Protecting Sensitive Health Information in the Context of Health Information Technology

June, 2010

This issue brief lays out key factors to consider in protecting sensitive health information in an electronic context. It includes a discussion of the definition of sensitive health information, the implications of electronic information sharing, and the challenges of separating sensitive information from other types. It then provides a set of principles, based on widely accepted Fair Information Practices, and some examples of how they can be applied through policy and technical solutions.

Introduction

Health information technology (HIT) provides opportunities to increase health care quality, efficiency, and access to services. But along with the promise of digital tools come concerns about privacy—especially when sensitive health information is involved. There are many ways HIT can enhance privacy, but it can also magnify the risks associated with privacy breaches.

Yet for the good of the individual and society, it is essential to encourage people to seek health care treatment when they need it, and to assure them that health information—especially sensitive health information—is as well protected as possible.

The intent of this issue brief is to educate and engage consumer organizations and inform their advocacy work, particularly as the HITECH provisions of the 2009 stimulus law and the 2010 health reform law encourage increasing numbers of health care providers and other health system participants to adopt HIT.

* This brief was drafted by Lygeia Ricciardi, Executive Director, Consumer Health, Clinovations, LLC, on behalf of the National Partnership for Women & Families and the Consumer Partnership for eHealth, with input from leading experts in the areas of health information technology, privacy, and consumer advocacy.
Defining “Sensitive Health Information” (or Not)

There has been considerable debate about what constitutes sensitive health information, and even whether it should be defined as a category distinct from other types of health information. For example, the Department of Health and Human Services (DHHS) does not make a distinction between the two in its implementation of the HIPAA Privacy Rule.¹

Among those that do make a distinction, most people agree that sensitivity is subjective and varies depending on the particulars of an individual’s situation and context. Influential factors include cultural and political norms, individual life circumstances, and the emotional and health status of the individual.² Despite a range of opinions about what qualifies, in general sensitive health information is considered to be information that carries with it unusually high risks in the event of disclosure.

Disclosure risks include the possibility of discrimination, social stigma, and physical harm (for example, in the case of information linked to domestic violence or reproductive health). In some cases, the disclosure risk effects extend beyond the individual to his or her family, employer, or others (for example, genetic information may divulge information about a family as well as an individual).

Categories of health information that are often considered “sensitive” include those related to:

- Domestic violence
- Genetics
- Mental health
- Reproductive care, including abortion
- Substance abuse

¹ In 45 CFR Parts 160 and 164, a response to public comment on the HIPAA Privacy Rule contains the following: “The Department treats all individually identifiable health information as sensitive and equally deserving of protections under the Privacy Rule.” p. 53222 http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privrulenot.txt.


*All links accessed on 6/18/2010.
• Sexually transmitted disease information, including HIV/AIDS
• VIPs such as celebrities, political figures
• Records for patients that have a personal (e.g. family member) or professional (e.g. co-worker) relationship with a facility employee

The existing body of laws and regulations on sensitive health information is not comprehensive or consistent—nor does it translate explicitly into an HIT environment. There are some federal requirements related to the handling of alcohol and drug abuse, in addition to a patchwork of state laws. The majority of states have laws that address information related to substance abuse, HIV/AIDS, and mental health, and fewer than half also have requirements that address genetics. But even states that have laws in these areas take different approaches and have differing requirements, a situation complicated by the fact that electronic health information exchange is increasing the flow of data across state lines.

The lack of consistent legal protections is also a concern throughout the payment chain, not just in the provision of health care services. Guidelines related to the provision of explanations of benefits (EOBs), for example, should support guidelines related to protection of records that are shared for treatment.

**Implications of HIT for Sensitive Health Information**

While the sharing of sensitive health information is not new, health information technology (HIT) intensifies both sharing and some of the concerns associated with it.

For purposes of this memo, HIT is defined in a very broad sense, encompassing numerous technologies, models, and entities engaged in using electronic tools to store and share data. While in practice the greatest short-term focus on this topic is likely to be on the implementation of EHRs and HIEs, thanks to funding from ARRA, the same general principles should also apply to sensitive information in PHRs, mobile applications, web sites, and other kinds of networks. The parties potentially soliciting and/or sharing information include health care providers, payers, patients, labs, pharmacies, insurance companies, and many others.

