P1 P2 P3 P4 P5 P6 P7 P8

T1 T2 T3 T4 T5 T6 M1 M2

The Architecture for Privacy in a Networked Health Information Environment

The Architecture for Privacy in a Networked Health Information Environment

The Architecture for Privacy in a Networked Health Information Environment*

Executive Summary

Introduction and Overview

A networked health information-sharing environment has the potential to enable decision support anywhere at any time, improving public and individual health, and reducing cost. Consumers and patients can benefit directly when their personal information is available to health care providers, and indirectly when their information is available in the aggregate to researchers seeking new ways to prevent, manage, or cure health problems. At the same time, the potential benefits must be weighed against the risks of privacy and security violations, which may increase if not addressed at the outset.

The accompanying document begins from the premise that any new health network needs to take into account the potential for such violations, and to build privacy and information security into its architecture from the outset, not as an afterthought. The document provides background on the issues at stake, explains the current status of health privacy, considers new challenges and opportunities in an electronic environment, and offers some solutions for a comprehensive response to those challenges.

I. What is at Stake?

The paper begins by examining why privacy matters, both in an online and offline environment. It first considers privacy as a matter of individual liberty, autonomy, and even a fundamental human right. All these perspectives remain applicable in a health context, but in addition, breaches of confidentiality are harmful because they can lead to so-called "privacy protective behavior," in which patients avoid seeking health care in order to protect their personal information. Such behavior has a toll on both individual health and, more generally, on public health. It suggests just one important reason why we need to build confidentiality and security into a networked environment.

II. Health Privacy: Definitions and Underlying Concepts

This section considers the concept of privacy, both as it applies to a general environment and more specifically to the medical context. It begins by considering the historical evolution of the term. In 1890, Samuel Warren and Louis Brandeis famously argued that privacy should be defined as "the right to be let alone." Today, definitions tend more closely to resemble Alan Westin's notion of "informational privacy," which suggests that the concept should be understood as an individual's right to control personal information.

Such a definition is particularly important in a global information age, and this section identifies two considerations that are repeatedly voiced regarding the handling of medical data. The first concerns the almost unlimited uses for medical information. Data gathered in a medical context and used for other purposes, it is argued, poses serious privacy risks. The second concern emphasizes the benefits that can be accrued through medical data. This section points to these tremendous benefits, and argues that, while confidentiality of information is essential, patients may miss out on some of the benefits if data controls in the name of confidentiality over-restrict the uses and dissemination of information. The solution is to find a balance between the potential harms and the potential benefits represented by medical

* **Connecting for Health** thanks Stefaan Verhulst, Chief of Research, Markle Foundation, for drafting this paper.

data. That balance can be achieved through a careful deployment of appropriate technologies, combined with strong laws and other forms of confidentiality protection.

III. Health Privacy in a Digital Health Information Networked Environment: What is Different?

This section argues that existing notions of medical privacy are somewhat outdated in a networked health information exchange environment. It discusses six risks increased by such an environment, arguing that these risks require new and innovative solutions. While some of these risks exist in an offline world, they have become more pronounced, in large part due to the scale of data transactions and the relatively greater ease of collecting, linking, and disseminating information over a network, and to a reduced ability to "leave the past behind" and to shield sensitive information. Among the increased risks include:

1. **Commercial misuses of data**, including the use of medical data to deny or restrict insurance coverage; restrict credit or other financial benefits; or in unsolicited marketing;
2. **Government misuses of data**, including secondary use of personal health information by government agencies (for employment and other purposes) and the need to balance national security with health privacy considerations;
3. **Criminal misuses of data**, including fraudulent acts that result in financial or other harm;
4. **Security breaches**, including hacking and other criminal activities that lead to "data leakage";
5. **Data quality issues**, including data corruption and loss; and
6. **Harmful social consequences**, including stigma, exposure, and embarrassment.

IV. Defining a Comprehensive Privacy Architecture: Establishing Trust in the Network

This section defines some principles for responding to the above risks and protecting medical privacy in a networked environment. It begins by discussing existing privacy protection principles adopted in the United States, the Organisation for Economic Co-operation and Development (OECD), and Canada. It then argues for the following nine principles:

1. **Openness and Transparency**
2. **Purpose Specification and Minimization**
3. **Collection Limitation**
4. **Use Limitation**
5. **Individual Participation and Control**
6. **Data Integrity and Quality**
7. **Security Safeguards and Controls**
8. **Accountability and Oversight**
9. **Remedies**

Together, these nine principles amount to a comprehensive privacy protective architecture that can—and should—be applied in a networked environment.

V. Current Laws and Guidelines and How They Integrate an Architectural Approach

This section includes a brief overview of existing privacy protection laws in the United States. It begins by discussing federal protections, and in particular protections built into the Health Insurance Portability and Accountability Act of 1996 (HIPAA). It then discusses the patchwork of state laws, pointing out that these generally fall into three categories: constitutional protections, common law protections, and statutory protections. Finally, it discusses the emergence of, and potential difficulties and opportunities posed by, new community based health networks.

VI. Conclusion

The conclusion offers a summary of the preceding discussion. In particular, it revisits the nine principles and argues that they need to be considered together, as part of an integrated and comprehensive approach to medical privacy.

Introduction and Overview

As we move towards the creation of a health information environment, the potential for privacy intrusions increases, with potentially devastating impact on quality and access to health care. Any up-front planning should take privacy and security into consideration. This paper starts from the belief that it is possible—and necessary—to build privacy into health information technology (HIT) applications so that its benefits can be maximized. It aims to provide background on what is at stake, what has already been achieved in health privacy, what makes the current environment different, and how to provide for a comprehensive response. The paper provides for nine privacy architectural principles that should guide the design of policies, practices, and technologies to protect privacy in a networked environment. In addition it briefly provides an overview of current attempts to address the privacy and security issues within the context of a networked health information environment.

I. What is at Stake?

Individual Liberty and Autonomy: An International Approach

In many countries and treaties, privacy is considered a fundamental right, equivalent to other basic individual liberties such as freedom of speech and thought. Both the United Nations Declaration of Human Rights and the International Covenant on Civil and Political Rights, for example, recognize the right to privacy. In these treaties, privacy is recognized as a form of autonomy, a way to ensure protection from "arbitrary interference"[1] by the state or other entities. In addition, several broad, international principles exist that have been adopted (and adapted) by a variety of countries. For example, as we shall see, in its 1995 Directive on Protection of Personal Data, the Organisation for Economic Co-operation and Development (OECD) led the way in defining several principles for privacy protection. The European Union (EU) and other countries have subsequently adopted these. Interestingly, this directive differs significantly from the US approach in that it takes a broad, omnibus approach to privacy protection rather than the sector and often state specific approaches adopted in the United States.

Understood in this broad way, as a fundamental human right, a violation of privacy can be considered a serious violation of an individual's basic rights, equivalent, perhaps, to imprisonment without trial or the denial of free expression. Naser and Alpert (1999) point out that this violation is particularly serious in a medical context, where patients are often already somewhat helpless and in a position of dependence.[2] They write: "When patients … disclose intimate secrets about themselves they also become more vulnerable. Patients who are ill already have a diminished sense of autonomy" (22). In such instances, robbing individuals of their privacy is tantamount to a serious violation of their individual liberty.

Privacy Protective Behavior in a Medical Context

In addition to a violation of individual rights, the loss of privacy in a medical context has other negative consequences, some of which can be understood as collective harms. Social scientists have frequently established that surveillance, not just in the medical field, but across fields, can have a "chilling effect" on individual behavior (Alpert 2003; Goffman 1966; Westin 1967). In the medical field, this chilling effect can lead to what experts call "privacy protective behavior" (Goldman 1998, 49). Such behavior includes hiding evidence of pre-existing conditions from doctors or insurance companies; paying out-of-pocket for treatment; or simply avoiding treatment altogether.

Goldman, in a paper on the importance of medical privacy, lists four negative consequences of such privacy protective behavior (Goldman 1998, 49):

[1] United Nations, Universal Declaration of Human Rights, Article 12. Available at: http://www.nps.gov/elro/teacher-vk/documents/udhr.htm.

[2] The EU Directives mentioned above similarly treat medical violations of privacy as particularly egregious cases.

(1) The patient may receive poor-quality care, risking undetected and untreated conditions.
(2) The doctor's abilities to diagnose and treat accurately are jeopardized by a lack of complete and reliable information from the patient.
(3) A doctor may skew diagnosis or treatment codes on claim forms, keep separate records for internal uses only, or send incomplete information for claims processing to encourage a patient to communicate more fully.
(4) The integrity of the data flowing out of the doctor's office may be undermined. The information the patient provides, as well as the resulting diagnosis and treatment, may be incomplete, inaccurate, and not fully representative of the patient's care or health status.

Survey Evidence

These negative consequences are not mere hypotheticals. A large number of surveys over the years have consistently shown that the public is concerned about breaches in confidentiality, and that "privacy protective behavior" is a very real phenomenon. For example, as reported by Janlori and Hudson (141), a 2000 survey of Internet users found that 75 percent of respondents were worried that health sites shared information without consent; and that a full 17 percent would not seek health information on the web due to privacy concerns. Another poll, also conducted in 2000, found that 61 percent of Americans felt that "too many people have access to their medical records."[3] Overall, concern about privacy seems to have increased over time: while a Harris Interactive Inc. poll conducted in 1978 found that 64 percent of respondents were concerned about privacy, a similar poll conducted in 1995 by Harris found the number had increased to 82 percent (Goldman 1998, 50).

