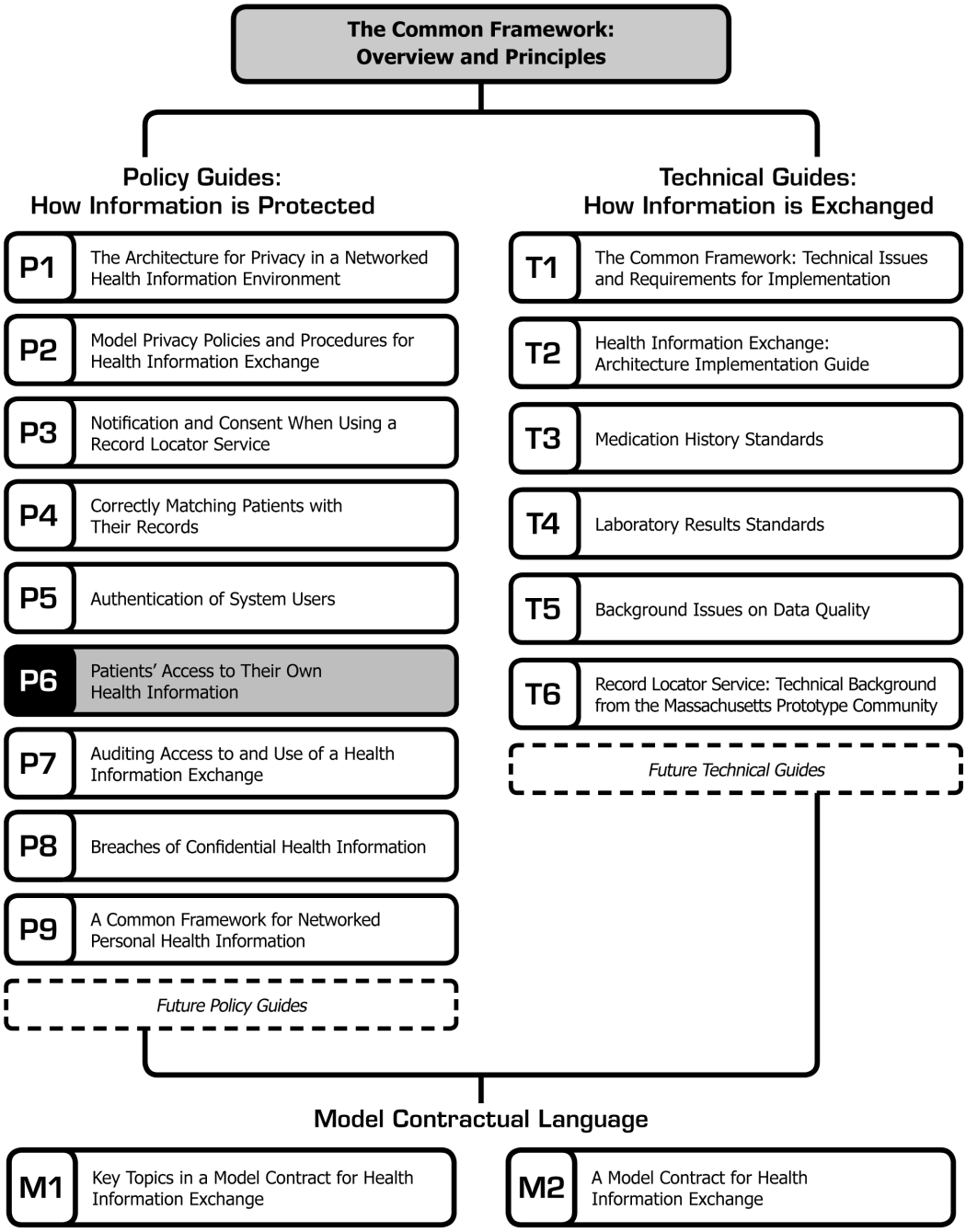
P1 P2 P3 P4 P5 **P6** P7 P8

T1 T2 T3 T4 T5 T6 M1 M2

Patients' Access to Their Own Health Information

Patients' Access to Their Own Health Information

The document you are reading is part of *The **Connecting for Health** Common Framework,* which is available in full and in its most current version at: http://www.connectingforhealth.org/. The Common Framework will be revised and expanded over time. As of October 2006, the Common Framework included the following published components:



Patients' Access to Their Own Health Information*

Collecting, storing, and sharing personal health information about patients is a fundamental component of health care. In addition to serving as the information hub to health care providers in treating patients, medical records are frequently used by a host of other health care professionals, such as quality improvement organizations, researchers, and public health officials.