Though the specifics vary by context, in general HIT makes information easier to share, both because it is easy to make multiple copies of medical records or other

---


data, and because the transmission of that data can be instantaneous and is nearly cost free. Digital technologies and new ways of using them (e.g. Twitter) also increase the overall volume of potentially sensitive health data. New devices make it easier to capture data that can be fed into an EHR or PHR, and patients themselves are increasingly likely to use social networking and health websites to generate information about themselves (for example, by joining an online support group for a particular health condition).\(^5\)

**The Importance of Trust**

Privacy protections for HIT must be strong and effective in part because the public’s willingness to share sensitive health information—and sometimes any information at all—depends on trust. Surveys show that a lack of trust leads people to withhold information about their health, a choice that can put individuals and society in danger.\(^6\)

Surveys also show that the public trusts healthcare providers (specifically those doctors and others who directly care for them) more than anyone else in the health system. In integrating technology into the existing health ecosystem, it is essential to do so in a way that strengthens, rather than undermines, the patient-provider relationship. Any recommendation consumer groups make about protecting health data should be viewed through the lens of whether it enhances consumer trust generally and, more specifically, bolsters the relationship and trust between patients and providers.

**The Role of Technical Architecture**

The design of systems or products fundamentally shapes how they are used and the impact they have on individuals and groups. As the Markle Foundation has pointed out, you can’t build a network and then tack privacy policies on as an afterthought.\(^7\) The protection of sensitive information (and other social goals, such as transparency) has to be built into the design from the outset.

Given the importance of health care providers vis a vis public trust, systems and tools that enable them (and/or patients themselves) to play significant roles as

---

\(^5\) For example, see Bob Coffield and Jody Joiner’s article on the legal implications of health information and social media [http://healthcarebloglaw.blogspot.com/2010/03/ahla-connections-legal-implications-of.html](http://healthcarebloglaw.blogspot.com/2010/03/ahla-connections-legal-implications-of.html).

\(^6\) See surveys released by the California HealthCare Foundation on consumers and health information technology, such as this most recent one from April, 2010: [http://www.chcf.org/publications/2010/04/consumers-and-health-information-technology-a-national-survey](http://www.chcf.org/publications/2010/04/consumers-and-health-information-technology-a-national-survey). Additional survey results by the Markle Foundation on consumer views of health information technology can be found at [http://www.connectingforhealth.org/resources/surveys.html](http://www.connectingforhealth.org/resources/surveys.html).

gatekeepers or stewards of health information are ideal, whether information is stored locally on a desktop or online via cloud computing.

**Shaping Public Perceptions**
The relationship between HIT and privacy is by no means a simple tradeoff in which more sharing = less privacy. Yet sometimes people misconstrue it that way. Privacy breaches involving technology have been widely publicized, a fact that contributes to public fears. Many people are less aware, however, that technology itself also contributes to protecting privacy in numerous ways. For example, although a paper medical record might be inappropriately viewed and no one would know about it, the data in EHRs can be encrypted (and otherwise technically protected) so they are less likely to be breached in the first place. In addition, tools such as immutable audit trails can both act as a deterrent and identify breaches so they can be avoided in the future and so the victims can be remedied appropriately.\(^8\)

One important challenge is communicating clearly and honestly with the public about HIT, including its privacy risks. Though we can improve upon current privacy protections, there will always be some limits. People need to be aware of those limits and at the same time view them in the greater context of HIT’s impact on the quality of health care. Individuals also need to be well informed so they can make choices that are appropriate to their unique circumstances about when and how their information is used.

The public education plan being developed by the US Department of Health and Human Services (HHS) as part of the implementation of ARRA provides a critical opportunity. The HHS effort is tied in part to clarification of confusion about the HIPAA Privacy Rule, which has resulted in numerous unintended consequences, including blocking patients from accessing their own (or their loved ones’) medical records\(^9\). Both patients and providers need additional clarification about the legal protections concerning the sharing of health information in the context of a broader understanding of the benefits and risks of HIT.

