable information that were involved in the breach (such as whether name, address, social security or account numbers, diagnosis, etc);
- Steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the entity that suffered the breach is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an email address, Web site, or postal address.[152]

The FTC takes a different position than DHHS with regard to use of email to provide notice to individuals. Since vendors of personal health records and PHR related entities operate online, the FTC rule allows use of email as the default method of notice, provided that individuals are given a clear, conspicuous and reasonable opportunity to choose to receive notification by first class mail, and the individual does not exercise that choice.[153] In its commentary, the FTC says that entities can provide this choice by sending their consumers an email or by posting an alert that appears when they access their account, which (1) informs them that they will receive breach notices by

[149] 16 CFR 318.3(a)(1)

[150] 16 CFR 318.4(a)

[151] 16 CFR 318.3(c)

[152] 16 CFR 318.6

[153] 16 CFR 318.5(a)(1)

email unless they choose to receive notice by first class mail, and (2) provides them with a reasonable opportunity to express a preference to receive notices by first class mail, by including a toll-fee number, a return email address, or a link allowing the consumer to opt-out of email notice and select first class mail instead.[154] It also suggests that entities that use email notice provide guidance to consumers about how to set up email spam filters so that they will receive such notices.

If the individual is deceased, the vendor of personal health records or PHR related entity must provide notice to the next of kin if the individual has provided contact information for his or her next of kin, along with authorization to contact them.[155]

If there is insufficient information or out of date contact information for 10 or more people, then the PHR vendor or related entity must provide substitute notice in the form of a conspicuous posting on the home page of the entity's web site, or conspicuous notice in major print or broadcast media in geographic area where the individuals affected by the breach likely reside. The notice must include a toll-free number that remains active for at least 90 days where an individual can learn whether his or her information was included in the breach.[156]

In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured PHI, the covered entity may provide information to individuals by telephone or other means.

Notification to the Media

In the event of a breach of security involving the unsecured PHR identifiable information of 500 or more individuals who are residents of the same State or jurisdiction, notice must be provided to prominent media outlets serving that State or jurisdiction. If the PHR vendor or related entity does not collect address information and suffers a breach affecting more than 500 people, the FTC says that notice should be provided to media on a national basis.[157] Notice to the media, if required, must be provided without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.[158]

Notification to the Federal Trade Commission

Vendors of personal health records and PHR related entities must notify the Federal Trade Commission following discovery of a breach of security. If the breach involves the unsecured PHR identifiable health information of 500 or more individuals, notice to the FTC must be provided as

[154] 74 Federal Register 42972

[155] 16 CFR 318.5(a)(1)

[156] 16 CFR 318.5(a)(2)

[157] 74 Federal Register 42974

[158] 16 CFR 318.4(a)

soon as possible and in no case later than ten business days following the date of discovery of the breach.[159]

Vendors of personal health records and PHR related entities are required to maintain a log of breaches involving fewer than 500 individuals and to submit a report of such breaches to the FTC no later than 60 days after the end of any calendar year. The FTC has posted a form Notice of Breach of Health Information on its website.

The HITECH Act requires the FTC to notify the Secretary of Health and Human Services of any breaches of security reported to the FTC.[160]

Third Party Service Providers

The HITECH Act and the FTC rule require third party service providers to notify the appropriate vendor of personal health records or PHR related entity following discovery of a breach of security.[161] Notice must be provided without unreasonable delay, and in no case later than 60 days after discovery of the breach.

The FTC rule requires the third party service provider to deliver notice to an official designated to receive notices in a written contract by the vendor of personal health records or PHR related entity. If no such designation has been made, notice must be sent to a senior official of the PHR vendor or entity. The third party service provider is required to obtain acknowledgement that the notice was received.

Third party service providers are required to include in their notice the identification of each customer of the vendor of personal health records or PHR related entity whose unsecured PHR identifiable health information has been, or is reasonably believed to have been, acquired during the breach. The FTC rule doesn't otherwise specify the content of the notice from the third party service provider.