Patients have a vital interest in accessing sensitive information about their own health care. A central principle of privacy policy is to provide people with access to their own information, so that they may make informed choices about who should get their information, under what circumstances, and be made aware of errors that the records may contain. Access to their own medical records can also empower consumers to become more engaged participants in their own health care.

Most consumers want access to their medical records. A national survey documents that 68 percent of Americans believe that "giving people the right to see and make corrections to their own medical records" would be an effective way of promoting privacy and health care.[1] In fact, Americans' interest in accessing their personal medical information has increased over the years. In 2005, 51 percent of Americans tried to access their medical records, up from 45 percent in 1999.[2] However, until recently, many people did not have the legal right to see, copy, and amend their health information held by their providers. As of April 2003, the HIPAA Privacy Rule mandates that people have such rights, whether their records are in paper or electronic format.[3]

Patients' ability to effectively access their own personal health information could be significantly enhanced with the use of new technologies. Although there are significant concerns about privacy that must be addressed, accessing personal health information electronically could have a positive impact on how patients participate in their own care. Some providers and companies have taken the lead by offering patients electronic access to their medical information. The growing movement towards the development of electronic health record (EHR) systems should include patients as authorized users of their health information for both practical and legal purposes, enabling compliance with the privacy regulation and enhancing a person's ability to make informed choices about his or her health and the use of his or her information.

While the Privacy Rule allows patient access to both paper and electronic records, the increasing use of technology in health care fosters the potential for streamlining the process of granting patients access to their records. The Privacy Rule provides a *floor* of protection, whereby individual states can—and have—enforced laws that both provide stronger protections for personal health information and allow patients easier access to their medical records.

* **Connecting for Health** thanks Janlori Goldman, Research Scholar, Center on Medicine as a Profession, Columbia College of Physicians and Surgeons; Health Privacy Project, and Emily Stewart, formerly of the Health Privacy Project, for drafting this paper.

1 "Medical Privacy and Confidentiality Survey," California HealthCare Foundation, Final Topline, 1/10/99, available at: http://www.chcf.org/documents/ihealth/topline.pdf.

2 California HealthCare Foundation, "National Consumer Health Privacy Survey 2005," Conducted by Forrester Research, Inc.

3 The Privacy Rule went into effect on 4/14/01, and most providers and health plans were required to be in compliance with the law by 4/14/03.

The HIPAA Privacy Rule—Accessing Protected Health Information

In promulgating the HIPAA regulations, the United States Department of Health and Human Services (HHS) recognized that allowing consumers access to their health information is a necessary component of a well-functioning health care system. Based on the principle of informed consent, the Privacy Rule acknowledges that in order to have meaningful control over personal health care decisions—including limitations on who can access information—individuals need to have access to their own health information. The Privacy Rule gives consumers rights with regard to certain health care organizations, or "covered entities," defined as health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with specified financial and administrative transactions.[4]

In general, protected health information under the Privacy Rule correlates with what most consumers would consider their medical record. Whether or not their health information is paper-based or stored electronically, the Privacy Rule affords patients the right to access their medical record within 30 days of a request.

The Privacy Rule explicitly gives patients the right to inspect and obtain a copy of protected health information held in a "designated record set" by the covered entity.[5] *Protected health information* (PHI) is defined as "individually identifiable health information," with the exception of some education and other records.[6] Consumers only have a right to access PHI if, and for as long as, it is maintained in a *designated record set*, which the Privacy Rule defines as a "group of records maintained by or for a covered entity that is:

(i) the medical records and billing records about individuals maintained by, or for a covered health care provider;

(ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by, or for a health plan; or

(iii) used, in whole or in part, by or for the covered entity to make decisions about individuals."[7]

Although the Privacy Rule grants consumers the right of access in most situations, there are several specific situations in which covered entities are *neither* required to give consumers access to their own protected health information held in a designated record set *nor* required to allow the individual a review of the denial. For instance, individuals do not have the right to access psychotherapy notes or information compiled in reasonable anticipation of, or for use in a civil, criminal, or administrative action or proceeding.[8]

On the other hand, there are some circumstances when covered entities have the right to deny access, *but* individuals also have the right to request a review of that denial. For example, if in the exercise of professional judgment, a licensed health care professional believes that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person, the covered entity can then deny access.[9] Also, if the PHI makes reference to another person, unless the other person is a health care provider, and a licensed health care professional believes that the access requested is reasonably likely to cause substantial harm to such other person, a covered entity can deny access to the health information.[10] Again, in these types of situations,

---

4 45 C.F.R. § 160.103.

5 45 C.F.R. § 164.524(a)(1).