The surveys also show that such concerns frequently lead to privacy protective behavior. For example, in a survey conducted by the California HealthCare Foundation, more than one out of six adults said they had done something "out of the ordinary" to hide private medical information (Alpert 305). In another survey conducted by Harris in 1993, 11 percent of respondents said they sometimes chose not to file an insurance claim, and 7 percent said they sometimes neglected to seek care in order to avoid damaging their "job prospects or other life opportunities" (Goldman 1998, 50).

Such behaviors do not just cause potential damage to an individual patient's health. They also impose a collective burden, leading to greater costs and public health problems that an already overstretched health system can ill-afford.

II. Health Privacy: Definitions and Underlying Concepts

Understanding the concept of privacy is essential to designing better policies, practices, and technologies to protect consumer and individual privacy. The trouble, however, as one observer points out, is that "privacy is a notoriously vague, ambiguous, and controversial term that embraces a confusing knot of problems, tensions, rights, and duties" (Bennett 1992, 11-12). In attempting to define privacy, one expert resorts to a version of Justice Potter Stewart's famous definition of pornography, arguing simply that: "You know it when you lose it" (Goldman 1999, 101). In an effort to lay the foundations for our following discussion of policies and principles, this section attempts to provide a certain amount of conceptual clarity to the idea of privacy.[4]

Privacy as a General Concept

One of the earliest definitions of privacy was published in 1890, in a *Harvard Law Review* article by Samuel Warren and Louis Brandeis. In that article, entitled "The Right to Privacy," Warren and Brandeis argued that privacy could be defined as "the right to be let alone." The article was drafted in response to concerns over the potential privacy violations that would occur as a result of a new technology. Warren and

[3] These and more survey results can be found at: http://www.epic.org/privacy/survey/.

[4] While much of this discussion refers to broad federal approaches to privacy, it is essential to recognize that privacy protections in the United States have been far more localized and sector-specific. Indeed, the states, not the federal government, have generally led the way in protecting privacy.

Brandeis were writing about the modern press, and particularly the instantaneous photograph, which they felt invaded "the sacred precincts of private and domestic life."

More than 100 years later, we continue to grapple with difficult problems surrounding privacy, and once again, the concern is largely driven by technology. The now-classic definition of privacy in the information age was supplied by Alan Westin, who in his 1967 book, *Privacy and Freedom*, argued that: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (7).

Westin's definition of privacy is probably the most prevalent, and widely-accepted, today. It is sometimes referred to as "informational privacy,"[5] and it is easy to see why this notion of privacy would have particular relevance in the digital era. In 1971, Harvard professor Arthur Miller predicted that all individuals would eventually be the subjects of a "womb-to-tomb dossier." Westin himself argued that, in the information era, every individual was accompanied by a "data shadow" which could reveal even the most intimate and apparently mundane details about his or her life.

Privacy is Not a Static Concept

Such a data shadow, if it indeed materialized, could seriously threaten individual privacy and, by extension, a host of other liberties that citizens in modern Western democracies take for granted. Michael Froomkin, for example, has predicted the "death of privacy." It is important to recognize that the notion of privacy is not static. It changes with time, as the evolution from Warren and Brandeis' concept to Westin's definition makes clear; and it changes depending on the field or environment to which it is applied. This means that privacy is a malleable concept; its treatment and protection can be changed to suit public concerns. In the following sections of this paper, we show how certain protections can be established in response to current concerns over privacy. First, it is important to understand how the concept of privacy is context-sensitive. It is sensitive to particular historical moments. In a more recent article, Westin argues that post-war understandings of privacy have undergone four distinct phases (2003, 434). These include:

- A Privacy Baseline Phase, which ran from 1945 to 1960, and was marked by a relative inattention to, and lack of concern regarding, privacy issues;
- The First Era of Contemporary Privacy Development (1961-1979), which for the first time "marked the rise of information privacy as an explicit social, political, and legal issue";
- The Second Era of Privacy Development (1980-1989), which continued some of the concern begun in the First Era, but overall, "can be seen now as a period of relative calm before the storm";
- And finally, the Third Era of Privacy Development (1990-2002), which "is the period when privacy became a first-level social and political issue in the United States, assumed global proportions, and was impacted by 9/11 and its aftermath."

Privacy and Health

In addition to these well-defined periods, privacy can also be applied to a range of distinct issues; it is sensitive, too, to the field or realm within which it is applied. National security, commerce, and fraud all have privacy dimensions. Although many of these may overlap, there might also be some differences. It is therefore useful to spend some time on the trajectory of privacy as a medical concern. This is particularly important because, as Westin points out, health plays a critical role in his Third Era. Indeed, Westin explicitly points to the rise of genetic testing and the possibility of electronic health records as concerns in this new era (2003, 442).

Although health may have risen to the top of the privacy agenda in recent years, it has long been a topic for privacy advocates and policymakers. As pointed out in a recent report

[5] The US National Information Infrastructure Task Force defines the term as: "Information privacy is an individual's claim to control the terms under which personal information—information identifiable to an individual—is acquired, disclosed, and used." (See http://www.disastercenter.com/Html/PrivacWG.htm; http://www.datenschutz-berlin.de/gesetze/internat/een.htm)

by the Health Privacy Working Group, an initiative, comprised of diverse health care stakeholders (plans, providers, accreditors, and scholars), located at Georgetown University and directed by the Health Privacy Project, national attention to medical privacy can be traced back at least to 1973, when "there were calls for increased attention to the privacy concerns presented by the use of computers in the health care industry" (10).[6] Janlori Goldman also points out that the guidelines and codes of practice developed by the US Department of Health, Education, and Welfare in 1973 continue to serve as the underpinnings for a variety of privacy laws across sectors, suggesting the central role always occupied by concerns over medical privacy (1999, 103). The Privacy Protection Study Commission, created by the Privacy Act, expressed some of those concerns in 1977. "It appears," wrote the Commission,

> *"that the importance of medical-record information to those outside of the medical-care relationship, and their demands for access to it, will continue to grow ... There appears to be no natural limit to the potential uses of medical-record information for purposes quite different from those for which it was originally collected."* [7]

In these and other discussions of health as a privacy concern, at least two distinct themes can be identified. The first, pointed out by Sheri Alpert in a wide-ranging review of the literature on medical privacy, is evident in the above quote, and particularly in the Privacy Protection Study Commission's concern that "there appears to be no natural limit" to the uses of private medical data. As Alpert puts it, there is a recurring concern in the literature over the potential "harm that can befall patients if their medical information is disclosed either in ways that exceed their expectations or if information reaches the hands of people who should not have access to it" (Alpert, 304). She cites a number of authors expressing concern over such potential misuse, and argues that the primary purpose for a patient's personal health information is—and should be—"the clinical diagnosis, treatment, and care of that patient" (305).

The second recurring theme is somewhat contradictory. It provides a counter-argument to Alpert's point, emphasizing the tremendous potential benefits that can be accrued through medical data. Briefly, it is anticipated that the use of medical data, particularly when enabled by electronic health records, has the potential to transform the way patients receive care, and to introduce a far greater degree of efficiency and effectiveness in our nation's medical care system.

Individuals recognize these potential benefits. The same surveys that reveal concern over privacy also show that people are eager to exploit the potential benefits of new technologies. A study conducted by Foundation for Accountability (FACCT) for **Connecting for Health** revealed that while 70 percent believe a personal health record would improve quality of health care, almost all respondents (91%) indicated that they were very concerned about privacy and keeping their health information secure.[8] Likewise, a 2005 survey conducted by the consulting firm Accenture found that an overwhelming number of respondents thought medical care would improve if doctors had access to electronic medical records (EMRs); at the same time, asked to rank their top five concerns with EMRs, respondents put privacy at the top of the list.[9] In recent congressional testimony, Westin stated that "surveys show that most consumers want the opportunities and benefits of our consumer-service and marketing-driven society. With proper notice and choice, more than three out of four consider it acceptable that businesses compile profiles of their interests and communicate offers to them." He pointed out that some 63 percent of Americans, or 125 million people, can be classified as "Privacy Pragmatists": they are willing to share a certain amount of information in the interests of greater efficiency and service,

[6] For a copy of the report, see http://www.healthprivacy.org/usr_doc/33807.pdf.

[7] http://aspe.os.dhhs.gov/datacncl/PHR1.htm.

[8] Available at: http://www.connectingforhealth.org/.

[9] See http://www.accenture.com/xd/xd.asp?it=enweb&xd=_dyn\dynamicpressrelease_857.xml.

as long as they know their information will be safeguarded with privacy protections.[10]

One of the central challenges confronting privacy advocates is to find a balance between these two themes—what Westin, writing on the concept of privacy generally, calls the "distinctive balance between the private sphere and the public order" (2003, 432). Much as it is essential to protect confidentiality of information, so it is essential for our privacy and information laws to maximize the potential benefits that can be offered by medical data. Patients must not feel that their information is misused in any way that violates their privacy; but equally, if information is not shared or disseminated at all, then patients themselves will be the losers.

The solution to achieving this balance lies in well-defined principles that protect information while permitting it to be shared in a meaningful and productive way. Building on the recommendations of the Health Privacy Working Group (many of which were included in HIPAA Privacy Regulations), this backgrounder discusses steps to "integrate privacy protections as part of information practices" (8). This process of integration, in which confidentiality and security protections are built into the architecture of electronic health records and other means of using data, is the best way to ensure that the full benefits of information technology are realized while at the same time protecting the confidentiality and security of personal health information.

