Health Information Exchange and Your Privacy (California Medical Privacy Series) [1]

Health Information Exchange, or HIE, is a way of sharing electronic health information among doctors’ offices, hospitals, labs, radiology centers, and other health organizations. The now-defunct California Office of Health Information Integrity, which was charged with developing policies for HIE, offered this definition of HIE and how it is expected to operate:

HIE allows access [to] the right health information [by] the right health care personnel at the right time, providing safer, more timely, efficient, patient-centered care. HIE will allow the doctors and nurses treating you in a hospital or doctor’s office to access your medical history. For example, doctors can review recent lab results whether the test was conducted at your primary care provider, at the hospital, or at participating labs across the State. . . . Because all authorized doctors and medical personnel will see the same health information through the HIE, this will help to reduce any errors, avoid unneeded duplication of tests and procedures, and consequently, could reduce medical bills.

Health care providers compile and create a lot of sensitive information about you, including lab results, pathology results, diagnostic test images and results (such as radiology and other imaging diagnostics), prescription history, allergies, health care provider treatment orders, patient care summaries, provider visit reports, and referrals. Although having such information in a medical record may be essential to treatment, electronic exchange of all of this sensitive health information raises many unresolved issues. For example, there is no universally accepted definition of sensitive information. This term generally includes records that refer to treatment for HIV/AIDS and other sexually transmitted diseases, treatment for substance abuse, mental health issues, and genetic information. Nor are there universal standards for who needs to know or access particular kinds of medical information, or what information is or is not necessary for a particular use or purpose. In addition, identifying and separating sensitive information from a larger record can be technologically challenging.

For these reasons, California health care providers and HIEs are generally excluding what California laws define as sensitive medical information from electronic exchange for the time being. However, excluding sensitive medical information is a practice, and not a formal policy.

2. Are there Health Information Exchanges already operating in California and elsewhere?

Although health information exchanges have a long way to go until they are actually performing all the functions expected of them, there are a number of operative HIEs across the U.S. and in California that are at various stages of fulfilling some of those functions.

It is likely you are already experiencing some effects of HIE. One change that should be apparent is that your health practitioner will likely enter information into a computer during your visit. This step is mandated by the HITECH Act as a step toward
meaningful use of technology in health information exchange. This practice is called computer-assisted physician order entry (CPOE), and involves recording an up-to-date list of diagnoses, all current medications (including non-prescription) and medication allergies, vital signs and changes in vital signs, smoking status, and demographics. If this sounds similar to a paper intake form you have filled out before, it is. The primary difference is that now all of the data is going into computer and may be shared more easily.

Another important goal of HIE is to involve patients more actively in their own health care by giving them more information about it. This means that you should receive an electronic copy of your health information including diagnostic test results, problem list, medication lists, and allergies on request and within 48 hours. You should also receive a clinical summary of each visit you make to a health care provider. If you are enrolled in Kaiser Permanente, for example, you already have a patient portal, where you can log in online, see your lab results, and send and receive secure emails with your providers.

3. What is the Nationwide Health Information Network?

The Office of the National Coordinator for Health Information Technology [2](ONC), part of the U.S. Department of Health and Human Services, defines the Nationwide Health Information Network [3](NHIN) as “the set of standards, specifications and policies that enable the secure exchange of health information over the Internet.”

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) set the goal of having an operative NHIN by 2014. However, the complexities of information sharing have been difficult to overcome. Vendors of health information and exchange systems have not helped with a reluctance to make competing systems compatible and by generally promising more than they deliver. Health providers remain possessive of their data and reluctant to share it. And the answer to the question of who pays for it all remains elusive.

4. Which laws protect the privacy and security of electronically exchanged health information?

HIPAA privacy regulations apply to medical records in any format, which generally means paper or electronic. The security regulations apply only to electronic health information. California law applies to both. The HIPAA Privacy Rule and Security Rule may be found at 45 CFR Parts 160, 162, and 164 [4].

HIPAA regulates covered entities, which it defines as health care providers, health insurers, and health care clearinghouses (an entity that standardizes health information, such as a billing service that processes data into a standardized billing format). An HIE that has access to your health information because of its role as a data exchange, must follow HIPAA regulations concerning the access, use, disclosure, and confidentiality of your medical records. It must also notify you about how the information will be used.