6 45 C.F.R. § 164.501. The Privacy Rule defines *individually identifiable health information* as "a subset of health information, including demographic information collected from an individual" that (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) 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; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. *See* 45 C.F.R. § 160.103.

7 45 C.F.R. § 164.501.

8 45 C.F.R. § 164.524(a)(1-2). *See* citation for more circumstances whereby a covered entity can deny access and refuse to allow the individual an opportunity for review of the denial.

9 Note that only "life or physical safety" is specified; possible harm to mental or emotional health is not a reason to deny access.

10 45 C.F.R. § 164.524(a)(3). *See* citation for more circumstances whereby a covered entity can deny access but individuals also have a right to request a review of the denial.

an individual has a right to request a review of the denial.[11]

The Privacy Rule outlines a basic process for individuals seeking access to their medical information and establishes guidelines to ensure covered entities provide access in a timely manner. As a basic principle, the Privacy Rule establishes that covered entities must allow individuals to request access to their own records; the law allows covered entities to require that requests be written provided that patients are informed of this requirement.[12] Otherwise, patients may request access orally.

Within 30 days of the receipt of the request, the covered entity must act on the request by providing the patient access, providing a written denial of access, or informing the individual of the reason for which the covered entity needs additional time (but no more than 30 days) to complete the request.[13] The one exception is for information not maintained or accessible to the covered entity on-site; in this instance, the covered entity may take up to 60 days to take one of the above actions.[14]

If the covered entity grants access, it must provide the individual with the information in the format requested if possible and otherwise in a readable hard copy or another format agreed upon by both the covered entity and the individual.[15] However, the covered entity may provide a summary of the health information if the individual agrees in advance to the summary *and* to any additional fees it would produce. The covered entity must arrange with the individual for "a convenient time and place to inspect or obtain a copy of the protected health information, or mail the copy of the protected health information at the individual's request" and may charge a "reasonable, cost-based fee" if the individual requests a copy of the record, but the fee can only include costs for copying, postage, and the development of a summary if the individual agreed to one.[16]

If the covered entity denies access to a patient, it must deny access only to the specific information for which it has grounds to deny access. In addition, and within 30 days, the covered entity must provide the individual with a denial *written* in plain language. The statement must contain the basis for the denial, information about the individual's review rights if applicable and how to exercise those rights, as well as a description detailing pertinent names, titles, and contact information of how the individual may file a complaint. Furthermore, if the covered entity does not maintain the protected health information about the individual requested, but has knowledge about where it is stored, the law requires the covered entity to inform the individual about where to submit a request for access.[17]

If the individual requests a review of the covered entity's denial, the covered entity must ensure that the review is conducted by a licensed health care professional who was *not* directly involved in the denial. The covered entity must forward the request in a timely manner to the reviewer, and the designated reviewing professional must determine "within a reasonable period of time" whether or not to deny access. Once a decision is made, the covered entity must immediately provide notice

[11] 45 C.F.R. § 164.524(a)(3).

[12] 45 C.F.R. § 164.524(b)(1). Often, covered entities may contract with "business associates" to perform some of the covered entity's functions. In the business associate contract, the business associates must agree to make protected health information available for access, amendment, and accounting of disclosures. *See* 164.504(e)(2)(ii)(E-G).

[13] If a covered entity needs more time to take action related to the individual's request for access, it must, within 30 days, notify the individual with a written statement establishing the reasons for the delay and the date by which the covered entity will complete its action. The covered entity may only have one extension of time. *See* 45 C.F.R. § 164.524(b)(2)(iii).

[14] 45 C.F.R. § 164.524(b).

[15] 45 C.F.R. § 164.524(c)(2)(i).

[16] 45 C.F.R. § 164.524(c). According to the Preamble to the Privacy Rule, 65 F.R. 82557, "If the individual requests a copy of protected health information, a covered entity may charge a reasonable, cost-based fee for the copying, including the labor and supply costs of copying. If hard copies are made, this would include the cost of paper. If electronic copies are made to a computer disk, this would include the cost of the computer disk. Covered entities may not charge any fees for retrieving or handling the information or for processing the request. If the individual requests the information to be mailed, the fee may include the cost of postage. Fees for copying and postage provided under state law, but not for other costs excluded under this rule, are presumed reasonable. If such per page costs include the cost of retrieving or handling the information, such costs are not acceptable under this rule." Available at: http://aspe.hhs.gov/admnsimp/final/PvcPre02.htm.