**The Treatment of Minors**
Among the most pressing topics that need clarification in the context of HIT is how to handle minors. Questions include when minors should be able to consent on their own to the sharing of their information, and whether their parents have a right to obtain information about the minor’s health. In many (but not all) states, these

---

\(^8\) Kaiser Permanente uses a pop-up window in its EHR to deter people from looking at restricted patient records. The window reminds users that the record should be viewed only for particular purposes, that their access will be tracked, and that disciplinary action will be taken if access is inappropriate.

decisions are now left to provider discretion.\textsuperscript{10}

The recently enacted health reform legislation is likely to complicate matters because it enables children up to 26 years old to remain on a parent’s health insurance policy. These young adults who are no longer minors will require a distinct set of legal guidelines concerning the handling of health information.

It will also be important to figure out a mechanism whereby parents can pay for the health care services their children receive via their insurance without compromising the children’s privacy; privacy concerns extend beyond clinical data to financial transactions, and protections will have to be comprehensive across these domains to be effective.

\textbf{Separating Sensitive from General Health Information}

If we presume that sensitive health information should be treated differently from other kinds of health information—which may not in fact be the case—then in addition to defining categories of information that qualify as “sensitive,” it is necessary to separate sensitive information from other types. There are several ways to do this, including:

\begin{itemize}
\item Identifying particular key words (or fields in an EHR) that are “sensitive”
\item Differentiating information according to particular types (e.g. HIV test results are different from general lab results)
\item Differentiating information based on source (e.g. all information from reproductive health clinics is “sensitive”)
\item Differentiating information based on its age (e.g. information about some conditions that is older than five years may be less relevant—and thus can be left out)
\item Differentiating records based on identity of the patient (e.g. treat records of high profile individuals, or people with certain conditions, differently)
\end{itemize}

\textbf{Structured Data and Rules Engines}

Medial records on paper are difficult to sort. Whatever is written on a single sheet of paper is associated with everything else on that paper—and volumes of paper are unwieldy. By contrast, most EHRs on the market today have the capability to structure data so it resides in fixed fields (as in a spreadsheet). Structured data content can support segmentation of data, particularly in combination with rules engines.

Rules engines are software systems that execute a set of directions, and can be used

\textsuperscript{10} See also the Federal Privacy Rule – 45 CFR.164.502G, I-III.
to customize responses to particular situations. For example, a young adult might stay on his or her parent’s health insurance policy through the age of 26. When the adult reaches a certain age, a rules engine could automatically segment certain subsets of information (eg concerning reproductive health) to block it from parental access.

**The Limitations of Information Segmentation**

Despite these enhanced capabilities, it is difficult to separate information in a way that effectively protects privacy. For example, although a patient’s positive HIV test could be left out of his or her EHR, a medication list might reveal the underlying condition. Further, even if you segment data in one system or institution, numerous digital copies of the same set of records might exist, so it would be necessary to follow parallel procedures wherever a copy of the data existed, including the records of general practitioners, medical specialists, pharmacies, insurance providers, PHRs, etc. Consistent and universal segmentation presents a set of technical and policy challenges, since these entities would likely use different technologies and be governed by different legal requirements.

The problem becomes even harder when considering the possibility of collecting data about the individual, not only from the traditional medial record, but also from other sources, such as his or her online activities including searches for health information, participation in health forums, or emails that disclose sensitive information that could, in aggregate, point toward the likelihood of a particular condition.11

**Potential Down-Sides of Effective Segmentation**

In addition to feasibility challenges associated with separating sensitive health information from other types, many argue that it is detrimental to try do so. If a relatively complete picture of a patient’s health enables a health care provider to give the best quality care, hiding certain details could create risks. Others argue that providers currently operate with very incomplete data on patients, so the impact of making certain data unavailable is not very significant. In any case, it may be difficult for patients (or others) to discern when certain information is relevant and when it isn’t. (Does a primary care physician really need to know about a patient’s abortion 15 years ago? Probably not, but it depends.)

Some people support the use of “flags” in a medical record to indicate that some information has been withheld from it at the patient’s request. However, this approach can significantly undermine trust in the provider-patient relationship (or the patient’s relationship with a parent who has access to his or her record), and

---

11 See the forthcoming book by Latanya Sweeney, Visiting Scholar at Harvard University in Computer Science: “Connecting Your Dots: What they know from what you leave behind.” For her additional publications on related topics, go to [http://dataprivacylab.org/people/sweeney/cv.html#publications](http://dataprivacylab.org/people/sweeney/cv.html#publications).
also has the unintended effect of implying that where there is no flag, a record is truly comprehensive.