In addition, HIPAA requires HIEs to have privacy and security policies and procedures in place to safeguard your health information when it is exchanged. These policies and procedures specify who is authorized to access your health information, and that the information must be encrypted. For more information about HIPAA, see PRC’s guide: Health Privacy: HIPAA Basics [5].

In California, the Confidentiality of Medical Information Act (CMIA) also regulates the access, use, and disclosure of individuals’ medical information. It applies to HIEs that exchange information electronically. For more information about California laws that protect the privacy of medical information, see PRC’s guide: Health and Medical Privacy Laws (California Medical Privacy Series) [6].

5. What are the benefits and risks of health information exchange?

Proponents claim that electronic health records and HIE will revolutionize medical practice. Not only will they improve the quality of health care, but they will also increase efficiency and reduce costs. The idea is that once a person’s medical records are electronic and available to every provider he sees, treatment will be better, safer, and more effective because it will be based on the complete record. In addition, overall costs will go down because providers will be able to eliminate redundant diagnostic tests, procedures, and prescriptions—no need to re-invent the wheel.

HIE’s anticipated benefits include:

- improved quality of care;
- reduction in medical errors;
- decrease in redundant or unnecessary services and tests;
- reduced administrative and clinical costs;
- ability to track who accesses medical records, including when and why;
improved monitoring of chronic conditions;
improved public health research, including the ability to detect and prepare for pandemics or bioterrorist events;
increased patient engagement in their care when patients can access their own health information.

It will be some time before we know whether the benefits of electronic health records have been over sold. However, it is clear that HIE will increase the exposure and vulnerability of everyone's medical information by making individual medical information universally available. Medical information is already widely exposed. The healthcare industry's non-standardized and duplicative record-keeping and billing procedures generate multiple records containing personally identifying information in the course of treatment and payment. In addition, third parties and contractors have access to personal medical information in order to perform many non-treatment-related functions on both the provider and payer sides of health care.

When electronic medical records are universally available, the number of locations and people accessing the information will increase. Even with access controls, technical security, and data breach laws and regulations, increased accessibility will increase the risk of medical identity theft and large-scale medical financial fraud. It also increases the likelihood that errors entering a medical record are replicated. Errors may enter a medical record when someone makes data entry mistakes, inadvertently or negligently mixes records, or commits medical identity theft.

**Additional security concerns posed by HIE**

Health care providers will need to address several security issues including encryption, use of personal mobile devices, and cloud storage.

- **Encryption** is an *addressable* security standard under HIPAA. This means covered entities must encrypt protected health information when it “is a reasonable and appropriate safeguard.” [45 CFR § 164.312(a)(2)(iv)]  
When the HIPAA Security Rule was implemented in 2002, encryption was expensive and challenging to use. The result is that many covered entities still do not encrypt their data. With the enormous amount of personal medical information that will be moving around electronically as a result of HIE, the U.S. Department of Health and Human Services (HHS) needs to make encryption a requirement and set standards for its use.

- **Personal mobile devices** like smartphones, tablets and USB drives are ubiquitous. Health care providers often use their own unsecured devices to record and transmit unencrypted work-related health information. The speed with which such devices have been adopted is well ahead of policies that govern their use. According to a number of recent studies, the vulnerability of mobile devices is already playing a significant role in medical data breaches.

At the outset of implementing HIE, one policy that health care providers should consider for all mobile devices, including personal devices, is allowing access to personal health data for viewing but not for download and storage.

- **The cloud**—that is, remote servers where more and more businesses are moving their data—will be essential in an era of electronic health information exchange, if for no other reason than the staggering quantities of data that digitizing the medical records of the entire U.S. population will create.

Health care providers may also want to host their patient portals on cloud-based servers. Patient portals are websites where patients can access their medical records and exchange email with their providers. HIEs may also find it convenient to perform their data search and exchange functions by way of cloud servers.

The vast potential of cloud service for storage and active use of data raises an obvious question: how good is cloud security? Although the cloud sounds like another world, it is digital, electronic, and subject to the usual earth-bound data security problems. A malicious and probably intrusive action, or even an inadvertent one, could cause a data breach. The API, or application programming interface, that defines how a third party connects an application to the service and verifies the authenticity of the third party could be insecure. Denial of service attacks can bring down cloud servers just as they do non-cloud servers.