III. Health Privacy in a Digital Health Information Networked Environment: What is Different?

We have seen that conventional notions of privacy are today equated with the right to protect information about one's self. The right to privacy may therefore be thought of as a right to secrecy, and privacy protections, whether legal or otherwise, commonly designed to remedy "invasions of secrecy", for example, through illegal entry into an individual's home. Such protections are often designed with reference to an individual's "right to consent" i.e., confidentiality is typically protected by the principle that individuals must give their consent before information about them is allowed to leave the protected domain.

As we shall see, these principles are somewhat outdated in the context of an electronic network. In particular, the widespread availability of databases containing personal information challenges the "right to consent" and "invasion" principles upon which so many privacy protections are currently based. For example, when an individual's personal health information is aggregated with other patients' data and resold as part of a database, no opportunity is given to the individual in question to provide consent on reuse of that information. Indeed, in many cases an individual will not even know that his or her personal health information has been reused.

The new environment poses a host of additional challenges to existing privacy protections and principles. If we are to develop effective solutions, it is essential to better understand these new challenges. It needs to be clear, at the outset, that while a digital and networked environment offers much potential and many opportunities, it also poses several new categories of risk. This section will explore some of those risks.

After exploring those new risks, this section will discuss some privacy architectural principles to deal with those risks. A central principle of this backgrounder is that new privacy challenges cannot be addressed solely by focusing on post-violation remedies and penalties, but also (and more importantly) through network architectures that govern the information flows and the handling of personal information. Such architectures must be designed in a way to protect privacy before violations occur. Therefore, after outlining the new risks, we argue that privacy in a digital setting requires *structural and systemic approaches*.

New Environment, New Risks

1. Commercial Misuses of Data

Perhaps the most serious—and probably pervasive—privacy violations in the information age stem from the potential for commercial

[10] http://energycommerce.house.gov/107/hearings/05082001Hearing209/Westin309.htm.

misuse of data. In recent years, an extensive data market has developed, driven largely by data aggregators or "data brokers." These data brokers collect, repackage, and sell information that is either available in the public domain, or they illicitly aggregate data that was collected for another purpose from that for which it is ultimately used.[11] Deborah Platt Majoras, Chairman of the Federal Trade Commission, described the general data market of personal information in recent Senate testimony:

> The information industry is large and complex and includes companies of all sizes. Some collect information from original sources, others resell data collected by others, and many do both. Some provide information only to government agencies or large companies, while others sell information to small companies or the general public.[12]

The emergence of data as a commodity, traded in often-opaque information markets, has led to serious concerns about privacy. In *No Place to Hide,* Robert O'Harrow describes in vivid detail the wealth of information that now exists on individuals, and the various and frequently harmful ways in which it can be used, often without the individual's knowledge or consent. Some possible harms include:

- *Denial or Restrictions on Insurance Coverage and Other Benefits:* Information acquired in one medical setting (for example, routine testing) can become part of an individual's data shadow and later be acquired by insurance companies to deny or otherwise restrict coverage. At least two companies, the Medical Information Bureau (MIB) and AllClaims, currently offer databases of patient medical records to insurance companies and others. Such commercial use of data represents a serious problem in part because inadequate insurance cover creates new and potentially serious public health problems. It is also a serious concern because, as we have seen, knowledge of such risks leads to privacy protective behavior on the part of individuals that can pose further health problems.

- *Restrictions by Credit or Other Agencies:* Medical data can also be acquired commercially and used by non-medical agencies like credit card companies or banks. If such data points, for example, to a serious underlying medical condition, it can lead to denial of credit, mortgages, or other financial services. This "leakage" of information from a medical to non-medical setting is a serious problem in an era of data aggregation; it shows the need not only to build privacy protections within the health care sector, but also to develop strict procedures to control transmission of information across sectors.

- *Unsolicited Marketing:* Data acquired commercially can also be used by pharmaceutical companies and others to market drugs based on information about individuals' medical condition. Two notable cases of such marketing occurred in 1998, when CVS and Giant Food, two pharmacy chains, offered patient prescription records to private companies that later used the records as the basis for marketing. In addition to the underlying privacy violation involved in making the data available, it can also be argued that the unsolicited marketing itself represents a privacy violation.[13]

2. Government Misuses of Data

The debate over privacy and data aggregation often refers to commercial uses of data. However, the state also makes frequent use of an individual's medical data shadow for law

[11] The illicit use of data is not particular to the networked environment. What has changed is the scope of potential violations: As the network expands and as the amount of data increases, so does the possibility of confidentiality violations. In addition, a networked environment facilitates the illicit acquisition (e.g., through theft) and dissemination of data. This is in large part due to digitalization of information, which is easier to store, and to steal without its original owner even noticing.

[12] http://judiciary.senate.gov/testimony.cfm?id=1437&wit_id=4161.

[13] Goldman (1998, 10).

enforcement and other purposes. In 1998, for example, police in Virginia, investigating a car theft from a parking garage near a drug treatment center, collected 200 medical records as part of their investigation; they later acknowledged their actions as an unnecessary violation of patient privacy. State welfare agencies and the Immigration & Naturalization Service (INS) have also used welfare and immigrant health records in the administration of their respective programs.[14]

An emerging category of risk that is particularly worth highlighting stems from the increasing capability of governments to indulge in surveillance activities. A recent report, jointly issued by the American Civil Liberties Union (ACLU), Focus on the Global South, Friends Committee (US), International Civil Liberties Monitoring Group (Canada), and Statewatch, highlights the risk.[15] It argues that individual pieces of information on travel and other practices that are currently being collected could lead to an international surveillance framework that "dwarfs any previous system and makes Orwell's book *Nineteen Eighty-Four* look quaint." These individual pieces include registration of foreigners, national ID policies, and biometric identification methods.

The report also points out that much of this information is collected in the name of national security. The authors argue that the information will not fulfill its stated purpose, but the stated reason for collection does point to a complication in addressing privacy violations by the state, namely, that government collection and use of data often has legitimate and vital national security purposes. In a post-9/11 environment, in particular, data can be useful in stopping terrorist attacks before they occur. A national information network is today considered critical to enhancing the nation's intelligence programs. As many—including the Markle Foundation—have argued, however, it is essential that such a network be designed with built-in protections for privacy.

Such protections would be both architectural (i.e., built into the design of the network), practices, *and* policy-based. We discuss architectural solutions below. One important policy step involves reform of the 1974 Privacy Act. In recent Senate testimony, James Dempsey, the Executive Director of the Center for Democracy & Technology (CDT), pointed out that government use of data is susceptible to privacy violations due to shortcomings in that act, which requires government agencies to collect and use data subject to the provisions of the Fair Information Practices. But as Dempsey further pointed out, such protections are only relevant to "federal 'systems of records', [meaning] ... that the government can bypass the Privacy Act by accessing existing private sector databases, rather than collecting the information itself." He went on to describe the possible negative consequences that can occur when the government accesses private data without the restrictions of the Fair Information Practices:

> *[A]lthough the Privacy Act requires notice to and consent from individuals when the government collects and shares information about them, gives citizens the right to see whatever information the government has about them, and holds government databases to certain accuracy standards, none of those rules applies when the government accesses commercial information without pulling that data into a government database. Currently, the government need not ensure (or even evaluate) the accuracy of the data; it need not allow individuals to review and correct the data; and the government is not limited in how it interprets or characterizes the data.*[16]

3. Criminal Misuses of Data

Both commercial and government uses of data have legitimate purposes; generally, misuses and privacy violations represent the exception rather than the norm. But digital data, medical or otherwise, is also susceptible to criminal misuse, which can result in serious violations of privacy, considerable financial expense, and even physical injury and death.

[14] Health Privacy Working Group (1999, 10).

[15] http://www.theregister.co.uk/2005/04/21/icam_surveillance_report/.

[16] http://judiciary.senate.gov/testimony.cfm?id=1437&wit_id=2875.

Identify theft, in which criminals acquire Social Security numbers or other identifying information, represents a particularly serious problem. In 2003, the Federal Trade Commission (FTC) estimated that 10 million Americans (nearly 5 percent of the adult population) were victims of some form of identity theft.[17] According to the FBI, the Internet Crime Complaint Center (IC3), a joint project between the FBI and the National White Collar Crime Center, received more than 100,000 complaints regarding identity theft in the 5-year period between its opening in 2000 and 2005. It estimated the costs of identity theft as nearly $40 billion annually, not including credit card fraud.[18]

For all its seriousness, identity theft represents just one possible instance of criminal misuse of data. It imposes substantial financial costs, but other types of illegal activity can result in even more dangerous consequences. Consider the following two examples:

- In 1999, a woman named Amy Boyer was murdered as the direct result of her data shadow. She was killed when a man purchased her Social Security number, address, and other information from a data broker called Docusearch (the man paid just $154). The information was used by the man, who had been obsessed with Boyer since her youth, to find her place of work and kill her.[19]
- Concerns about similar criminal misuse of data were also raised in a 2005 case brought by a Juneau, Alaska nurse who sought to have her address removed from public records, a licensing condition for all nurses. Expressing a fear of stalkers, she argued, with the assistance of the ACLU, that making her address publicly available posed a serious threat not only to her privacy, but also to her physical safety.[20]

[17] http://judiciary.senate.gov/testimony.cfm?id=1437&wit_id=4161.

[18] http://judiciary.senate.gov/testimony.cfm?id=1437&wit_id=4162.

[19] http://judiciary.senate.gov/member_statement.cfm?id=1437&wit_id=2629.

[20] http://www.adn.com/news/alaska/story/6399520p-6278454c.html.