Finally, questions about the impact of separating sensitive data from other types also apply to aggregate uses of data. Such actions could skew research, the development of new drugs, quality measures, or public health information in ways that could negatively impact members of the populations whose data was hidden—or society more broadly. For example, failure to share information about communicable diseases that fall into the category of “sensitive”—such as sexually transmitted diseases—could dangerously increase their likelihood of spreading.

**Principles and Practices for Protecting Sensitive Health Information**

There are a variety of ways to approach protections for sensitive health data, some technical, some policy-related. The National Committee on Vital and Health Statistics (NCVHS), among others, has made recommendations for addressing sensitive health information, but its recommendations have not been enacted. As previously stated, the intent of this issue brief is to lay out some options. No matter which options consumer advocates decide to support, it is important to get direct input from consumers themselves and their representatives in addition to HIT or policy specialists.

An important point to address at the outset is whether sensitive health information should in fact be treated differently from other kinds of health data. If the consensus is yes, the approach will most likely vary depending on particular contexts, such as design or use of an EHR, PHR, HIE, etc. Any approach will also need to continue to evolve over time.

---

12 In 2008 NCVHS made recommendations to the Secretary of HHS concerning sensitive health information. It recommended that individuals be given “limited control” over the disclosure of certain categories of information about them via the Nationwide Health Information Network (NHIN). A patient would be able to choose from one or more designated categories (e.g. mental health information), and restrict the extent to which information in that category would be shared among providers. NCVHS acknowledged that work would need to be done in defining categories and developing mechanisms for sequestering data. See [http://www.ncvhs.hhs.gov/080220lt.pdf](http://www.ncvhs.hhs.gov/080220lt.pdf).


14 See Jan Walker, David Ahern, et al, “Insights for Internists: “I Want the Computer to Know Who I Am” for research on how members of the public can contribute to the design of PHRs and related technologies: [http://www.springerlink.com/content/2257k62j3r8850t5/fulltext.pdf?page=1](http://www.springerlink.com/content/2257k62j3r8850t5/fulltext.pdf?page=1).
The table below presumes a preference for treating sensitive health data differently from other kinds and gives some examples of particular policies and technical requirements. It is organized according to Fair Information Practices (FIPs) as interpreted by the Markle Foundation's Connecting for Health Collaborative (the column on the left). FIPs principles are widely accepted guidelines for the handling of electronic information. The Markle Foundation has reworked them in the specific context of electronic health information, and Markle's iteration of the principles has been widely endorsed. The Center for Democracy and Technology (CDT) has also contributed greatly to an analysis of how these principles should be applied in an HIT context.

Though this analysis does not definitively support a particular policy or technical solution, we do believe that FIPs should be comprehensively applied to the handling of all health data. The column on the right includes examples of how such principles have been and might be applied in practice. FIPs were intended to be used as a group. Rather than cherry picking one or two solutions, it is important to consider numerous mutually enforcing solutions that together address all of the principles.

---

<table>
<thead>
<tr>
<th>Connecting for Health Core Principles—based on Fair Information Practices (FIPs)</th>
<th>Applications of the Principles to Provide Extra Protection to Sensitive Health Data</th>
</tr>
</thead>
</table>
| **1. Openness and transparency:** Consumers should be able to know what information has been collected about them, the purpose of its use, who can access and use it, and where it resides. They should also be informed about how they may obtain access to information collected about them and how they may control who has access to it. | Facilities or providers that specialize in/treat sensitive health conditions should meet particular patient education objectives concerning how their data is handled. (e.g. spend time consulting patients face to face, distribute brochures, make materials available in numerous languages, etc.)

Online services that specialize in or handle information about sensitive health conditions (e.g. web sites geared toward substance abuse) should meet particular conditions for notice (e.g. layered notice, pop-up notice,) and content of that notice—such as warnings about whether anything posted by the patient is searchable on the Internet.