Health care providers and HIEs considering cloud services need to know the cloud provider’s practices and policies for:

- keeping data from different tenants on the same virtual server separate, unmixed, and inaccessible from each other;
- internal encryption of data and entire systems within the cloud, including management of encryption keys. For example, will cloud service providers require access to their tenants’ encryption keys?
- ensuring the tools are in place for detecting and responding to data breaches;
the physical location of cloud servers and which laws apply. Cloud services are developing more quickly than laws or regulations can address. As a patient you’re unlikely to know where your medical records actually reside. And you’re forced to rely on the security practices of others to protect the privacy of your information.

6. How does health information exchange work?

Health information exchange begins with health care providers of all sizes—from a small practice to a large medical center—buying an electronic medical records system (EMR) to computerize their records. The computerized records are called electronic health records (EHRs).

Once it has electronic records, the provider will likely contract with an HIE so it can exchange medical data with other providers. The HIE does not actually collect or maintain any records. For a basic understanding of how HIE operates, it may help to compare HIE to online air reservation aggregate information from multiple airlines. When you enter a destination and date, the site displays all the available flight information from airlines that participate in its system. Similarly, when your doctor enters your name, and possibly one or two additional identifiers, the HIE Record Locator Service (RLS) checks the Master Patient Index (MPI) of every provider that participates in the HIE. The MPI is a database that has a unique identifier for every patient registered at a health care organization (HCO). It contains a patient’s name, birth date, gender, race, SSN, and address, along with her medical history at that HCO.

Providers who may participate in an HIE include individual physicians, practices of any size, large medical centers, laboratories, imaging centers, and pharmacies, although not all of these entities are involved in the start-up phase. When the RLS finds a match in a provider’s MPI, it transmits the record to the requestor as a read-only file, which can be downloaded or printed. This record is a snapshot in time; that is, it reflects all the information about you that the RLS can find at the time of the request.

The process of exchanging health information assumes that detailed data-sharing agreements among the providers and between the providers and the HIE are all in place. Interim privacy and security standards require encryption of data at rest (in the provider’s servers) and in transmission (between providers, via the HIE), but actual adoption of encryption may be slow to happen.

Another means of sharing records that is independent of an HIE middleman is the personal health record (PHR). You (the patient) control this type of record. A PHR may have a fee or may be free but supported by advertising or sale of your de-identified data. It’s important to note that there is no protection under HIPAA or the CMIA for de-identified data. The business that is de-identifying it need only procure an unmonitored certification that the data is truly de-identified and has had all HIPAA-mandated identification elements removed. 45 CFR § 164.514(b)(2)

The easiest format to use is a web-based PHR, which allows you to request records electronically from your health providers to include in your record. The PHR also lets you send all or parts of your record to other providers online. Before you decide to go this route, it is a good idea to learn about PHRs, including the privacy risks, from a source that is not selling them.

- See PRC’s guide: HIPAA Basics: Medical Privacy in the Electronic Age to learn more about the difference between EHRs and PHRs.
- In addition, see PRC’s Alert: Online Personal Health Records: Are They Healthy for Your Privacy?

7. Who has access to your medical records via HIE?

How can you find out who has accessed your medical records?

Because HIE’s primary purpose is to improve the quality of medical care, your health care providers’ priorities are to gain and allow access to a comprehensive record of your medical history. When the U.S. Department of Health and Human Services (HHS) finalizes its accounting of disclosures rule, providers that maintain EHRs will have to account to you for all disclosures of your personal health information that it makes for purposes of treatment, payment, and business operations for three years prior to the date of your request.

Until HHS’ rule is final, you can get an accounting that goes back six years prior to your request, but this DOES NOT include disclosures for treatment, payment, or business operations. Therefore the disclosures you are currently able to get may seem largely incomplete and irrelevant to the purposes for which you want them.

Read the full text of the Proposed Rule: HIPAA Privacy Rule Accounting of Disclosures Under the HITECH Act published
Can you access your own medical records?

You can access to your records (apart from psychotherapy notes), but you must request them directly from your providers. It is not possible to request your records through an HIE.

However, your doctor should be able to provide you with what’s called a Continuity of Care Record (CCR) after each visit. The CCR is a summary of the most relevant and up-to-date facts about your care and treatment with that provider. A CCR can be helpful for you, and can also provide a current snapshot of your medical status for the next doctor you visit. A CCR may be transmitted either on paper or electronically.