4. Security Breaches

As the above examples illustrate, data can be acquired and misused by criminals in two ways:

- Through legal means, by following or purchasing a legitimate data trail. In such cases, it is the subsequent misuse that is illegal, not the acquisition of the data itself.
- Through criminal acquisition and use of data, in which the way the data is collected is itself illegal. Such criminal acquisition frequently arises as a result of security breaches, discussed in this section.

Security breaches, sometimes referred to as "data leakage," represent a serious category of risk in the information age.[21] They are not unique to the information age, but digital records and networks present particular vulnerabilities that do not exist in a paper-based world. These risks include the relatively greater ease of remotely hacking a network than physically breaking into a paper records depot; and the fact that large quantities of data are stored on servers and hard disks that are connected to the world, protected only by firewalls or other imperfect security protocols. In addition, digital data is much easier to replicate, and such replication can be done without damaging or removing the original, making it easier to acquire data illegally without the owner even being aware.

These and other factors make it easy to steal or criminally acquire data in the information age. Recent examples suggest that criminals are well aware of network vulnerabilities and that criminal acquisition of data is a growing risk. Recently, for instance, Ameritrade, an online broker, announced that it had lost a tape backup containing data on 200,000 current and former customers. This followed announcements by Lexis Nexis that up to 310,000 customer records may have been hacked; and reports by ChoicePoint, a data aggregator, of similar violations.

Such examples highlight the inherent vulnerabilities of networks and information stored in a digital format. While we have

[21] For a listing of recent security breaches and data violations, see http://www.privacyrights.org/ar/ChronDataBreaches.htm.

outlined some of the security vulnerabilities, many more exist. Of course it is impossible to fully protect a network against all forms of intrusion—the best we can hope for is to minimize intrusions.[22] The important point is that the existence of such vulnerabilities requires architectural solutions that build security protections from the start, rather than post-fact remedies. We discuss some possible architectural solutions in the following section.

5. Data Quality Issues

In addition to introducing a greater potential for security breaches, a digital environment also introduces potential data quality issues. Problems with data quality, which include data loss or corruption, are not traditionally thought of as privacy violations, but are closely interrelated with current privacy concerns.

Consider, for example, some recent anecdotes regarding the wrongful inclusion of individuals on national no-fly lists or other terror databases. Inclusion in such databases can be considered a privacy violation on at least two counts. First, it can automatically lead to private data being viewed by a range of agencies and groups, which could claim access on national security grounds. For example, if an individual is wrongly placed on a federal no-fly list, local law-enforcement agencies might also gain access to that individual's information based on law-enforcement sharing procedures.

Second, and more relevant to a discussion of medical privacy, it is important to recognize that much as individuals can be placed by mistake on no-fly lists, so they can be included in medical databases with false identifying information. Patients could, for example, be denied insurance based on mistaken information regarding medical conditions; similarly, they could be forced to pay higher life insurance or other premia.

It is important to acknowledge that, for the moment, such risks remain often theoretical, and that they are not particular to the online world, but also exist in a paper-based system of records. Nonetheless, they highlight the need not only to build strong privacy protections into network architecture, but also remedies and means of appeal against data quality issues. If patients are not able to have privacy or data quality grievances addressed in a quick and clearly identifiable manner, there is a danger that those grievances will be compounded. In addition, a comprehensive approach to data quality must include procedures to ensure information integrity to prevent errors from occurring in the first place.

6. Harmful Social Consequences

Finally, while much analysis of privacy focuses on adverse economic or health consequences, it is important to recognize that privacy violations can impose a very real social cost on individuals, making it difficult for them to live meaningful lives within their communities. One notable example occurred in 1998, when a San Diego pharmacist revealed a man's HIV-positive condition to his ex-wife. The man, who was locked in a custody battle with the woman in question, ultimately settled the case rather than face the stigma of his condition being made public.[23]

The need to carefully control such social consequences is all the more apparent when we consider that societies also use such "shaming" techniques as regular tools for law-enforcement procedures. Consider the widespread use of so-called Megan's Laws to maintain public sex offender registries. The use of such legitimate and legal shaming techniques makes it essential to draw up strict rules to differentiate between acceptable disclosures of personal information in the public domain, and unacceptable disclosures.

Writing more than 200 years ago, Adam Smith, often considered the father of modern economics, argued that material well-being was just as important to human happiness as "the right to appear in public without shame." This argument is as true today as it was then, and it draws attention to the very real need for controls on how information about an individual is released into the public domain, and shared with a community.

[22] See for instance Paul Clayton (Chair): *For the Record: Protecting Electronic Information*; National Academy Press, 1997.

[23] Health Privacy Working Group (1999, 10).

IV. Defining a Comprehensive Privacy Architecture: Establishing Trust in the Network

The previous section described some of the categories of risk represented by new technologies and methods of information dissemination. Clearly, these risks and vulnerabilities require new responses. These responses, moreover, must not be ad-hoc or post-fact, but designed in a systematic and comprehensive manner. At the core of adequate privacy protection in the digital age is that it must be supported by policy, practice, and the architecture of the network.

The purpose of this section is to provide privacy architectural principles for the policy, technology and, more generally, for the social and economic context within which the technology is used. In what follows, we present nine core principles of privacy protection based upon Fair Information Practice Principles (FIPPs) and explain how they must be built into the way information is collected and shared. Before that, we review currently existing Fair Information Practice Principles.

Throughout this discussion, we must keep in mind that to be effective, the scope of the protection will need to be determined and defined. This requires considering whether different kinds of protections should apply for different kinds of data; the kind of relationship and the level of trust (either socially, contractually, or legally determined) one aims to address and achieve. In addition, one needs to focus on the various systems of records or the information flow and any third party that maintains those systems.

Fair Information Practice Principles

Before discussing our core principles for a networked environment, it may be useful to briefly consider some existing principles for privacy protection. These principles provide a useful template, but they are not optimized for a network-driven world. Many were designed long before the age of the Internet, data brokers, and data aggregation. As such, they may need to be tailored, adapted, and, in some cases, expanded to address the specific risk management challenges posed by the digital age in general, and the rise of EMRs in particular.

The Privacy Rights Clearinghouse, a nonprofit consumer group located in California, provides a useful review of existing Fair Information Practices.[24] Here, we provide a summary, based on that review, of existing privacy laws in three jurisdictions:

1. The ***United States***, including the 1973 Fair Information Principles and the 1974 Privacy Act;
2. The ***OECD***, including the 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; and
3. ***Canada***, including the 1995 Canadian Standards Association Model Code for the Protection of Personal Information.

1. The United States

The Fair Information Practices were implemented over thirty years ago (1973), when the US Department of Health Education and Welfare (HEW) formed a task force to consider the privacy effects of the spread of computer medical records. The Code of Fair Information Practices developed by this task force includes the following principles:[25]

1. **Collection limitation:** There must be no personal data record keeping systems whose very existence is secret.
2. **Disclosure:** There must be a way for individuals to find out what information about them is in a record and how it is used.
3. **Secondary usage:** There must be a way for individuals to prevent information about them that was obtained for one purpose from being used or made available for other purposes without their consent.
4. **Record correction:** There must be a way for individuals to correct or amend a record of identifiable information about them.
5. **Security:** Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the

[24] See http://www.privacyrights.org/ar/fairinfo.htm for a full discussion.

[25] Reproduced from "The Law of Privacy in a Nutshell," Robert Ellis Smith, *Privacy Journal*, 1993, pp. 50-51.

reliability of the data for their intended use and must take precautions to prevent misuse of the data.

It is important to note that, unlike many other industrialized countries, these practices have not been put into law at the federal level. While they have been codified at the state and sectoral levels,[26] no blanket safeguards exist to implement and oversee these protections at the national level.

One notable exception is the Privacy Act of 1974. However, as noted earlier, this law only applies to systems of records that exist within government agencies. A major weakness is that it allows agencies to use private sector data without applying any of the protections contained in the law.

2. The OECD

Unlike the United States, many European countries have adopted broad, omnibus privacy protections that apply across sectors and jurisdictions. The OECD developed its Fair Information Practices as far back as 1980, and the European Union (EU) has adopted many of these principles. In particular, they were codified in the European Union's Directive on Protection of Personal Data, implemented in 1995. The privacy guidelines adopted by the OECD include the following eight principles:[27]

1. **Collection Limitation:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. **Data quality principle:** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.
3. **Purpose specification:** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. **Use limitation principle:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9[28] except:
   (a) with the consent of the data subject; or
   (b) by the authority of law.
5. **Security safeguards principle:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.
6. **Openness principle:** There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity about usual residence of the data controller.
7. **Individual participation principle:** Individuals should have the right:
   (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;
   (b) to have communicated to them, data relating to them
      1) within a reasonable time;
      2) at a charge, if any, that is not excessive;
      3) in a reasonable manner; and
      4) in a form that is readily intelligible;
   (c) to be given reasons if a request made under subparagraphs (a) and (b) is

[26] E.g., in the form of the Fair Credit Reporting Act, the Right to Financial Privacy Act, the Electronic Communications Privacy Act, and the Video Privacy Protection Act.

[27] Reproduced from http://www.privacyrights.org/ar/fairinfo.htm.

[28] Para 9 of the OECD Privacy Guidelines states: "The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose." See http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

denied, and to be able to challenge such denial; and

(d) to challenge data relating to them and, if the challenge is successful, to have the data erased; rectified, completed, or amended.

8. **Accountability principle:** A data controller should be accountable for complying with measures which give effect to the principles stated above.

3. Canada

Canada has adopted a unique model when it comes to privacy protections. Its privacy guidelines have been formulated not by the state, but by a nonprofit entity, the Canadian Standards Association (CSA), which in 1995 adopted the "Model Code for the Protection of Personal Information."[29] This Code, which includes the 10 principles listed below, can be adopted on a voluntary basis by companies or other entities.