[17] 45 C.F.R. § 164.524(d).

to the individual and take any necessary action.[18]

The HIPAA Privacy Rule—Amending Protected Health Information

The Privacy Rule recognizes the importance of allowing patients the right to amend inaccurate or incomplete medical records. Under the law, after an individual has reviewed his or her medical records, he or she may request that the covered entity amend the protected health information in the designated record set.[19] However, in order to protect both the integrity of the record and the patient, the individual does not have the right to request that the covered entity delete any information from the record.[20] Instead, information is added to the record, identifying and amending the pertinent information.

The Privacy Rule allows covered entities to require that individuals make amendment requests in writing and also provide a reason for the request, as long as individuals are notified in advance of any requirements. Within 60 days of receiving the request, the covered entity must either make the requested amendment or deny it.[21] However, just as with the other access provisions, the law does allow the covered entity one extension (of no more than 30 days), provided that it sends the individual a written statement explaining the delay and listing the expected completion date.[22]

If the covered entity decides to accept the amendment request, the Privacy Rule requires that at a minimum, it must identify the records that are affected by the amendment and either attach the amendment or provide a link to the location of the amendment. The law also requires the covered entity to notify the individual that the record has been amended in a timely manner and to secure the individual's agreement allowing the covered entity to inform other relevant persons. Also in a timely manner, the covered entity must make reasonable efforts to notify and provide the amendment to anyone that the individual designates as having received PHI needing amendment. The covered entity must also notify others, including business associates, which have the information and may have relied or could rely on the un-amended information to the detriment of the individual.[23]

If a covered entity decides to deny the amendment request, it must still abide by several related requirements, such as using plain language and within 60 days, the covered entity must provide the individual with a written denial that details both the basis for the denial and the individual's right, as well as how to exercise this right, to submit a written statement disagreeing with the denial. If the individual submits a statement of disagreement, the statement, the original request, the covered entity's denial, and any rebuttal must be appended to the designated record set and included in any future disclosures.[24] Even if the individual does not submit a statement of disagreement, he or she may request—and the covered entity must comply—that the covered entity include the request for amendment and the denial with any future disclosures of pertinent sections of the designated record set.[25] In addition, the covered entity is required to append or link to the appropriate section of the designated record set, as a recordkeeping function, the individual's amendment request, the denial of request, the statement of disagreement, and any rebuttal statement.[26]

---

[18] 45 C.F.R. § 164.524(d)(4).

[19] 45 C.F.R. § 164.526(a)(1).

[20] It is important to note that any amendment made to an individual medical record is technically a supplement to that record. In other words, no information is discarded in the amendment process. Instead, information is added, identifying and amending the medical record. This process was designed primarily to ensure the integrity of the record and to protect the patient. *See* 45 C.F.R. § 164.526(c)(1).

[21] 45 C.F.R. § 164.526(a-b).

[22] 45 C.F.R. § 164.526(b)(2)(ii).

[23] 45 C.F.R. § 164.526(c).

[24] 45 C.F.R. § 164.526(d). The Privacy Rule also allows covered entities to include in future disclosures—in lieu of including the actual request, denials, disagreement statements, and rebuttals—"an accurate summary of any such information." *See* 45 C.F.R. § 164.526(d)(4)-(5).

[25] 45 C.F.R. § 164.526(d). The Privacy Rule requires covered entities to inform individuals that if a disagreement statement is not submitted, the individual may request that the covered entity attach the request and denial to any future disclosures. *See* 45 C.F.R. § 164.526(d)(1)(iii).The Privacy Rule also allows covered entities to include in future disclosures—in lieu of including the actual request, denials, disagreement statements, and rebuttals—"an accurate summary of any such information." *See* 45 C.F.R. § 164.526(d)(4)-(5).

[26] 45 C.F.R. § 164.526(d)(4).

The HIPAA Privacy Rule—Accounting for Disclosures

Knowing who has had access to one's personal health information is related to having access oneself. Accordingly, the Privacy Rule acknowledges the importance of allowing patients the ability to see who accessed their personal health information. With exceptions, the Privacy Rule gives patients the right to see to whom covered entities have disclosed their personal health information for the six years prior to the date of the request.[27]

Upon request, covered entities must provide consumers with an accounting of disclosures during the previous six years, including the date of the disclosure, the name of the person who received the information, a brief description of the protected health information disclosed, and a brief statement of the purpose of the disclosure. If a covered entity has made multiple disclosures to the same person for the same purpose, it may provide the above information only for the first disclosure as long as it also provides the frequency of the disclosures and the date of the last disclosure.[28]

Within 60 days of the request, a covered entity must provide the accounting or a written statement detailing a reason for why it needs an extension of time (no more than 30 days).[29] The covered entity must provide an accounting of disclosures once a year without charge. However, if an individual requests an accounting more than once a year, a reasonable, cost-based fee may be imposed, provided that the individual was informed in advance of the fee and the covered entity also provides the individual with an opportunity to withdraw or modify the request in order to avoid the fee.[30]