For purposes of ensuring implementation of this notice requirement, the FTC requires vendors of personal health records and PHR related entities to notify third party service providers that they are subject to the requirements of the Health Breach Notification Rule.

Vendors of Personal Health Records or PHR Related Entities that are also Business Associates

A vendor of personal health records that only operates as a business associate of HIPAA covered entities is subject to the DHHS rule and not the FTC rule. But if the vendor also offers personal health records to the public, it is subject to both the HHS and FTC breach notification rules. If it

[159] 16 CFR 318.5(c)

[160] HITECH Act §13407(d),

[161] HITECH Act §13407(b), 16 CFR 318.3(b)

experiences a breach, it would be required to provide direct breach notification to individual customers under the FTC rule. At the same time, under the HHS rule, it would be required to provide notice to the covered entities that they serve so that the HIPAA covered entities could notify individuals. That could lead to individuals receiving multiple notices of the same breach, a result that both DHHS and the FTC wish to avoid.

Both DHHS and the FTC noted that covered entities and business have the flexibility in business associate agreements to establish the specific obligations that each will have with regard to notification of breaches, including which party will provide notice to individuals and when the notice from the business associate to the covered entity will be required.[162]

The FTC is actively encouraging vendors of personal health records that are also business associates of HIPAA covered entities to agree to send breach notices on behalf of the covered entity, and has agreed to deem compliance with the DHHS rule to be compliance with the FTC rule in some cases. It suggests that the breach notice should come from the entity with which the consumer has a direct relationship, and says:

> *...[I]t may be desirable in some circumstances for a vendor of personal health records to provide notice directly to consumers even when the vendor is serving as a business associate of a HIPAA covered entity. For example, a consumer that obtained a PHR through a HIPAA covered entity may nevertheless deal directly with the PHR vendor in managing his or her PHR account, and would expect any breach notice to come from the PHR vendor. Similarly, where a vendor of personal health records has direct customers and thus is subject to the FTC's rule, and also provides PHRs to customers of a HIPAA-covered entity through a business associate arrangement, it may be appropriate for the vendor to provide the same notice to all such customers. In the latter situation, the Commission believes that the vendor of personal health records should be able to comply with one set of rule requirements – those promulgated by HHS – governing the timing, method, and content of notice to consumers. Thus, in those limited circumstances where a vendor of personal health records (1) provides notice to individuals on behalf of a HIPAA-covered entity, (2) has dealt directly with those individuals in managing the PHR account, and (3) provides such notice at the same time that it provides an FTC mandated notice to its direct customers for the same breach, the FTC will deem compliance with HHS requirements governing the timing, method, and content of notice to be compliance with the corresponding FTC rule provisions.*

The FTC commentary goes on to give examples of circumstances in which notification by the vendor of personal health records would be advantageous. It notes that a vendor of personal health records that serves multiple HIPAA covered entities will be required to associate individuals with specific covered entities so that the correct covered entity can be notified in the event of a breach. It discusses situations in which the personal health record is portable, where an individual is first associated with one covered entity, then with another, and cases where family members may get two different notices, one from a covered entity and another direct notice from the PHR

[162] 74 Federal Register 42754 (DHHS rule)

vendor.[163]

The comments by DHHS and the FTC do not have the force of law. But they are likely to influence contract negotiations between covered entities and business associates, as well as the forthcoming DHHS report to Congress about regulation of vendors of personal health records and other organizations that are not now subject to the HIPAA requirements.

Burden of Proof

Vendors of personal health records, PHR related entities, and third party service providers have the burden of demonstrating that all required notifications of a breach of security were made in a timely manner, including evidence demonstrating the necessity of any delay.[164]

Enforcement

A violation by a vendor of personal health records, PHR related entity, or third party services provider of the obligation to provide notification of breaches of the security of unsecured PHR identifiable health information will be treated as an unfair and deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.[165]

The FTC is empowered by law to conduct investigations and administrative hearings regarding rule violations, issue cease and desist orders, and to initiate litigation seeking a variety of remedies, including payment of damages to consumers affected by a violation of its rules.[166]

The FTC noted in its rulemaking that the breach notification requirements apply to not for profit organizations. They also apply to non-US based organizations as regards PHR identifiable information of US citizens or residents.