1. **Accountability:** An organization is responsible for personal information under its control and shall designate a person who is accountable for the organization's compliance with the following principles.
2. **Identifying purposes:** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
3. **Consent:** The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, with certain exceptions.
4. **Limiting collection:** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. **Limiting use, disclosure, and retention:** Personal information shall not be used or disclosed for purposes other than those for which it was collected except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.
6. **Accuracy:** Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
7. **Safeguards:** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
8. **Openness:** An organization shall make readily available to individuals specific information about its policies and practices relating to its handling of personal information.
9. **Individual access:** Upon request, an individual shall be informed of the existence, use, and disclosure of personal information about the individual and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. **Challenging compliance:** An individual shall be able to challenge compliance with the above principles with the person who is accountable within the organization.

As in many countries, these 10 principles are substantially similar to the OECD guidelines described above. However, it is worth noting that two principles in particular have been strengthened in Canada:

- **Consent:** As Principle 10 suggests, consent in Canada includes not just the right to limit access to one's personal data (number 3), but also the right to challenge an entities' compliance with the Code (number 10).
- **Accountability:** Accountability is held to be so important in Canada that it ranks first on the list of 10 principles. This puts the burden of protecting privacy substantially onto collectors and users of data.

Core Principles for a Networked Environment

Below, we present nine specific recommendations to ensure privacy. While some of these recommendations reflect and are derived from the Fair Information Practice Principles, they have been updated and designed specifically to protect privacy in a

[29] For more information, see http://www.privcom.gc.ca.

networked environment, keeping in mind the unique and new risks described in the previous section.

1. Openness and Transparency

Perhaps the most important mechanism for privacy protection in the information age, this first principle stipulates that there should be a broad and universal practice of transparency in the way data is handled. Individuals should be able to establish what information exists about them in the data market and in government databases. They should be able to track how that information is used, and by whom, and they should be able to control how that information is disseminated. Individual choice is critical; control of information rests with persons, not with data aggregators or data users.

It is also essential that individuals be aware of how they can exert such control. Having strict laws to ensure transparency and openness serves little purpose if people do not know how they can find out where information about them exists, and how they can control who has access to that information. Ideally, patients should be able to give their informed consent to any use of their information.[30] Outreach and education regarding privacy are critical, as is the role of civil society and consumer groups in facilitating such efforts.[31] One possible policy option is to require all data collectors and aggregators to register with a government agency, probably the Federal Trade Commission (FTC), and for that agency to maintain a secure[32] "one-stop" web site where people can view their data shadow.

2. Purpose Specification and Minimization

Data should never be collected without people knowing that it is being collected. Furthermore, they should always be aware of why that information is being collected, and how it will be used. This will allow them to give their informed consent to any act of data collection.

In addition, an important extension exists to this principle of purpose specification: data must be used only for the originally stated reason, or, in rare cases, for other purposes with specific legal sanction: see discussion below regarding "Use Limitation" (Principle 4). Currently, a number of privacy violations occur when data is collected for one legitimate purpose, with individual consent, and then resold and reused in another context, for a very different purpose. For example, clinical data may be collected to treat a patient, but later find its way to the hands of insurers or credit agencies that could use the information to deny coverage. A strict minimization requirement can prevent such unauthorized reuses of data.

3. Collection Limitation

The collection of personal information should be obtained by lawful and fair means and with the knowledge and consent of persons. There should be well-drafted and explicit permissions to ensure that data collectors state their purpose in ways that are clear and easily understood by the population for whom they are intended, without misleading language.

Collection limitation can be seen as an extension of "Purpose Specification and Minimization" (Principle 2). However, it goes beyond the requirement that data collectors specify *why* they are collecting information and suggests a blanket application of Principle 1 ("Openness") to all aspects and forms of data collection. For example, the principle of collection limitation requires that information only be gathered in a legal manner, and in a manner that is apparent to patients. This last requirement is particularly important in a networked environment, because technology is often opaque and unclear to average users. Many users, for example, have little idea of the wealth of information that exists on their computers in the form of cookies. They may similarly not be aware of the potential abuses

---

[30] Any provisions for informed consent need to be drafted in such a way that ensures the sharing of information is not unduly cumbersome on data users. It is probably unrealistic to assume that patients can or should give their assent to each and every use of their medical data.

[31] At the same time, outreach and awareness-building must be conducted with consideration for the potentially harmful effects on a public that is overly-concerned about privacy violations. See, for instance, the following article, which highlights concerns that patients might avoid care due to recent privacy fears: http://www.ihealthbeat.org/index.cfm?Action=dspItem&itemID=110098.

[32] Valid concerns have been raised that such a centralization may create additional security vulnerabilities.

that occur when they submit personal information to a medical or other web site. Thus, in addition to declaring their purpose clearly (Principle 2), data collectors should also be required to declare the very fact that they are collecting information.

4. Use Limitation

As stated, a minimization requirement would strictly limit whether data collected for one purpose could be reused in another context. Generally, we believe that such reuse should not be permissible without explicit consent of individuals.

However, certain legal exceptions may apply, particularly in the case of national security or law enforcement. Such cases should be the exception instead of the norm, and should be controlled by strict laws and sanctions. In addition, when information is reused, it is far preferable that the data in question be non-identifiable (i.e., it may consist of aggregated or demographic data), but to the greatest extent possible should not include information that could identify an individual. This allows data to be reused without representing a gross violation of an individual's privacy.

5. Individual Participation and Control

An important principle of privacy protection is that an individual has a vital stake in, and thus needs to be a participant in, determining how his or her information is used. Privacy protections should be designed with this principle in mind: individuals should be seen as key participants in processes of information collection and dissemination, and not as mere subjects or passive spectators. At all stages in the information chain, they should be able to inspect and query their information, and to determine who uses that information. In addition, as we shall explore further, they should have clear avenues to correct information.

Such control can be facilitated through the principles of transparency and the various limitations we have outlined above. In addition, whenever possible, personal information should be collected directly from the individual rather than from a third-party. This enhances patient control over personal information. Finally, control means that people should have meaningful opt-out clauses when they do not want their information to be reused, or when they want to "reclaim" their information. Currently, many opt-out procedures administered by web sites and others are complicated and cumbersome, making it near-impossible for people to exert real control. In addition, opt-out provisions can be diluted when they represent all-or-nothing choices, forcing people to choose, for example, between privacy and inefficient service.[33] For such reasons, "opt-in" is often regarded as providing more control to the patient: it allows patients explicitly to determine when, by whom, and for what purpose information is used. In the event patients do not understand the conditions under which their information is being used, they can choose to request more information, or refuse permission.

It is also important to note that greater individual control may confuse existing methods of determining and allocating liability for privacy violations and medical errors. For example, practitioners may be blamed for errors stemming from an individual's refusal to release medical information. Similarly, an individual could accidentally "leak" his or her own data through a "phishing" attack or other online breach. Overall, there will certainly be new and unforeseeable liability issues raised by greater use of EMRs and greater patient control. To the extent possible, these need to be addressed beforehand, in a systematic manner, as part of any Fair Information Practice Principles.

6. Data Integrity and Quality

We have seen that data corruption is a key—and new—source of privacy violation in the information age. It follows that mechanisms need to be developed to address this violation, and for establishing accountability among those who maintain records. Such mechanisms can include technical tools for quality control, as well as regular backups and redundancy in systems

[33] It is important to recognize that the flexibility of opt-out provisions is limited by what is technologically feasible. Any steps or provisions taken to protect confidentiality need to consider what is possible with existing technology. At the same time, technical limitations should never be used to justify breaches of confidentiality or privacy.

and databases. In addition, individuals should have clear avenues to view all information that has been collected on them, and to ensure that the information is accurate, complete, and timely. The tools could include laws drafted along the lines of the Fair Credit Reporting Act, which permits people to correct mistakes in their credit report.

Individuals should also be able to ensure that information is being used for the originally stated purpose—they should be able to correct errors in context as well as content. This requires that people be able to view not only *what* information exists on them, but *how* it is being used. A discrepancy in either can be viewed as a form of data corruption, requiring clearly-articulated and publicized avenues for redress.

7. Security Safeguards and Controls

Security breaches, discussed above, represent another potential source of privacy violation, and so security safeguards represent another important principle for privacy protections. Given the increasing frequency of hacking and other forms of cyber-crime, it is imperative that reasonable security safeguards be built against loss, unauthorized access, destruction, use, modification, or disclosure of personal information. In addition, all data collectors and disseminators should be mandated to immediately disclose any security breach through a direct communication to those consumers affected (i.e., not just by releasing the news to the media). Such laws, similar to California's information security breach law (Civil Code § 1798.29), will allow individuals to protect themselves through post-fact remedies.

Security represents an important example of how protections can be built into the design of technology. By implementing the right technologies, and by consulting security experts at the outset, key precautions can be taken at the design stage to increase the robustness of network security. For example, networks can be designed and built with enhanced identity management tools to ensure that access to information is limited to those with a specific need and authorization to see it. In addition, data scrubbing, hashing techniques, real-time auditing mechanisms, and a range of other technical tools can be deployed to ensure security. The key is to supplement legal protections with technical protections. That is the only way to ensure true data privacy.

8. Accountability and Oversight

It is essential that mechanisms be built to ensure that the responsibility for privacy violations is identifiable, and that remedial action can be taken. Boards of directors and senior management must be held accountable for any violations. It is their responsibility to ensure steps are taken to instigate, review, or modify their organization's risk management strategy as it relates to handling patients' information.