Individuals do not have the right to accountings of certain disclosures, most notably disclosures to carry out treatment, payment, and health care operations and disclosures to the individual actually requesting the accounting of disclosures of their own PHI.[31] Furthermore, a covered entity must temporarily suspend an individual's right to receive an accounting of disclosures made to a health oversight agency or law enforcement official, if the agency or official provides the covered entity with a written statement illustrating that such an accounting would be reasonably likely to impede the agency's activities. The written statement must also specify the time period for which such a suspension is required.[32]

The HIPAA Privacy Rule and State Laws

In general, covered entities are required to follow both the Privacy Rule and related state laws. However, if a Privacy Rule provision contradicts state law, the Privacy Rule automatically preempts that law.[33] Still, there are exceptions, for example, a state law prevails when that law "provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance,

---

[27] 45 C.F.R. § 164.528(a).

[28] Additionally, if a covered entity has made PHI disclosures for research purposes for 50 or more people, the accounting of disclosures may (with respect to such disclosures for which the PHI of the individual may have been included) provide: the name of the protocol or research activity; a description in plain language about the activity, including purpose and criteria for selecting records; a description of the type of PHI that was disclosed; when the disclosure occurred (date or period of time and the date of the last disclosure); contact information (name, address, and telephone number) of the entity that sponsored the research and of the researcher to whom the PHI was disclosed; and a statement that the PHI of the individual may or may not have been disclosed. If it is reasonably likely that the PHI of the individual was disclosed, and at the request of the individual, a covered entity must assist in contacting the entity or the researcher. *See* 45 C.F.R. § 164.528(b).

[29] 45 C.F.R. § 164.528(c)(1)(ii). The covered entity is allowed only one 30-day extension.

[30] 45 C.F.R. § 164.528(c).

[31] Other exceptions include (i) for the facility's directory or to persons involved in the individual's care or other notification purposes; (ii) for national security or intelligence purposes; (iii) to correctional institutions or law enforcement officials for certain purposes; (iv) as part of a limited data set; or (v) that occurred prior to the compliance date for the covered entity. *See* 45 CFR 164.512(k)(2), 45 CFR 164.512(k)(5), and 45 C.F.R. § 164.514(e)(2).

[32] 45 C.F.R. § 164.528.

[33] According to 45 C.F.R. § 160.202, "contrary" means, when used to compare a provision of state law to a standard, requirement, or implementation specification adopted under this subchapter: (1) a covered entity would find it impossible to comply with both the state and federal requirements; or (2) the provision of state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act or section 264 of Pub.L.104-191, as applicable.

investigation, or intervention."[34] State law remains in effect in other circumstances as well, such as when the Secretary of HHS determines that the state law is necessary to prevent fraud and abuse related to health care services, to meet state reporting on health care delivery or costs, or for the purposes of serving a need related to public health, safety, or welfare.[35]

The Privacy Rule also establishes that patients may be afforded stronger privacy safeguards at the state level. The Privacy Rule expressly stipulates that when state laws are more stringent than the Privacy Rule, they remain in force.[36] Therefore, in some states, patients are granted easier access to their personal health information. For example, some state laws actually cap copying and postage fees for medical records, institute shorter time frames for granting access, or require additional accountings of disclosures.

State laws vary widely in terms of how they address health privacy, including the right to access personal health information. Whereas in some states, patients will be afforded only access rights guaranteed under the Privacy Rule, other states offer stronger rights of access. For instance, in New York, patients have a right to see their protected health information within 10 days, as opposed to the 30 days allowed by the Privacy Rule.[37] New York caps copying charges at 75 cents per page, while California establishes a fee of 25 cents per page for a regular photocopy.[38] In fact, many states, including Illinois, Missouri, Georgia, Arkansas, New Hampshire, and Nevada, cap copying fees to varying degrees.[39] Meanwhile, states such as New York and Florida stipulate that access cannot be denied because of inability to pay.[40]

The HIPAA Privacy Rule and Electronic Access to Medical Records

The Administrative Simplification section of HIPAA, under which the Privacy Rule is mandated, was aimed at fostering the electronic exchange of health information. In that section, Congress called for the development of a "health information system through the establishment of standards and requirements for the electronic transmission of certain health information."[41] The Privacy Rule and the related Security Rule[42] were devised to establish a baseline of policies and practices to safeguard health information to

[34] 45 C.F.R. § 160.203(c), (d).