Consumers should have access to audit trails wherever sensitive information is concerned. |
| **2. Purpose specification:** The purposes for which personal 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. | Sensitive information should not be used for “secondary uses” such as law enforcement, hiring/firing decisions, research, marketing, decisions about whether to provide insurance coverage or financial support, etc. without explicit consumer permission.

There should be no fishing expeditions for law enforcement (e.g. in a the neighborhood of a substance abuse clinic where there is a lot of crime, police shouldn’t be able to request a list of patients).

Requests for access to identifiable health information about individuals should go through their healthcare providers as opposed to through Health Information Exchange (HIE) organizations, PHR providers, or other intermediaries.

PHRs and possibly EHRs and other technologies should offer proxy accounts (requiring separate authentication) so different users can access different subsets of data about an individual. (A patient may not want to share all of his or her information with a caregiver.) |
| **3. Collection limitation and data minimization:** Personal health information should only be collected for specified purposes and should be obtained by lawful and fair means. The | Consumers should not be required to divulge sensitive health information as a condition of receiving something else, such as general health treatment, a job, a raise, etc.

Be especially careful to use only the minimum necessary health information, particularly in the case of sensitive data.

Always use information in the least identifiable form. (For example, in |
<table>
<thead>
<tr>
<th>Collection and storage of personal health data should be limited to that information necessary to carry out the specified purpose. Where possible, consumers should have the knowledge of or provide consent for collection of their personal health information.</th>
<th>research in some cases it would be appropriate to eliminate exact birth dates of subjects and use ages instead.) Ensure that the architecture of systems that store sensitive health data supports decentralized control with patients and/or their providers acting as gatekeepers.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>4. Use limitation:</strong> Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.</td>
<td>The sharing of health information need not be reciprocal. For example, a substance abuse clinic that is part of an HIE should be able to request information about a patient from other HIE participants, but not be required to share data with others.</td>
</tr>
<tr>
<td><strong>5. Individual participation and control:</strong> Consumers should be able to control access to their personal information. They should know who is storing what information on them, and how that information is being used. They should also be able to review the way their information is being used or stored.</td>
<td>Make sure patients are able to change their preferences (or settings) concerning access to and use of sensitive health information. Require patient consents for use or redisclosure of sensitive health information that are separate from those for general health information. Patients should be able to decide whether and in what format they receive notifications related to their sensitive health conditions.</td>
</tr>
<tr>
<td><strong>6. Data quality and integrity:</strong> All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and up-to-date.</td>
<td>Patients should have access to their own information to help ensure its accuracy.</td>
</tr>
<tr>
<td><strong>8. Accountability and oversight:</strong> Entities in control of personal data.</td>
<td>The use of data sharing agreements such as the Data Use Agreements (DUA) and the Data Use and Reciprocal Support Agreement (DURSA) should be strongly encouraged or required of appropriate entities.</td>
</tr>
</tbody>
</table>

---

17 Some states (e.g. New York) require that separate consents be obtained from consumers concerning the redisclosure of sensitive health information in an HIE.
18 This is supported by 45 CFR.164.522, B1 – A provider must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.
| health information must be held accountable for implementing these principles. | Laws should be enacted barring discrimination using sensitive health information.\(^{19}\) In addition, stronger mechanisms to increase transparency are needed—currently it is difficult to trace the flow of data in order to discover discriminatory practices.

A mechanism to facilitate the sharing of sensitive health information across state lines while preserving differing state laws should be developed.

Entities not covered by HIPAA that handle sensitive health information (eg PHRs, HIEs) should be required to follow consistent guidelines.

Chain of trust agreements should extend to vendors and others who handle sensitive health information.

Independent bodies should be created to oversee the safe handling of sensitive health information in an HIT context (or of health information more broadly).

Consumers should be well represented in policymaking bodies related to sensitive health information. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>9. <strong>Remedies:</strong> Remedies must exist to address security breaches or privacy violations.</td>
<td>Additional guidelines and/or funding is required. Consumer groups should track the progress of the Department of Health’s Office of Civil Rights’ plan required by ARRA for addressing this issue.</td>
</tr>
</tbody>
</table>

\(^{19}\) GINA (the Genetic Information Nondiscrimination Act) is an example of such a law, but it covers only one category of sensitive health data.