Several specific steps can be taken to enhance accountability and oversight. Organizations could be mandated to create a post for chief privacy officers (CPOs), who would fulfill the same duties with regard to privacy as CFOs and CTOs do with regard to finance and technology, respectively. In addition, organizations should hold regular employee training programs as well as privacy audits to monitor organizational compliance. These audits can be facilitated by technical tools that ensure clear audit trails and reveal patterns of use and potential abuse.

9. Remedies

This principle is closely related to Principle 8, with the exception that it probably entails greater participation by the state in the form of legal sanctions. One of the key challenges with enforcement of privacy rights is the difficulty (often impossibility) of clearly pinning blame, or even of tracing the source of a privacy violation. Solove and Hoofnagle (2005, 13) point out that approximately 50 percent of identity theft victims do not know how their information was accessed. Similarly, it is likely to be extremely difficult for a patient to monitor and identify violations of information contained in their EMRs. Without such information, it obviously becomes very difficult to seek remedies.

Some of the strategies described above (e.g., audit trails) can help pin the blame more accurately. In addition, internal controls such as those described in Principle 8 are also important to monitor uses and abuses of information.

While such remedies are not foolproof, they do help identify a data trail.

When it is possible to identify the source or perpetrator of a privacy violation, the next step is to ensure that clear legal remedies exist to address the situation. Minimum statutory punishments must be clearly articulated, as must damages for any violations.[34] Solove and Hoofnagle have also suggested that ways must be developed to avoid extensive class action litigation, e.g., by allowing state authorities to fine companies and disburse remedies to victims of privacy violations from a state-administered fund. Whatever the specific steps adopted, the important point is that enforcing sanctions and remedies is as important as establishing the protections themselves.

V. Current Laws and Guidelines and How They Integrate an Architectural Approach

The above describes a template for privacy protections. We have seen nine key steps required to protect medical data in the information age. In this section, we provide an overview of existing policies, both at the state and federal levels. In addition, we discuss the emergence of community-based or other health sub-networks and describe the challenges and opportunities they pose to the integration of federal and state provisions.

The overview provided in this section is somewhat limited. The variety and patchwork of laws that exist, particularly in the states, makes it near-impossible to present a comprehensive overview in this backgrounder. We have therefore chosen to focus on the most important and relevant laws and statutes and, within those laws, to focus on key themes. Throughout the text, we have provided links where more detailed information can be found.

A. Federal: HIPAA Privacy Regulation

In 1996, the United States Congress passed the Health Insurance Portability and Accountability Act (HIPAA), which governed how medical information could be collected and shared. HIPAA's privacy protections, contained in the HIPAA Privacy Rule, became effective for most organizations in 2003. These marked the first (and, thus far, only) federal-level protections for privacy of medical data.

Among the more significant measures introduced by the Privacy Rule were a guarantee of patient access to medical records; provisions to protect personal health information from misuse; provisions to ensure notice of use to patients; the right to file a complaint; and a requirement for health providers to provide patients with information on their privacy practices. Below we provide an overview of these and other key privacy protections. It also includes a discussion of HIPAA's related Security Rule, which governs how electronic information can be used, stored, and shared.[35]

Protected Health Information (PHI): One of the initial functions performed by HIPAA's Privacy Rule is to define the notion of protected health information (PHI). PHI covers a variety of information and data that could be used to identify a patient, including names, addresses, Social Security numbers, license numbers, medical record numbers, and so on. Under HIPAA, all PHI is subject to the limits on use and disclosure described below.

Limits on Use and Disclosure: Generally, PHI can only be used or disclosed for a person's medical treatment, payment-related activities, or routine operations of a health care provider. Other than for these three purposes, known as TPO, information can be disclosed only when it is considered in the public interest, or when it forms part of a de-identified data set (see discussion below). Under HIPAA, all other uses or disclosures of information must receive written authorization from the patient. In addition, patients have the right to access and view how their information has been used and disclosed.

Reasonable Safeguards: HIPAA also requires health care providers and businesses to ensure "reasonable safeguards" to protect PHI. Such safeguards could include shredding

[34] It is also worth noting that some observers have suggested that penalties for abuses should be strengthened in order to act as a deterrent against future abuses.

[35] The full and updated text of the Privacy Rule is available at: http://www.hhs.gov/ocr/hipaa/finalreg.html. The Security Rule is available at: http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp.

documents, ensuring that medical records are safely locked, using curtains or other dividers in treatment rooms, and a variety of measures to protect electronic health information (or ePHI; see the discussion below). While the range of possible safeguards is broad, the law clearly puts the burden of protection on providers, in the process establishing clear lines of responsibility and liability.

Providing Notice of Privacy Practices: As mentioned above, HIPAA requires providers to ensure that patients are aware of their privacy rights and of providers' privacy practices. Under the law, a "Notice of Privacy Practices" must be provided to patients in written form. In addition, the law also requires providers either to obtain written acknowledgement from the patient that he or she has received such notice; or at a minimum, providers must document that reasonable efforts have been made to obtain such acknowledgement.

Limited Data Set: One exception to the strict disclosure restrictions mentioned above is in the case of de-identified information and what the HIPAA law calls "limited data sets." In the case of such information, no explicit written authorization is required for sharing. Information is considered de-identified when it does not contain PHI identifiers, and when it is stored using standard statistical and scientific methods (e.g., for research purposes). Even when PHI identifiers are removed, a Data Use Agreement must exist between the provider and user of the information.

Mimimum Necessary Information: Although HIPAA permits providers to share information without patient authorization for TPO purposes, it nonetheless requires them to share the minimum amount of information. This concept of "minimum necessary" information is central to HIPAA's privacy protections. In practice, it means that providers need to have standards and codes in place that define the extent of information necessary for certain practices. It also generally means that providers or other entities can request a patient's full medical record only in exceptional circumstances.

Compliance and Enforcement: In addition to these central provisions, HIPAA includes a variety of provisions to ensure compliance and enforcement. These include stronger civil and criminal penalties for improper disclosures of PHI, as well as measures to train and provide information for health care providers to ensure that they are in compliance with HIPAA's privacy standards. The law also gives patients the right to monitor how their information is accessed and used, and to seek redress in cases where violations have occurred.

Security Rule: Although technically separate from the law's privacy provisions, HIPAA's Security Rule is closely related. While the Privacy Rule covers all forms of data (including paper-based information), the Security Rule applies specifically to electronic protected health information (ePHI). Under the Security Rule, entities are required to protect ePHI from reasonably anticipated threats, institute appropriate technical protections to defend networks, ensure the integrity of data and physical infrastructure, and limit access to authorized individuals. The Security Rule is technology-neutral, meaning that it does not prescribe particular technologies or standards for protecting ePHI, but it is nonetheless, quite specific in its requirements.

B. State Laws

In addition to the above designed federal laws, a patchwork of state laws exists to provide privacy protections. Indeed, in the absence of a national set of privacy standards, individual states have historically taken the lead in protecting medical privacy in the United States. This has offered certain benefits, particularly in those states where protections are strong, but many also feel that it represents a weakness in the US system, which lacks an over-arching approach to privacy.

A comprehensive overview of state laws is not possible here. In an extensive report on state statutes, the Health Privacy Project noted the difficulty of the task, pointing out that the terrain was uneven (Pritts *et al* 2003). That report, *The State of Health Privacy, Second Edition, A Survey of State Health Privacy Statutes,* remains the best resource for state protections.[36] In addition, Pritts presents a

[36] It can be accessed at: http://medicalrecordrights.georgetown.edu/publications.html. The 2003 version of the report updated an earlier version -*The State of Health Privacy: An Uneven Terrain (A Comprehensive Survey of*

conceptual discussion of many of the most important issues raised by state laws, including their relationship to federal laws like the HIPAA Privacy Act.[37] Other key issues include the federal pre-emption and the floor v. ceiling debate, and the way in which state laws are condition specific/circumstance specific and may be more stringent than HIPAA (Pritts 2002, 343, 335-36).

Pritts (2002, 330) notes that states can protect privacy through three legal avenues: constitutions, common law, and statute. The following summary of each of these avenues owes significantly to her discussion.

Constitutional Protections

State constitutional protections have recently been in the news due to alleged violations of Rush Limbaugh's medical privacy in Florida. In fact, state constitutions generally offer only limited protection. Most states contain an implied right to privacy similar to that in the US Constitution, and some explicitly protect medical privacy. Yet, as Pritts notes, those protections are generally designed to limit only state action, and are easily outweighed by disclosure requirements.

Only two states, California and Hawaii, stand out for their strong, constitutional protections of medical privacy. These protections apply both to violations by the state, and by the private sector. In addition, they are explicitly written to cover medical information, providing a strong bulwark against the lack of adequate federal protections.

Common Law Protections

State common law is somewhat more robust in its protections than state constitutions. Here, too, state law is fragmented and varied, but a growing number of courts have found grounds for two privacy rights in particular: the right to maintain confidentiality of information and a patient's right to access his or her medical information. These rights are important because many states do not grant a statutory right to access (Pritts 2002, 333, 349-50).

Despite the steady expansion of these rights, Pritts (2002, 332) notes at least two shortcomings in existing common law protections:

1. In cases involving disclosure of information, courts are increasingly finding legal grounds to accept cases,[38] but patients have had trouble proving the guilt of those who have allegedly "leaked" their information. There exists, in short, a high burden of proof for many patients, and court decisions in general have led to the conclusion that "the underlying duty of confidentiality is not absolute" (Pritts 2002, 332).
2. In cases allowing patients access to their information, courts have found numerous legal grounds on which to consider patients' complaints (e.g., adopting property principles). At the same time, there exists some disagreement on what "reasonable access" requirements would imply, and to what extent health care providers have discretion in deciding what information to make available to patients.