[35] *See* 45 C.F.R. § 160.203(a) for more instances whereby the Secretary can make a determination where state law prevails. Section 45 C.F.R. § 160.204 outlines a process by which a request can be filed with the Secretary for such a determination. Any exception determination made by the Secretary applies to all persons subject to the state provision in question. When a determination is made, HHS will publish a notice in the Federal Register and on related HHS web sites. *See* HHS's Office of Civil Rights, Frequently Asked Questions, Answer ID 407.

[36] According to 45 C.F.R. § 160.202, "more stringent" means, in the context of a comparison of a provision of state law and a standard, requirement, or implementation specification, a state law that meets one or more of the following criteria: (1) 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; (2) 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; (3) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration; (4) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information. 45 C.F.R. § 160.203(b) establishes that state laws that are more stringent are exempted from being preempted by the Privacy Rule.

[37] Health Privacy Project, The State of Health Privacy: A Survey of State Health Privacy Statutes, Second Edition, 2002, available at: http://www.healthprivacy.org/info-url_nocat2304/info-url_nocat.htm. *See also* State of New York, Department of Health, HIPAA preemption charts, October 15, 2002, available at: http://www.health.state.ny.us/nysdoh/hipaa/hipaa_preemption_charts.htm.

[38] Health Privacy Project, The State of Health Privacy: A Survey of State Health Privacy Statutes, Second Edition, 2002, available at: http://www.healthprivacy.org/info-url_nocat2304/info-url_nocat.htm.

[39] Health Privacy Project, The State of Health Privacy: A Survey of State Health Privacy Statutes, Second Edition, 2002, available at: http://www.healthprivacy.org/info-url_nocat2304/info-url_nocat.htm.

[40] Health Privacy Project, The State of Health Privacy: A Survey of State Health Privacy Statutes, Second Edition, 2002, available at: http://www.healthprivacy.org/info-url_nocat2304/info-url_nocat.htm.

[41] Health Insurance and Portability and Accountability Act of 1996, Pub. L No. 104-191, 261, 110 Stat.1988 (1996).

[42] The HIPAA Security Rule (with an April 2005 compliance date) provides detailed provisions related to how covered entities must protect electronic health information.

ensure that technology would improve care without jeopardizing confidentiality.

As the health care industry adopts more technologically sophisticated methods of record maintenance and patient communication, patients' access to their own personal health information could potentially become easier and more cost-efficient. By guaranteeing patients access to their own health information, the Privacy Rule set in place an important incentive for consumers to actively engage in health information technologies, such as electronic medical record (EMR) systems and personal health records (PHRs).[43] In fact, the Privacy Rule requires that covered entities provide information in the requested format if it is "readily producible."[44] At the same time, covered entities can exercise their ability to impose reasonable fees associated with providing access to personal health information. As such, the preamble of the Privacy Rule points out that if, in the course of providing access to a patient, electronic copies are made to a computer disk, any fees could include, for instance, the cost of the computer disk.[45] It is important to note that where covered entities receive the services of vendors, or "business associates," in the course of developing an EMR system, for instance, the contract must stipulate that the business associate will make protected health information available for access, amendment, and accounting of disclosures.[46]

However, since the Privacy Rule only applies to "covered entities," some entities that have access to protected health information are not covered by the federal law. For instance, some private companies offering consumers PHR services are not covered by the law and therefore the federal right to an accounting of disclosures would not apply. This is problematic and serves as a critical reminder that strong laws and standards must be implemented to protect and extend established rights of patients.

As long as covered entities are collecting, using, and storing protected health information, the Privacy Rule and its access requirements apply to that entity—whether the information is stored electronically or not. The opportunity exists to build in patient access to records, even if not directly required by HIPAA. State laws related to patient access may also surpass HIPAA's requirements in this area.

Patient Access and the Record Locator Service

Connecting for Health's Record Locator Service (RLS) is intended as a critical line of communication within and among sub-network organizations (SNOs),[47] and, as a matter of principle, patients should be able to access the RLS. At this stage, however, there are serious privacy and policy issues that must be addressed regarding such access.

Both the HIPAA Privacy Rule and the **Connecting for Health** "Architecture for Privacy in a Networked Health Environment" are instructive here. As discussed above, patients have a federal right to see and copy their medical records held by a provider. However, since the RLS may not be covered under the HIPAA Privacy Rule as a provider, plan, or clearinghouse, there may be no legal obligation to provide patients access to the information in the index. But, as a matter of principle, the RLS should be designed to provide such access in a secure, authenticated manner.