[163] 74 Federal Register 42964-42965

[164] HITECH Act § 13402((d)(2), 16 CFR 318.4(b)

[165] HITECH Act § 13407(e), 16 CFR 318.7

[166] 15 U.S.C. 57b, 57b-1

II. PRIVACY POLICY FOR THE HEALTH INFORMATION ORGANIZATION

Given this legal background, the challenge for Anasazi and subscribers is to establish a Privacy Policy to inform decisions regarding disclosure of individually identifiable health information through electronic health information exchange.

Privacy policies operate at three levels:

- ***Jurisdictional Policy*** – Describing the requirements of the law governing use and disclosure of various types of health information in a given state or province. Jurisdictional policy informs organizational policies.

- ***Organizational Policy*** – The policies adopted by a particular health care organization governing its use and disclosure of health information. These policies may be more stringent than jurisdictional requirements. For example, a community mental health center could decide that it will never disclose patient information for treatment purposes without written consent, even if the law (jurisdictional policy) permits such a disclosure.

- ***Individual Policy or Consent*** - Individual patients (or substitute decision makers) exercise rights granted by law or by organizational policies to give or to withhold permission to use or disclose individually identifiable health information. In those circumstances, the individual's consent directive would determine the "policy".

2.1 Draft HL7 Domain Analysis Model

Health Level Seven International, Inc. (HL7) is a not-for-profit, ANSI-accredited standards developing organization dedicated to providing a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information that supports clinical practice and the management, delivery and evaluation of health services. HL7 has over 2,300 members, including approximately 500 corporate members who represent more than 90% of the information systems vendors serving healthcare. Its mission is to provide standards for interoperability that improve care delivery, optimize workflow, reduce ambiguity and enhance knowledge transfer among all of its stakeholders, including healthcare providers, government agencies, the vendor community, fellow standards development organizations and patients.[167]

HL7 has published a draft Domain Analysis Model for trial use and comment that illustrates the use of electronic privacy policies and electronic consent directive as it relates to the privacy policy. HL7 is careful to note that this is not an accredited American National Standard. (See HL7 Version 3 Domain Analysis Model: Medical Records; Composite Privacy Consent Directive, Draft Standard for Trial Use, Release 2 (February 2010)).[168] ~ A Domain Analysis Model (DAM) is an

[167] http://www.hl7.org/about/index.cfm?ref=common

[168] The HL7 document was prepared in collaboration with SAMHSA, and Richard Thoreson of SAMHSA is identified as one of the authors. The document describes use cases in which 42 CFR Part 2 would apply. Unfortunately, the document suggests legal requirements that do not exist within 42 CFR Part 2, such as a

abstract representation of a subject area of interest to provide a generic representation of a class of system or capability and suggest a set of approaches to implementation. A Domain Analysis Model is not a functional implementation model. ~ This domain analysis model contains the analysis of several representative use cases illustrating the use of electronic privacy policies (Privacy Policy) and electronic consent directive (Consent Directive) as it relates to the Privacy Policy. It provides a composite view of Consent Directives and their underlying privacy policies. That is understood to mean that the HL7 DAM for Composite Privacy Consent Directive is a generic recommendation that provides few specifics as to how the standard would be implemented with existing HL7 interoperability standards.[169]

The information structure used by HL7 to represent Privacy Policies is displayed in the illustration that follows. As stated by HL7, "*Figure 7 shows the elements of a privacy policy from a jurisdictional or organizational standpoint. Electronic privacy policies are exchanged in a platform-independent, semantically interoperable, and standard-based way. A privacy policy is intended to protect individually identifiable health information from unauthorized use and disclosure.*"

---

requirement that a recipient delete substance abuse program records after use. Furthermore, the Sample Privacy Policy based on 42 CFR Part 2, found at pages 27 and 28 of the document inaccurately suggests that application of 42 CFR Part 2 is triggered by the condition of the patient and the use of public funds to pay for the service. In fact, application of the regulation is based upon the originating provider's identity as a substance abuse program.