Who else will be able to access your medical records through HIE in the future?

HIEs will be able to transmit medical records required for public health reporting, including immunization registries. HIEs will also transmit data to disease registries, which track the care and health outcomes of patients with a chronic disease or condition, such as coronary artery disease, diabetes, or asthma. Paper registries have done this kind of tracking in the past, but automating record collection through HIE may be more effective.

HIEs can support care management by making it possible to generate patient reports for use at the point of care. It may also be easier to identify patients who are not following a prescribed care regimen or not meeting its goals, and to measure how well providers are delivering recommended care. This all goes along with the government’s goal of shifting the health care payment model from one of fee for service to payment based on outcomes; that is, not just whether you saw a doctor but whether you benefited from seeing her.

The goals of HIE are to improve the quality of care and make delivering it more efficient and cost-effective. Once electronic medical records are available everywhere, for all patients, though, it is inevitable that more people will want access to this data. It is a goldmine for medical research and all kinds of statistical analysis, for example.

It will be important to follow the evolution of HIE and make certain as its uses expand that the focus remains on improving the quality of care for individuals whose records are the raw material of HIE. Others who are not directly involved in patient care and treatment will undoubtedly want this information. Access should be subject to clear restrictions, such as the following:

- statistically certified de-identification of data;
- disclosures of how the data will be used;
- limits on how data may be used;
- and highly specific consent agreements.

8. Is your consent required to electronically exchange your medical information?

Consent to HIE is a matter of individual providers’ policies; it is not currently governed by laws or regulation. The consent models now in use in California are opt-in, opt-out, and multiple choice:

- Opt-out assumes your records can be shared through an HIE unless expressly say no. Even with an opt-out policy mental health and substance abuse records still require specific patient authorization in order to be shared.
- Opt-in requires your consent before your records can be shared.
- One HIE, San Diego Health Connect, offers a choice of opt-in or opt-out. If you opt in you can give full consent (lets a provider access your records during any office or hospital visit) or emergency consent that allows access only during a medical emergency.

Keep in mind that California’s opt-in consent requirement applies only to sharing your medical records electronically. It does not supersede the HIPAA regulations or their presumption of consent for the use of your medical information for purposes of treatment, payment, and routine business operations. For more about consent, see PRC’s guide: How Is Your Medical Information Used and Disclosed (California Medical Privacy Series) [12].

In addition, there are some exceptions to opt-in consent to HIE, including emergency situations—referred to as break the glass—when you (or a representative) are unable to give consent for electronic access to your records. Mandatory public health reporting is another exception. This would include, for example, reporting of staph infections, including MRSA (methicillin-resistant Staphylococcus aureus); communicable diseases [13]; HIV/AIDS [14]; and hospital-acquired infections [15].

California regulations also allow you to revoke HIE consent. The revocation becomes effective on the date it is made, and does
not apply to health information already exchanged prior to revocation.

Opt-in consent to having your medical information shared widely through electronic transmission is a reasonable consumer protection and one that gives you a bit of control over the dissemination of your medical records. The health care industry, which was well represented in the meetings from which the HIE regulations evolved, generally views opt-in consent as a barrier to HIE.

9. Additional resources

CalOHII has been dismantled, and California government sources for HIE information went with it. The Health Information Partners for Tennessee website [16] has five educational videos on the benefits of HIE, viewed from the perspective of health care providers, consumers, and administrators, that explain the process and the reasons for using it clearly. The videos are about 9-12 minutes long. Much of the information in them is repeated in each video, so if you have time for only one, try watching one of these three: Consumers: Access to Care; Providers: either Urgent Care or Virtual Medical Home.

The Office of the National Coordinator of Health Information Technology (ONC) ONC [2] is the division of the U.S. Department of Health and Human Services that oversees the implementation of health information technology, including HIE. You’ll find consumer information here [17].

Originally funded in 2012 with cy pres award from Rodriguez et al. v. NDHealth et al.

Updated in 2017 with funding from the Rose Foundation for Communities and the Environment.


Links
[10] https://www.privacyrights.org/blog/online-personal-health-records-are-they-healthy-your-privacy
[17] https://www.healthit.gov/patients-families