Statutory Protections

For some decades now, the main protections for patient medical privacy have come not through constitutional or common law, but rather through specially enacted statutory protections. Statutory protections have become so important that the previously mentioned Health Privacy Project reports focus almost entirely on this category of legal protection.

The scope of privacy laws is particularly diverse and uneven in this category of protections. Each state has its own principles and standards, and sometimes these principles clash. In addition, state laws are often highly specific, applying differently to various conditions, contexts, and participants.

In an attempt to enforce some cohesion on the patchwork of laws, Pritts (2002, 332)

State Health Privacy Statutes). Pritts (1999). In addition, the Health Privacy Project's web site offers a state-by-state listing of laws at: http://www.healthprivacy.org/info-url_nocat2304/info-url_nocat.htm.

[37] For a discussion, see Goldman (2001) and Pritts (2002).

[38] Colorado and Minnesota, for example, have recognized torts on the basis of "unreasonable disclosure of public facts." Others, including New York and Nebraska, have explicitly denied this right.

identifies the following six principles that are upheld to a greater or lesser degree across states:

1. Access to Information
2. Right to Amend Health Records
3. Restrictions on Use and Disclosure of Information
4. Notice of Information Practices
5. Security Safeguards
6. Accountability

As noted, these principles are upheld unevenly, and in different ways, across states. In addition, the situation is fragmented within individual states, where a patchwork of laws often means that privacy is protected in a somewhat piecemeal fashion. However, Pritts (2002, 339) notes a recent trend towards "uniformity" in at least some states. She cites California, Maine, and Hawaii as notable examples. Hawaii, in particular, has a "truly comprehensive health privacy law," which was adopted in 1999, and California has similarly inched towards such a comprehensive approach with a series of consumer- and patient-protective statutes.

A General Observation

Finally, while the above has highlighted the diversity of state laws, it is worth emphasizing one key and crosscutting finding of the original 1999 version of the Health Privacy Project overview of state laws. In one of the three main conclusions presented in its executive summary, the 1999 report indicates that, in general, "state laws have not kept pace with changes in health care delivery and technology" (Pritts 1999, 9). The report points out, for instance, that individual and institutional access to medical data will increase substantially as new technologies are adopted, and that state laws often fail to acknowledge this fact.

In addition, the patchwork and unevenness of state laws poses evident challenges to any attempt to adopt national EMRs or to protect privacy at the national level. This landscape of often robust but uneven protections is a critical factor that needs to be taken into account when designing privacy protection principles. Ultimately, both the technologies and the policies deployed will need to be flexible and forward-looking enough to adapt to this unevenness.

C. Health Information Sub-Networks: Emerging Rules

In addition to the above discussion of federal- and state-level protections, it is important to briefly consider the tremendous and exciting growth of community based or non-geographic sub-network health information organizations. Such organizations, which provide care at a community-level, are increasingly seen as an effective grassroots way to facilitate information sharing.[39]

As envisioned, these sub-networks would act as "nodes" on an eventual information-sharing platform. The urgency and importance of information sharing to transform health care is widely understood. Unacceptable rates of avoidable medical errors, as much as $300 billion in unnecessary expenses, and continuing disparities in health care quality constitute a call to action to the health care system and to policymakers. An information-sharing environment has the potential to enable decision support anywhere at any time, improving public and individual health and reducing cost.[40]

However, the US health care system is highly fragmented. Many types of organizations exist as part of the current health care network, from giant hospital systems and insurance agencies to individual practices, with all manner of specialists, clinics, and agencies in between. In addition, and perhaps more importantly,

[39] For a discussion of these sub-networks, often called "regional health information organizations" or RHIOs, see the following links: http://ccbh.ehealthinitiative.org/communities/community.aspx?Section=102&Category=148&Document=590 and http://www.healthcareitnews.com/NewsArticleView.aspx?ContentID=1751&ContentTypeID=3&IssueID=12. In addition, sub-network organizations operate as health information data exchange organizations (whether regionally or affinity-based) that operate 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."

[40] For a full analysis of the benefits of an information sharing environment, see *Achieving Electronic Connectivity in Healthcare: A Preliminary Roadmap from the Nation's Public and Private Healthcare Leaders*. Available at: http://www.connectingforhealth.org.

sharing patient's information will only succeed and be beneficial when it happens within a strong radius of trust.

Towards those ends, we must assume that any information sharing improvement will have to happen through a decentralized approach, where decisions about sharing are made by participating institutions and providers at the edges of the network. The system proposed, for instance, by the **Connecting for Health** Working Group on Accurately Linking Information for Health Care Quality and Safety,[41] would leave it to the providers to determine locally with their patients what to link, share, and disclose, building upon their existing foundation of trust.

By leaving these decisions at the edges or local sub-networks, it is assumed that the information-sharing environment can grow incrementally, if based upon interoperable standards, and provide for the necessary security and trust. However, multiple challenges remain to be solved for those local and regional entities from the outset. In particular, as they grow beyond their regional origins, they will require coordination between existing state, federal, and local protections.

In addition, networking health information poses certain practical challenges to the sharing of patient information. For example, when data is shared between a larger provider and a small, regional provider, assurances will need to be built into the system to ensure that both adhere to the same privacy safeguards. Without such assurances, both the smaller and the larger provider might be reluctant to share information due to liability concerns. Similarly, concerns have been raised that the proliferation of these community-based networks could overload existing organizations that need to comply with HIPAA and other statutes. The paperwork required to ensure privacy requirements have been met at every step could simply prove overwhelming.

These and other obstacles do not suggest that health information networks at the community level do not provide immense potential to realize a national health information environment; nor are they meant to imply that they should be exempt from existing and emerging privacy protections. Rather, the above discussion is intended to suggest the range of issues raised by the creation of a health information network, and that need to be addressed by technology and policy. Both avenues—technology and law—offer potential solutions, but it is important that we acknowledge the problems from the outset.

VI. Conclusion

The preceding discussion has made clear the complexity of the topic at hand. Protecting medical privacy and confidentiality in a networked era involves a wide range of issues, and requires the cooperation and involvement of a similar range of actors. Practitioners and patients are, of course, critical to the effective deployment of EMRs, or indeed any other successful use of technology in health care. But the involvement of public health authorities, insurance companies, data marketers, civil society organizations, and a variety of other entities is also essential. In addition, governments and others at different jurisdictions—municipal, county, state, national, and international—will have to be considered.

Each of these actors brings different perspectives to the table. These differences can be productive, representing a wealth of knowledge and experience. But they can also be problematic. The range of experiences is accompanied by a variety of agendas, and—put more charitably—a variety of priorities. Harmonizing and doing justice to all these priorities is one of the key tasks confronting advocates of medical privacy.

Success, essentially a balancing act, will require more than the somewhat piecemeal approach to privacy that currently exists and that has been reviewed in this backgrounder. This underscores the need for a systematic and architectural solution. The foundations of this solution are the nine principles described in Section IV. Considered and applied together, these principles add up to an integrated and comprehensive approach to privacy that can help overcome the current fragmentation. It is critical that the nine principles be considered as part of one package. Elevating certain principles

[41] Their report is available at: http://www.connectingforhealth.org.

over others will simply weaken the overall architectural solution this backgrounder has proposed.

Of course, the principles remain just that—principles—and their precise manifestation will vary from state to state, and from country to country. Yet while they are broad enough to apply across organizations, stakeholders, and jurisdictions, they are also specific and tangible enough to have real significance and practical effect. The key is to apply them in a thorough and comprehensive manner before creating any new information network, not as an afterthought, and not as an after-the-fact band-aid solution.

Works Cited

Alpert, Sheri A. 2003. "Protecting Medical Privacy: Challenges in the Age of Genetic Information." *Journal of Social Issues* 59:2: 301.

Bennett, Colin. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca, NY: Cornell University Press.

Brandeis, Louis D., and Samuel D. Warren. 1890. "The Right to Privacy." *Harvard Law Review* 4, 193–197.

Clayton, Paul. 1997. *For the Record: Protecting Electronic Information*. National Academy Press.

Froomkin, Michael. 2000. "The Death of Privacy?" *Stanford Law Review* 52: 1461, 1469.

Goffman, Erving. 1966. *Behavior in Public Places: Notes on the Social Organization of Gatherings*. New York, Free Press.

Goldman, Janlori. 1998. "Protecting Privacy To Improve Health Care." *Health Affairs* (Nov-Dec): 47.

Goldman, Janlori. 1999. "Privacy and Individual Empowerment in the Interactive Age." Pp. 97 in *Visions of Privacy*, eds. Colin Bennett and Rebecca Grant. Toronto: University of Toronto Press.

Goldman, Janlori. 2001. "The New Federal Health Privacy Regulations: How Will States Take the Lead?." *Journal of Law, Medicine and Ethics* 3/4: 2: 395.

Goldman, Janlori, and Zoe Hudson. 2000. "Virtually Exposed: Privacy and E-Health." *Health Affairs* (Nov-Dec): 141.

Health Privacy Working Group. 1999. *Best Principles for Health Policy*. Available at: http://www.healthprivacy.org/usr_doc/33807.pdf.

Kelman, Alistair. 2000. "*Review of Database Nation: The Death of Privacy in the 21st Century* by Simson Garfinkel." JILT (1). Available at: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_1/kelman/.

"Medical Files or Fishbowls?" *Washington Post*, 23 September 1997, A16.

Miller, Arthur. 1971. *The Assault on Privacy: Computers, Data Banks and Dossiers*. Ann Arbor: University of Michigan Press.