[169] Quoting from the HL7 DAM above: "Publication of this draft standard for trial use and comment has been approved by Health Level Seven International (HL7). This draft standard is not an accredited American National Standard. The comment period for use of this draft standard shall end 24 months from the date of publication. Suggestions for revision should be submitted at http://www.hl7.org/dstucomments/index.cfm. Following this 24 month evaluation period, this draft standard, revised as necessary, will be submitted to a normative ballot in preparation for approval by ANSI as an American National Standard. Implementations of this draft standard shall be viable throughout the normative ballot process and for up to six months after publication of the relevant normative standard." Substantial revisions to a DAM are common during the evaluation period and during normative balloting.

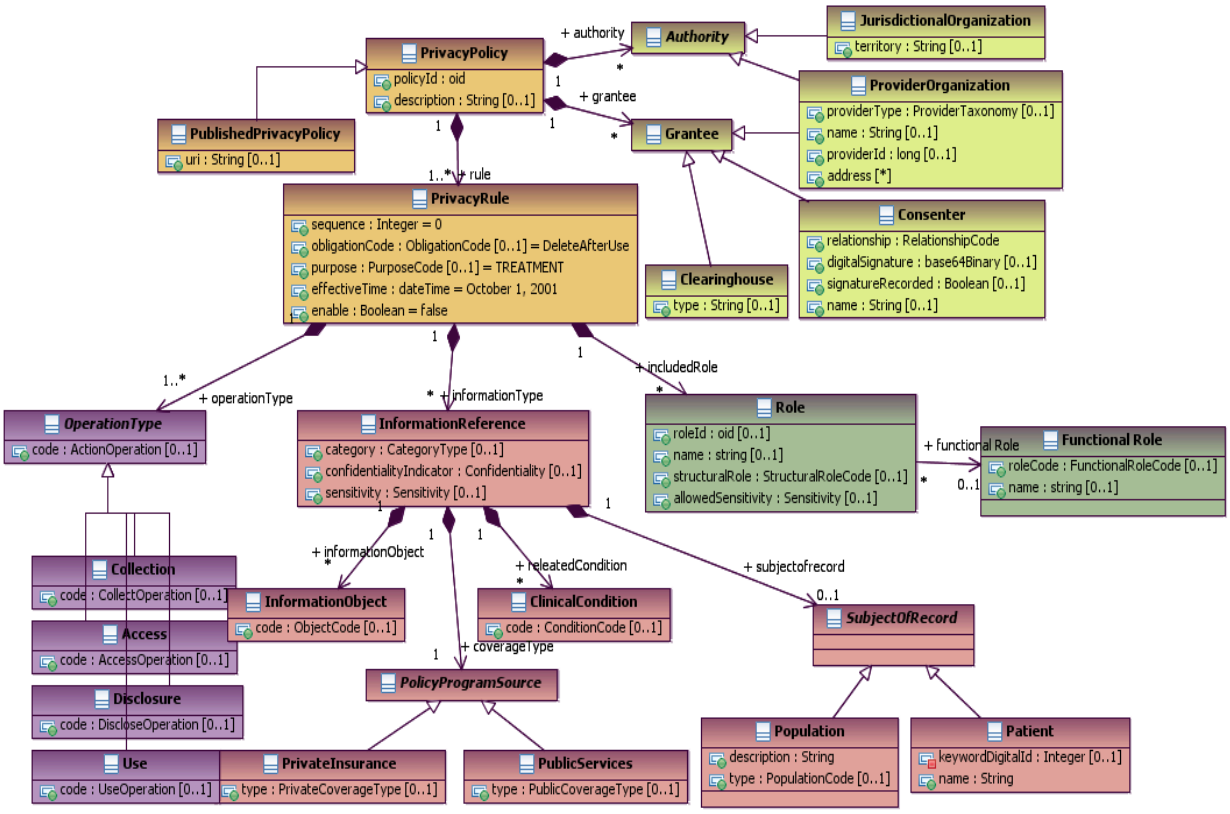

Figure 7: Privacy Policy Structure Overview Diagram

While this model is interesting, and could support future work towards development of functional standards for transactions involving the granting, recording, and termination of permissions to disclose individually identifiable health information, it is, at this point, a draft high-level view of classes of information, actors, and operations associated with consent transactions, presented to the public for review and comment. The public review period will continue until February of 2012. Anasazi cannot rely on the draft DAM as a definitive statement of programming standards to ensure interoperability.

Nor does the HL7 Domain Analysis Model address the legal issues discussed in Part 1 of this memorandum. In order to develop and operate the health information exchange, it will be necessary for Anasazi (and any other developer/operator of a health information organization) to identify the legally relevant variables, reduce those variables to classes and subclasses of data, and, on a jurisdiction by jurisdiction basis, identify the interactions among those variables that define the outcome of an analysis of whether and under what conditions individually identifiable health information may be disclosed. (Note that the Composite Privacy Consent Directive assumes the availability of a network of authoritative jurisdictional "Privacy Policy Authors" that are responsible for informing yet to be established consent directive management services that automate the process of application of national, state and local laws that apply to requests for disclosure of health information. In addition, it would require the development of a new set of standard interoperability transactions that would support communication of privacy policies

between the Privacy Policy Authors and all EHRs and HIOs, There is no indication yet that this approach has been endorsed or supported by the NHIN or ONC and will therefore be developed.)

2.2 A Note on Granularity

On December 15, 2008, the Office of the National Coordinator for Health Information Technology published a Nationwide Privacy and Security Framework For Electronic Exchange of Individually Identifiable Health Information. ONC described the purpose of this document as follows:

> *Electronic health information exchange promises an array of potential benefits for individuals and the U.S. health care system through improved clinical care and reduced cost. At the same time, this environment also poses new challenges and opportunities for protecting individually identifiable health information. In health care, accurate and complete information about individuals is critical to providing high quality, coordinated care. If individuals and other participants in a network lack trust in electronic exchange of information due to perceived or actual risks to individually identifiable health information or the accuracy and completeness of such information, it may affect their willingness to disclose necessary health information and could have life-threatening consequences. A key factor to achieving a high-level of trust among individuals, health care providers, and other health care organizations participating in electronic health information exchange is the development of, and adherence to, a consistent and coordinated approach to privacy and security. Clear, understandable, uniform principles are a first step in developing a consistent and coordinated approach to privacy and security and a key component to building the trust required to realize the potential benefits of electronic health information exchange.*
>
> *The principles below establish a single, consistent approach to address the privacy and security challenges related to electronic health information exchange through a network for all persons, regardless of the legal framework that may apply to a particular organization. The goal of this effort is to establish a policy framework for electronic health information exchange that can help guide the Nation's adoption of health information technologies and help improve the availability of health information and health care quality. The principles have been designed to establish the roles of individuals and the responsibilities of those who hold and exchange electronic individually identifiable health information through a network.*

The framework is comprised of eight principles:

- ***Individual Access*** - Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format.

- ***Correction*** - Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied.

- ***Openness and Transparency*** - There should be openness and transparency about policies,

procedures, and technologies that directly affect individuals and/or their individually identifiable health information.

- *Individual Choice* - Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information.

- *Collection, Use, and Disclosure Limitation* - Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.

- *Data Quality and Integrity* - Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.

- *Safeguards* - Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.

- *Accountability* - These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

In 2010, ONC formed a Privacy and Security "Tiger Team" under the auspices of the HIT Policy Committee. ONC asked the Tiger Team to focus on a set of targeted questions raised by ONC regarding the exchange of personally identifiable health information required for doctors and hospitals to qualify for incentive payments under Stage 1 of the Electronic Health Records Incentive Program. Among the questions that ONC asked the Tiger Team to consider was the ability of technology to support more granular patient consents (i.e., authorizing exchange of specific pieces of information while excluding other records).

