Handling Sensitive Information in an NHIN

*by **Chris Dimick***

The topic of sensitive health data and how to keep it private in the electronic age is one of the most complex issues facing the development of a nationwide, interoperable health information exchange network.

Physicians need accurate medical records to provide adequate care. Yet patients must be assured that their sensitive information—such as substance abuse treatment or HIV status—will remain confidential. Any future network must deliver that assurance if physicians are to expect patients to be forthright about their afflictions and history.

A number of organizations are taking on the issue. One is the National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Privacy and Confidentiality, which has held meetings on the handling of sensitive information in a future national health information network (NHIN). This month the committee plans to recommend to Health and Human Services Secretary Michael Leavitt a framework and principles for how to handle sensitive health data during record exchange.

The challenges of exchanging sensitive information also appear frequently in research conducted through the Health Information Security and Privacy Collaboration (HISPC), a group of 34 state and US territories gathered to discuss problems in, and solutions for, protecting health information in nationwide health information exchange. HISPC's summary report "Privacy and Security Solutions for Interoperable Health Information Exchange" was published in 2007 by the Agency for Healthcare Research and Quality.

Complex Problems

Both the NCVHS subcommittee and the HISPC group agree that protecting information while ensuring proper physician access is a complex problem. As more healthcare facilities implement EHRs, and as the landscape for the NHIN is laid out, the problem will only become more evident.

Sensitive information issues do exist in the paper world, but an electronic system multiplies those issues into a much bigger, national problem, according to Mark Rothstein, JD. Rothstein is the Herbert F. Boehl Chair of Law and Medicine and director of the Institute for Bioethics, Health Policy and Law at the University of Louisville School of Medicine. He also serves as chair of the NCVHS Subcommittee on Privacy and Confidentiality.

A nationwide network will substantially increase the amount of information available for any given healthcare provider. Much of that newly accessible information will be very sensitive in nature, Rothstein says.

Medical records hold a variety of information that can be considered especially sensitive, such as diagnoses of sexually transmitted diseases, mental health problems, and treatment for drug and alcohol abuse. Today, many of those records are protected from disclosure just due to the fragmentation of the healthcare system, Rothstein says. A chiropractor can't instantly access his or her patient's entire medical record electronically. Medical records on a patient lie in unconnected offices.

"Going forward, if [healthcare organizations] are linked, then those same records from all these sources are going to be disclosable to every doctor, nurse, dentist, chiropractor, optometrist, physical therapist, or other healthcare provider that you see in the future," Rothstein says. "A doctor, even, who is treating a woman because she has a sprained ankle, doesn't really need to know that 10 years ago she had an abortion." But without appropriate governance, that information potentially could be accessed in an NHIN simply by obtaining the patient's general medical record.

"I think what we need to do as a system, as we are designing this, is try to find some sort of reasonable way in which we still give the healthcare providers the essential information that they need to provide effective care," Rothstein says, "and at the same time protect some level of privacy in this most sensitive information."

Just What Is Sensitive?

But just what is sensitive information is hard to pin down. A receptionist who is diagnosed with a leg bone fracture probably wouldn't consider that information sensitive, while a professional basketball player hoping to extend a team contract might think differently.

"Every patient has a different understanding of what is sensitive for them," says William Braithwaite, MD, PhD, FACMI, a health information policy consultant who serves on the HISPC technical advisory panel and co-authored the HISPC privacy report. Because of these differences, he believes it will be very difficult to come up with standards for how to protect sensitive information.

Too Much Control?

There are two lines of thought when it comes to protecting sensitive information. Healthcare providers can allow patients the chance to permit or ban disclosure of their entire record over the NHIN, or they can give the consumer some control over what sensitive information they want specially protected from general disclosure.

While Rothstein thinks consumers should have some control, he notes that "line-item control" could lead to records that physicians don't trust. "If you allow the patients to have too much control, then the providers are not going to have any confidence whatsoever in the completeness or integrity of the record," he says. "That is the opposite of the purpose of going to an EHR system."