The nine principles articulated in the **Connecting for Health** "Architecture for Privacy in a Networked Health Information Environment" support this philosophy. The most pertinent principles are "openness and transparency," "individual participation and control," and "data integrity and quality." The principle of openness and transparency asserts that patients should be able to establish what information exists about them in the data

[43] Like electronic health records (EHRs), personal health records (PHRs) can be Internet-based and are designed to provide easy access to important health-related information about patients. Unlike EMRs, however, PHRs would be controlled entirely by the patient and would include information provided by the patient.

[44] 45 C.F.R. § 164.524(c)(2).

[45] Available at: http://aspe.hhs.gov/admnsimp/final/PvcPre02.htm.

[46] *See* 164.504(e)(2)(ii)(E-G).

[47] A sub-network organization (SNO) is to operate as a health information data exchange organization (whether regionally or affinity-based) that operates as a part of the National Health Information Network (NHIN), a nationwide environment for the electronic exchange of health information made up of a "network of networks."

market and in government databases, should be able to track how that information is used, and by whom. The principle of individual participation and control clearly stipulates that patients should be able to see and amend their information: "at all stages in the information chain, they should be able to inspect and query their information…they should have clear avenues to correct information." The data integrity and quality principle further emphasizes this point, establishing that patients "should have clear avenues to view all information that has been collected on them, and to ensure that that information is accurate, complete, and timely."[48]

Based on the access provisions of the Privacy Rule and the principles articulated in the **Connecting for Health** "Architecture for Privacy in a Networked Health Information Environment," it becomes clear that, ideally, patients should have access to the information in the RLS. Allowing patients the opportunity to independently access information held in the RLS will empower patients to be more informed and active in their care.

However, providing access to the RLS is not a simple task. Significant privacy and security concerns come into play when considering giving patients direct access to the service. Authentication poses a significant challenge for allowing such access. Ensuring that information is not accessed by unauthorized individuals is central to establishing privacy and security, but developing a reliable and convenient method of authentication even beyond the issue of patient access remains a significant obstacle in the field of health information exchange. The problem with authentication is both fundamental and widespread. Indeed, one of the longest functioning SNOs—the Indianapolis Network for Patient Care (INPC)—cites authentication as a challenge.[49] Outside of the health care industry, experts in banking and government continue to struggle with devising policies and technologies that would allow individuals access to data while ensuring security. Many proposals have come forth. For instance, the Liberty Alliance Project—an open standards organization representing over 160 companies—emphasizes decentralized authentication, allowing individuals to link "elements of their identity…without centrally storing all their personal information."[50]

A few current health information exchange networks have taken steps to address patient access in a secure environment. Caregroup, a Massachusetts-based hospital consortium using electronic information exchange, is often noted for its strong privacy and security practices, including those for authentication. Caregroup implements a three-tiered authentication process for providers, requiring users to prove identity with a user name, password, and a SecurID Token system.[51] Caregroup's PHR service for patients follows this model—requiring users to authenticate themselves twice—passing through both a front and interior "door."

The RLS poses unique challenges related to patient access and authentication; yet given the imperative of allowing patients the ability to see, copy, and amend their personal health information, it is important to work towards realizing goals supported by the **Connecting for Health** "Architecture for Privacy in a Networked Health Information Environment" principles.

Recommendations:

- Each SNO should have a formal process through which information in the RLS can be requested by a patient or on a patient's behalf.
- Participating entities and SNOs shall consider and work towards providing patients direct, secure access to the information about them contained in the RLS.

Conclusion

The access provisions of the Privacy Rule serve as an important baseline for ensuring that patients have adequate control over their personal health information. Meanwhile the

[48] *See* **Connecting for Health**, "The Architecture for Privacy in a Networked Health Information Environment."

[49] **Connecting for Health**, "Clinical Data Exchange Efforts in the United States: An Overview," Data Standards Working Group: Background Paper, available at: http://www.connectingforhealth.org/resources/dswg_bckgrdr_appx_a.pdf

[50] Liberty Alliance Project, "Introduction to the Liberty Alliance Identity Architecture," March 2003.

[51] Pam Abramowitz, "Be Prepared. Be Very Prepared: Hospitals Forging Ahead With IT Security Plans," Health Care Finance, http://www.hcfinance.com/May/secure.html.

principles articulated in the **Connecting for Health** "Architecture for Privacy in a Networked Health Information Environment" recommend taking these rights further, establishing that patients should have access to all their information, including information held outside of a covered entity. With this in mind, a discussion about how to give patients access to the information held in the RLS is appropriate.

The RLS could ultimately empower patients. Patients' ability to access a reliable list of where their personal health information is stored could significantly enhance their ability to access and potentially amend information. It is, therefore, important to adopt policies and procedures that adhere to the notion that patients should have the same access to their own information that health care providers do.