The question of the granularity of controls over disclosure of specific categories of information in a clinical record is one that challenges all health information organizations and developers of electronic health records and personal health records. It requires a difficult balancing of what is technically possible and what is practical. The August 19, 2010 response of the Tiger Team to the granularity question presented by ONC is instructive about the current state of the art in this area. It is quoted below in its entirety.

> *In making recommendations about granular consent and sensitive data, we have the following observations:*
>
> *All health information is sensitive, and what patients deem to be sensitive is likely to be dependent on their own circumstances.*

However, the law recognizes some categories of data as being more sensitive than others.

Unless otherwise required by law and consistent with our previous recommendation [3.1], with respect to directed exchange for treatment, the presence of sensitive data in the information being exchanged does not trigger an additional requirement to obtain the patient's consent in the course of treating a patient.

Our recommendations on consent do not make any assumptions about the capacity for an individual to exercise granular control over their information. But since this capability is emerging and its certainly fulfills the aspiration of individual control, we sought to understand the issue in greater depth.

The Tiger Team considered previous NVHS letters and received a presentation of current NCVHS efforts on sensitive data. We also held a hearing on this topic to try to understand whether and how current EHR technology supports the ability for patients to make more granular decisions on consent – in particular, to give consent to the providers to transmit only certain parts of their medical record.

We learned that many EHR systems have the capability to suppress psychotherapy notes (narrative). We also learned that some vendors offer the individual the ability to suppress specific codes. We believe this is promising. With greater use and demand, this approach could possibly drive further innovations.

We also note, however, that the majority of witnesses with direct experience in offering patients the opportunity for more granular control indicated that most patients[*] agreed to the use of their information generally and did not exercise granular consent options when offered the opportunity to do so. The Tiger Team also learned that the filtering methodologies are still evolving and improving, but that challenges remain, particularly in creating filters that can remove any associated or related information not traditionally codified in standard or structured ways.

While it is common for filtering to be applied to some classes of information by commercial applications based on contractual or legal requirements, we understand that most of the commercial EHR systems today do not provide this filtering capability at the individual patient level. There are some that have the capability to allow the user to set access controls by episode of care/encounter/location of encounter, but assuring the suppression of all information generated from a particular episode (such as prescription information) is challenging.

Preventing what may be a downstream clinical inference is clearly a remaining challenge and beyond the state of the art today. Even with the best filtering it is hard to guarantee against "leaks."

The Tiger Team believes that methodologies and technologies that provide filtering capability are important in advancing trust and should be further explored. There are several efforts currently being piloted in various stages of development. We believe communicating with patients about these capabilities today still requires a degree of caution and should not be over sold as fail-proof, particularly

[*] Witnesses offered estimates of greater than 90%

in light of the reality of downstream inferences and the current state of the art with respect to free text. Further, communicating to patients the potential implications of finegrained filtering on care quality remains a challenge.

We acknowledge that even in the absence of these technologies, in very sensitive cases there are instances where a completely separate record may be maintained and not released (abortion, substance abuse treatment, for example). It is likely that these practices will continue in ways that meet the expectations and needs of providers and patients.

In our ongoing deliberations, we discussed the notion of consent being bound to the data such that it follows the information as it flows across entities. We know of no successful large-scale implementation of this concept in any other sector (in that it achieved the desired objective), including in the case of digital rights management (DRM) for music. Nonetheless, we understand that work is being done in this emerging area of technology, including by standards organizations.

While popular social networking sites are exploring allowing users more granular control (such as Facebook), the ability of individuals to exercise this capability as intended is still unclear.[*] *In addition, the data that populates a Facebook account is under the user's control and the user has unilateral access to it. Health data is generated and stored by myriad of entities in addition to the patient.*

Even the best models of PHRs or medical record banks provide individuals with control over copies of the individual's information. They do not provide control over the copy of the information under the provider's control or that is generated as a part of providing care to the patient. They also do not control the flow of information once the patient has released it or allowed another entity to have access to it.