Naser, C., and Sheri A. Alpert. 1999. *Protecting the Privacy of Medical Records: An Ethical Analysis* (White Paper). Lexington, MA: National Coalition for Patient Rights.

Pritts, Joy et al. 1999. *The State of Health Privacy: An Uneven Terrain (A Comprehensive Survey of State Health Privacy Statutes)*. (Available upon request from the author.)

Pritts, Joy. 2002. "Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule." *Yale Journal of Health Policy, Law, and Ethics* II(2): 327–364.

Pritts, Joy et al. 2003. *The State of Health Privacy, Second Edition, A Survey of State Health Privacy Statutes.* Available at: http://medicalrecordrights.georgetown.edu/publications.html

Solove, Daniel, and Chris Hoofnagle. 2005. "*A Model Regime of Privacy Protection*," George Washington University Law School Public Law Research Paper No. 132. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=681902.

Westin, Alan. 1967. *Privacy and Freedom*. New York: Atheneum.

Westin, Alan. 2003. "Social and Political Dimensions of Privacy." *Journal of Social Issues* 59:2: 431

Privacy Architectural Principles[1]	Policies and Procedures in a Networked Health Information Environment	Use of Technology for Privacy Protection[2]	HIPAA Baseline Provisions[3]
Openness and Transparency *There should be a general policy of openness about developments, practices, and policies with respect to personal data. Individuals should be able to know what information exists about them, the purpose of its use, who can access and use it, and where it resides.*	– Transparency and tracking policies; – Collection and uses of personal data; – Adequate proper notice of privacy practices; – Disclosure procedures to individuals of security breaches; – Outreach and public education efforts to enhance awareness of privacy issues and privacy rights, as well as the risks and benefits of a networked environment.	– Standards and technologies for expressing policies; – Standards and technologies for discovering policies once an institution's HIPAA provider number is known; – Defenses against people using transparency as an opportunity for phishing.[4]	Notice of Privacy Practices. Under HIPAA, patient information can be used or disclosed for treatment, payment, and health care operations without specific patient consent or authorization. The term *health care operation* includes quality assessment, outcomes evaluation, underwriting, legal services, auditing, business planning, customer service, and numerous other functions. The rules give each patient the right to request that a covered entity modify the standard terms. However, the covered entity has no duty to agree to a patient's request.
Purpose Specification and Minimization *The purposes for which personal*	– Define acceptable uses of the system; – Define purposes of	– Audit and logging technologies (including versioning);	Authorization for use of protected health information for marketing and fundraising and minimum

[1] Considered and applied together, these principles add up to an integrated and comprehensive approach to privacy necessary for a connected health information exchange environment. **It is critical that the nine principles are considered as part of one package—elevating certain principles over others will simply weaken the overall architectural solution to privacy protection in a networked health information environment**.

[2] The use of technology for privacy protection depends to a large extent on the level of automatization of the envisaged process.

[3] HIPAA applies directly only to *covered entities*, which are health care providers, health plans (e.g., insurers, health maintenance organizations), and health care clearinghouses (organizations that facilitate the processing of health care claims and information). No other health care record keepers are covered directly. However, an organization that is not a covered entity may still become subject to the HIPAA rules if it functions as a *business associate* for a covered entity. A business associate is someone who carries out a function involving the use or disclosure of individually identifiable health information on behalf of a covered entity. The limited scope of the HIPAA rules and the narrow onward transfer provision mean that some health data covered by the rules can be transferred to others and escape the privacy protections of HIPAA.

[4] Phishing is a tool used to gain personal information for purposes of identity theft. It involves using (fraudulent) e-mail messages that appear to come from legitimate businesses.

data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes or others that are specified on each occasion of change of purpose.	collection and of access for separate users such as: health care provider; health plan; public health authority; other government agency (law enforcement); researchers; individuals accessing their own health information; contractors and vendors (these might have a separate agreement); – Develop policies requiring that data collected for one purpose should not be used for another; – Implement a minimization requirement.	– Standards for expressing uses.	necessary rule. Treatment cannot be conditioned on an individual giving authorization to disclose to other parties.

Collection Limitation *Personal health information should only be collected for specified purposes, should be obtained by lawful and fair means and, where possible, with the knowledge or consent of the data subject.*	– Define purposes of collection and of access for separate users such as: health care provider; health plan; public health authority; other government agency (law enforcement); researchers; individuals accessing their own health information; contractors and vendors (these might have a separate agreement).	– Separation of clinical and demographic information.	Authorization for use of protected health information for marketing and fundraising and minimum necessary rule.
Use Limitation *Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.*	– Define acceptable uses of the system; – Decisions about linking and sharing are to be made by the participating institutions and providers at the edges of the network; – "User" limitation: different categories of users to be governed by different rules based upon separate use agreements; – Some data may not be shared because of special sensitivity (e.g., alcohol/drug abuse history, psychiatric treatment); – Patient authorization procedures need to be clarified and streamlined; – Permitted disclosures need	– Technologies for de-identification; – Technologies for data aggregation; – Security to prevent unintended disclosures; – Limiting queries.	Use and disclosure controls and business associate provisions, including minimum necessary rule. *Note:* The rule creates specific standards for uses and disclosures for purposes such as public health, research, law enforcement, health oversight, abuse reporting, judicial proceedings, emergencies, organ donations, and other purposes.

	to be clarified (e.g., disclosure to health care providers for purposes of treatment, disclosure to health plans for payment); – Define reuse exceptions in cases of national security or law enforcement; – Use and disclosure for management and administration of Sub-Network Organizations (SNOs).		
Individual Participation and Control *Individuals should control access to their personal information;* *Individuals should be able to obtain from each entity that controls personal health data, information about whether or not the entity has data relating to them.* *Individuals should have the right to:* – *Have personal data relating to them communicated within a reasonable time (at an affordable charge, if any), and in a form that is readily understandable;* – *Be given reasons if a request*	– Patient authorization procedures; – Patient access to information procedures when information is: • Maintained by provider • Maintained by third party vendor; – User's responsibility w/r/t consent prior to sharing data; – Need for meaningful and clear patient control clauses that do not present "all or nothing" choices; – Consider ways to enhance patient control; – Clarify new liability issues arising from greater individual control; – Policies by which data may be withheld at direction of	– Differing degrees of control should be built into technology; – Users should be able to choose the level of control and necessary tradeoffs that are acceptable to them; – Defenses against phishing and data theft (through user authentication).	Right to access. *Note:* Authorization is required before disclosure to third parties other than for treatment, payment, operations, and other specified purposes.

(as described above) is denied, and be able to challenge such denial; and – *Challenge data relating to them and have it rectified, completed, or amended.*	patient; – Requirement to draft consent and authorization forms in clear language, easily understandable to users.		
Data Integrity and Quality *All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and current.*	– Policies to ensure accuracy, consistency, and completeness of data; – Check their information and correct any errors (possibly model on Fair Credit Reporting Act); – Patient should be able to correct context of data use as well as content of data (i.e., they should be able to correct any misuse of data); – Clarify the SNO's liability in the case of: • Failure of the system to operate as expected or at all; • Loss or corruption of data within the system; • Incomplete or inaccurate data; • Misuse of the system by others, including other users; • Breach of security of the system.	– Practices to ensure quality, accuracy, and availability, including backups, integrity checks, and periodic sampling; – Technical methods for allowing an individual to access and review his/her health record.	HIPAA Security Regulation and Privacy Regulation each require physical, technical, and administrative safeguards.

Security Safeguards and Controls *Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.*	– Authorizing, managing, and policing access to information in the system by all categories of users; – Clear security policies (User's responsibility to implement reasonable and appropriate measures to maintain the security of the system and to notify the SNO of breaches in security, including any specific measures required by the SNO's policies and procedures); – Policies to handle intra- and extra-community matching issues.	– Matching algorithm and thresholds; – Authentication of users; – Encryption technologies; – Auditing, service management, and logging.	HIPAA Security and Privacy Rules each require physical, technical, and administrative safeguards. *Note:* The general Security Rule requires covered entities to: – Ensure the confidentiality, integrity, and availability of all electronic protected health information (EPHI) 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 by the Privacy Rule; and – Ensure compliance by its workforce.

Accountability and Oversight *Entities in control of personal health data must be held accountable for implementing these information practices.*	– Contract administration; – Policies by which the user has clear and sole responsibility for use of the system and actions taken in reliance on data in the system; – Consider mandating a position of Chief Privacy Officer (CPO) in organizations; – Clear user enrollment and termination procedures; – Designate someone responsible for ensuring patients' rights, such as access and amendment.	– Logging tools; – Auditing tools (including versioning); – Tracking systems; – Standards and technologies for allowing remote institutions to identify those accessing data at the individual level.	Enforcement by United States Department of Health & Human Services (HHS) of Security and Privacy rules. *Note:* HIPAA imposes on each covered entity a series of administrative requirements. These include: 1) designating a privacy official responsible for development and implementation of privacy policies and procedures; 2) training staff in privacy; 3) establishing appropriate administrative, technical, and physical safeguards to protect the privacy of information; 4) establishing a compliance process for individuals; and 5) developing and maintaining written policies and procedures for implementing the privacy rules.
Remedies *Legal and financial remedies must exist to address any security breaches or privacy violations.*	– Policy and remedies for unauthorized disclosures.	– Web site with information about how patients can identify and pursue possible remedies.	HIPAA provides no private right of action, although state law may permit such suits. The Secretary of HHS accepts complaints and can investigate and seek civil penalties against covered entities that violate the privacy rules. Criminal enforcement may be available.

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*