EHRs, PHRs, and similar information systems could significantly enhance patient participation, with untold benefits to both individuals and the general public. Using the RLS and asserting their rights to access under the Privacy Rule could go a long way to ensuring that patients play an active and informed role in their own health care.

Acknowledgements

The members of the **Connecting for Health** Policy Subcommittee have accomplished an extraordinary task in less than a year's time—the development of an evolving piece of work that can serve as the core of nationwide health information exchange—the policy components of **The Common Framework**. During this time, we have been fortunate to work with respected experts in the fields of health, information technology, and privacy law, all of whom have contributed their time, energy, and expertise to a daunting enterprise. Our consultants and volunteers have worked long hours in meetings and conference calls to negotiate the intricacies of such issues as privacy, security, authentication, notification, and consent in health information exchange.We offer them our heartfelt thanks for taking on this journey with us, and look forward to the remaining work ahead.

In addition, we would like to offer special thanks to the volunteers and consultants who authored the initial drafts of this body of work—their hard work created a strong foundation upon which to focus the Subcommittee's deliberations:Stefaan Verhulst, Clay Shirky, Peter Swire, Gerry Hinkley, Allen Briskin, Marcy Wilder, William Braithwaite, and Janlori Goldman.

Finally, we must note that none of this work would have been possible without the leadership and inspiration of our co-chairs, William Braithwaite and Mark Frisse.They have led us with steady hands and determination of spirit.

Connecting for Health Policy Subcommittee

William Braithwaite, MD, eHealth Initiative, (Co-Chair)

Mark Frisse, MD, MBA, MSc, Vanderbilt Center for Better Health, (Co-Chair)

Laura Adams, Rhode Island Quality Institute

Phyllis Borzi, JD, George Washington University Medical Center

Susan Christensen*, JD, Agency for Healthcare Research and Quality, United States Department of Health and Human Services

Art Davidson, MD, MSHP, Denver Public Health

Mary Jo Deering*, PhD, National Cancer Institute/National Institutes of Health, United States Department of Health and Human Services

Jim Dempsey, JD, Center for Democracy and Technology

Hank Fanberg, Christus Health

Linda Fischetti*, RN, MS, Veterans Health Administration

Seth Foldy, MD, City of Milwaukee Health Department

Janlori Goldman, JD, Columbia College of Physicians and Surgeons

Ken Goodman, PhD, University of Miami

John Halamka, MD, CareGroup Healthcare System

Joseph Heyman, MD, American Medical Association

Gerry Hinkley, JD, Davis, Wright, Tremaine LLP

Charles Jaffe, MD, PhD, Intel Corporation

Jim Keese, Eastman Kodak Company

Linda Kloss, RHIA, CAE, American Health Information Management Association

Gil Kuperman, MD, PhD, New York-Presbyterian Hospital

Ned McCulloch, JD, IBM Corporation

Patrick McMahon, Microsoft Corporation

Omid Moghadam, Intel Corporation

Joyce Niland, PhD, City of Hope National Medical Center

Louise Novotny, Communication Workers of America

Michele O'Connor, MPA, RHIA, MPI Services Initiate

Victoria Prescott, JD, Regenstrief Institute for Healthcare

Marc A. Rodwin, JD, PhD, Suffolk University Law School

Kristen B. Rosati, JD, Coppersmith Gordon Schermer Owens & Nelson PLC

Sara Rosenbaum, JD, George Washington University Medical Center

David A. Ross, ScD, Public Health Informatics Institute

Clay Shirky, New York University (Chair, Technical Subcommittee)

Don Simborg, MD, American Medical Informatics Association

Michael Skinner, Santa Barbara Care Data Exchange

Joel Slackman, BlueCross/BlueShield Association

Peter P. Swire, JD, Moritz College of Law, Ohio State University

Paul Tang, MD, Palo Alto Medical Foundation

Micky Tripathi, Massachusetts eHealth Collaborative

Cynthia Wark*, CAPT, United States Public Health Service Commissioned Corps, Centers for Medicare and Medicaid Services, United States Department of Health and Human Services

John C. Wiesendanger, MHS, West Virginia Medical Institute/Quality Insights of Delaware/Quality Insights of Pennsylvania

Marcy Wilder, JD, Hogan & Hartson LLP

Scott Williams, MD, MPH, HealthInsight

Robert B. Williams, MD, MIS, Deloitte

Joy Wilson, National Conference of State Legislatures

Rochelle Woolley, RxHub

Amy Zimmerman-Levitan, MPH, Rhode Island State Department of Health

**Note: Federal employees participate in the Subcommittee but make no endorsement*