Discussions about possible or potential future solutions were plentiful in our deliberations. But the Tiger Team believes that solutions must be generated out of further innovation and, critically, testing of implementation experience.

The Tiger Team also considered previous NCVHS letters and received a presentation of current NCVHS efforts on sensitive data.

The Tiger Team therefore asked whether and what actions ONC might take to stimulate innovation and generate more experience about how best to enable patients to make more granular consent decisions.

Tiger Team Recommendation 4: Granular Consent

The technology for supporting more granular patient consent is promising but is still in the early stages of development and adoption. Furthering experience and stimulating innovation for granular consent are needed.

---

* See http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html and http://www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html.

This is an area that should be a priority for ONC to explore further, with a wide vision for possible approaches to providing patients more granular control over the exchange and use of their identifiable health information, while also considering implications for quality of care and patient safety, patient educational needs, and operational implications.

The goal in any related endeavor that ONC undertakes should not be a search for possible or theoretical solutions but rather to find evidence (such as through pilots) for models that have been implemented successfully and in ways that can be demonstrated to be used by patients and fulfill their expectations. ONC and its policy advising bodies should be tracking this issue in an ongoing way and seeking lessons learned from the field as health information exchange matures.

In the interim, and in situations where these technical capabilities are being developed and not uniformly applied, patient education is paramount: Patients must understand the implications of their decisions and the extent to which their requests can be honored, and we encourage setting realistic expectations. This education has implications for providers but also for HIOs and government.

(Continued on Following Page)

2.3 Model Consent Form For Health Information Exchange in California

The model form that follows permits electronic exchange of health information for treatment purposes. It includes the notice and affirmative consent to electronic information exchange required by regulations proposed by the California Office of Health Information Integrity. It also includes the commonly required elements of the form for permission to disclose substance abuse program records set forth in 42 CFR 2.31 and the form of permission to disclose health records set forth in the California Confidentiality of Medical Information Act)(Civil Code 56.11).

A few notes regarding the design and use of this Model Consent Form:

- The model form begins with an explanation of electronic health information exchange.

- The form permits disclosures of health information for treatment purposes only. Consistent with California's proposed regulations, this includes referral for health care from one provider to another, provider consultation regarding health care, provision of health care services, and coordination or management of care by a health care provider with a third party.

- The model form records an individual's permission to disclose a specific set of health records to specifically identified health care providers. Both the sender and the recipient of the record are identified. This is consistent with NHIN-Direct transactions between known, trusted providers and meets the requirements of 42 CFR 2.31.

- Note the marked difference between the specificity of the model form and the consent forms used by the Veteran's Administration and New York State RHIOs. The VA form permits disclosure for treatment purposes of all VA health records to any "community" that participates in the National Health Information Network. The New York RHIO form permits a specific provider to locate and receive any health record about an individual that is created by any provider that participates in the state health information exchange.

- The model form permits disclosure of the entire health record maintained by a provider as needed for the purposes of treatment, with the exception of psychotherapy notes. The assumption is participating health care providers will exchange Continuity of Care Documents that contain problem lists, laboratory results, medication lists, medication allergies, and other information in accordance with the "Meaningful Use" rules (45 CFR Part 495).

- The model form does not enable individuals to permit disclosure of portions of health records while refusing to permit disclosure of other parts of the record. As noted by the Privacy and Security Tiger Team, such a granular approach to management of disclosure and re-disclosure of health information is not feasible at this time.

- The model form neither prohibits nor permits re-disclosure of health information by the recipient of the record. It is assumed that the recipient of health information will secure any legally required permission before re-disclosure of that information to third parties.

- Note that it would be possible to create a 42 CFR Part 2 compliant consent form that permits a set of identified providers to re-disclose substance abuse records to one another through electronic health information exchange. But this would not be a practical approach to consent directive management in the context of the National Health Information Network because it is not scalable beyond limited communities of identified providers.