Members of the NCVHS subcommittee have found it hard to agree on how to protect sensitive information. In November, the subcommittee's draft letter to the HHS secretary was debated at the full NCVHS meeting in order to get some direction for future subcommittee discussions. A final letter will be sent to HHS this month, if the full committee can agree on several differences of opinion, one being whether or not patients should be given the right to restrict certain information from disclosure to a healthcare provider. (The final letter will be posted at www.ncvhs.hhs.gov shortly after it is sent to HHS. Subcommittee discussions on the topic are also available on the site.)

Lack of Standards

But before patients start trying to understand medical disclosure laws, those in healthcare must become experts. The HISPC report notes that healthcare facilities usually cite HIPAA as the reason why they do not disclose health information, even for treatment purposes. HIPAA, however, allows the exchange of health records for treatment, payment, and healthcare operations without patient consent. It is some state and federal laws that heighten protection of certain kinds of information, like substance abuse and HIV/AIDS records.

The HISPC privacy and security report discusses the confusion that varying state laws create when organizations face exchanging information—especially specially protected information—across state lines. Some organizations participating in the study reported that they simply do not transmit health information that requires specific permission for disclosure.

That is not good news for the NHIN, which would rely on complete understanding of the privacy rules in order to operate effectively. More education is needed for the healthcare community about privacy laws, according to the report.

Touchy Subjects

Examples of information that could be considered sensitive include:

- Data about minors
- Reproductive health information
- Communicable disease data
- Sexually transmitted disease, HIV/AIDS data
- Mental health data
- Chemical dependency data

- Genetic information
- Prescription drug information that may lead to disclosure of a sensitive condition
- Abuse and neglect exposure
- Social and family history

Masking the Info

The discrepancies regarding how sensitive information is exchanged between states needs to be resolved before any NHIN can be formed. Technology then needs to catch up. Aside from the debate of whether certain pieces of information should be specially protected, another discussion continues on just how such protection could be achieved.

Masking or blocking out sensitive data in a record and ensuring access by those deemed acceptable is one way to protect information. For example, a woman could set up her record to disclose her reproductive information to her gynecologist only and require consent for other doctors.

But line-item masking can become complicated, since most patients don't always know what information will be vital for their treatment. Take, for example, a man with mild anxiety who is prescribed Valium. He elects to mask mental health information in his record, including prescriptions associated with mental health treatment. After a car accident that injures his back, he is sent to an orthopedic surgeon who administers pain killers without knowing the patient is taking Valium. Complications arise from the drug interaction.

The HISPC report suggests developing an information classification schema that ranks pieces of information based on their sensitivity. However, nit-picking pieces of information for special protection is impossible with the EHRs and healthcare system of today, Braithwaite says. They can label whole records as sensitive or not, but no EHR system can currently pick out sensitive items in documents and mask them for data exchange.

"The information systems currently in existence can't handle the granularity of allowing a patient to say, 'You can release this to this person and not that to that person,'" Braithwaite says.

No Privacy Standards, No NHIN

The NHIN can't exist without strict standards for exchangeing sensitive health data, Rothstein says. "Consumers are going to have a fit if their sensitive information is whizzing around cyberspace without their knowledge, notice, or permission," he notes.

Many of the disclosures that people should be concerned about do not come as the result of hackers or people snooping around computer systems. They come from "compelled authorizations," Rothstein says, which occur 25 million times in the US each year. These authorizations occur when people sign away their right of medical record privacy to get a job or apply for disability insurance. That information potentially can be used to discriminate, Rothstein says.

Though an electronic system makes it easier to obtain information, it could also make it easier to protect sensitive information. EHR systems have the ability to improve privacy since they could, in the future, automatically mask sensitive electronic information.

"We could send life insurers only the stuff that was relevant to someone's mortality risk, instead of sending everything, which includes these sensitive areas," Rothstein says. Only time will tell the EHR's impact on this debate.
"As a privacy person, I view the electronic health record as a possible savior," Rothstein says. "But it also could be the devil in disguise unless we get a handle on it."

Chris Dimick *(chris.dimick@ahima.org) is staff writer at the Journal of AHIMA.*

Article citation:
Dimick, Chris. "Handling Sensitive Information in an NHIN" *Journal of AHIMA* 79, no.2 (February 2008): 58-59;64.