- A specific form of notice of the applicability of 42 CFR Part 2 must accompany substance abuse program records that are disclosed with patient consent. The health information exchange transaction should include that notice. But the notice itself is not part of the Model Consent form.

- The model is designed to enable creation of an electronic consent record. This will make it easier for participants in electronic health information exchange to automate the process of determining that a current and legally valid consent permits disclosure of health information

- The NHIN-Direct standards assume that the sending organization is responsible for securing required legal permission to disclose health information. But if the sender and receiver are known and trusted, a sender could rely on a Consent obtained by the receiver. Authentication of the identity of requesting organization, confirmation of the trust relationship (through reference to a DURSA or similar agreement) and confirmation that the Consent includes the required legal elements to permit disclosure could be a service provided by a HISP.

- Note that the duration of the validity of the consent is based on time, not an event. There are two reasons for this. First, the form is written for use in California, and California Civil Code 56.11 requires that the duration of consent to disclosure of outpatient mental health records be limited by time, not events. Second, and as importantly, it is possible to automate the process of tracking the validity of a consent that expires on a fixed date, but impossible to automate the process of tracking a consent that expires upon the occurrence of an event that may never be reported and logged into the system.

Model Consent to Disclosure of Electronic Health Information

Information About Electronic Health Information Exchange and This Consent Form

In this Consent Form, you can choose whether or not to allow disclosure of your health records through electronic health information exchange. Health Information Exchange is the use of secure computer systems, instead of paper, to make information about your health available to doctors and other care providers you choose.

By permitting electronic health information exchange, you will make it easier for your doctors and other care providers to get a complete picture of your health, which can help you get better care. Your health records provide information about your illnesses, injuries, medicines and/or test results. Your records may include sensitive information, such as information about HIV status, mental health records, reproductive health records, drug and alcohol treatment records, and genetic information.

Your electronic health information will only be used to provide you with medical treatment and related services. This includes referral for health care from one provider to another, consultation regarding your health care, provision of health care services, and coordination or management of care by a health care provider with a third party.

Your electronic health information may be re-disclosed only to the extent permitted by state and federal laws and regulations. Federal law provides special protections for substance abuse program records. Those records may not be used as evidence to investigate or prosecute you in criminal proceedings.

This Consent does not authorize disclosure of psychotherapy notes.

Please note that your choice to give or deny consent to disclose electronic health information may not be the basis for denial of health services.

Note also that electronic health information about you may be disclosed without your consent in a medical emergency or for public health reporting as mandated by law.

You can withdraw your consent at any time by signing a Withdrawal of Consent Form and giving it to [Contact name, phone number, email address, and website.] You can also change your consent choices by signing a new Consent Form at any time. Please note that organizations that receive health information while your consent is in effect may retain that information. Even if you later decide to withdraw your consent, they are not required to return it or remove it from their records.

You are entitled to get a copy of this Consent Form after you sign it.

Model Consent to Disclosure of Electronic Health Information

1. The person whose information may be used or disclosed is:

Name: _____.
Date of Birth: _____.
Patient Identification Number: _____.

2. This information may be disclosed by:

The persons or organizations listed below (insert picklist)

3. This information may be disclosed to:

The persons or organizations listed below (insert picklist)

4. The information that may be disclosed includes all records of diagnosis and treatment. Disclosure of psychotherapy notes is not permitted.

5. Disclosure of this information is permitted or treatment purposes only.

6. ☐ I GIVE CONSENT for electronic health information exchange.

☐ I DENY CONSENT for electronic health information exchange.

7 This permission expires on _____ (date);

8. I understand that this permission may be revoked. I also understand that records disclosed before this permission is revoked may not be retrieved. Any person or organization that relied on this permission may continue to use or disclose records and protected health information as needed to complete work that began because this permission was given.

I am the person whose records will be used or disclosed. I give permission to use and disclose my records as described in this document.

_____

Signature Date

I am the personal representative of the person whose records will be used or disclosed. My relationship to that person is (picklist)_____. I give permission to use and disclose records as described in this document.

_____

Signature Date