HiBBs
Health Informatics Building Blocks

# LECTURE TRANSCRIPT

## *PRIVACY, CONFIDENTIALITY, AND SECURITY: BASIC CONCEPTS*

**William Hersh, M.D.**



**SLIDE 1**

Welcome to the Health Informatics Building Block on Privacy, Confidentiality and Security. I'm Dr. William Hersh of Oregon Health and Science University.

**SLIDE 2**

In this Health Informatics Building Block we will begin with definitions of the terms related to privacy, confidentiality, and security. We'll discuss some of the concerns that we have as a society for privacy and security of health information. We will then talk about tools for protecting this information and approaches that are used, including those by governments, to protecting health information.

**SLIDE 3**

Let's start with definitions of terms related to privacy, confidentiality, and security. It's important to define these terms and use them properly when we're having a discussion about this overall issue. Privacy is the right to keep something to yourself. That is, I have some information about myself that I do not wish others to have. That's privacy. Confidentiality is the right to keep things about yourself from being disclosed to others. So I may vest confidentiality in a healthcare provider and I expect that that provider will not disclose that information to others. Security in the context of this discussion is the protection of this personal information. There are both policy issues and technology issues related to security. Individually identifiable health information is any health related data that can be correlated with an individual person. Personal health information is a term used in the United States. It is individually identifiable health information as defined by the HIPAA Privacy Rule. Consent in this context is when an individual provides written or verbal permission that allows use of their individually identifiable health information.

**SLIDE 4**

In the next several slides we will discuss concerns about privacy. We'll talk about the tension of personal privacy versus common good. We'll talk about some of the continued disclosures of information that keep taking place. We'll discuss concerns that the public has for privacy and then some issues related to de-identified data.

**SLIDE 5**

There truly is a spectrum of personal privacy versus the use of some personal information for the common good. It's not like the spectrum is from complete nondisclosure all the way to complete unrestricted disclosure, but the spectrum is more related to nondisclosure versus disclosure for the common good. So one end of the spectrum holds that while personal privacy is important, there may be some instances when the common good of society outweighs it, such as in bio surveillance or emerging disease threats. The other end of the spectrum holds that personal privacy trumps all other concerns. One of the individuals most known for representing this point of view is Dr. Deborah Peel. These individuals do have some concerns. There is a somewhat tongue-in-cheek, but worth considering video from the American Civil Liberties union which shows an individual ordering a pizza and that individual being identified and having information about their health available to the person taking the pizza order. More balanced views come from the California Healthcare Foundation and the American College of Physicians which lie more towards the side of the spectrum that says there are some instances where the common good does outweigh complete and absolute privacy. We must recognize that these are matters of opinion and you may have views that fit in somewhere along the spectrum.

**SLIDE 6**

The disclosure of information about patients continues to happen. The concerns are real and they're exacerbated in the Internet era when information can be distributed so quickly and widespread. We've known for years that search engines like Google can pick up patient data that gets put on the Internet, but also can pick up access points to databases and those databases may not be well protected. There are many instances of information being leaked through the loss of computer equipment. One of the most publicized incidents occurred in Portland, Oregon on New Year's Eve in 2005, when an individual left backup disks and tapes in his car and it was broken into and determined that there was data from about 365,000 patients on these disks and tapes. There have been several episodes from the US Veterans Administration -- one of note was a laptop, with data on over 1 million veterans, was stolen. The laptop was recovered and it wasn't clear that the information was accessed, but nonetheless someone had that laptop and the ability to get to that information. These continued breaches have led to the HITECH Act in the United States which invests in electronic health records to require notification when there are 500 or more individuals whose information is leaked. And, in fact, there is a website that has an ongoing list of all of these breaches.

**SLIDE 7**

Another concern is that healthcare organizations are not well prepared for security. Security is not a top priority. There are other competing needs and the implementation of electronic health records is complex and requires many activities such that security might not get the attention that it deserves. A report from

the Deloitte consulting firm noted that data leakage out of the system is a primary threat. Organizations must make identity and access management a top priority. Many clinicians don't want to take the time to login or to use security devices. They want to quickly get to their data because they are busy healthcare providers, but there must be some sort of trade-off where the information receives enough protection. Another concern is the trend towards outsourcing of IT in healthcare organizations and this raises many third-party security concerns -- Who has access to that data? Where does it go? There is increasing need and role for a chief information security officer in healthcare organizations. And in general as the security environment becomes more complex and government regulations continue to grow, security budgets must keep pace with the protection of security even though they all don't already do that. Another report on security came from HIMSS which had a similar conclusion that healthcare organizations are not keeping pace with security threats and the readiness for them.

**SLIDE 8**

Technology and its ease-of-use connects to worsen the problem of security. For example most of us like the convenience of USB or thumb drives that we can plug into our computers to move files around. When these drives are plugged into computers they run a small software program that is on the USB drive. Adam Wright showed that this program can be modified to extract data from the computer without the user knowing it including data in electronic health records. Other concerns come from the widely used productivity applications such as Microsoft Access and Microsoft Excel. There are a number personal health record systems based on Microsoft Access which does have some encryption ability, but is easily compromised. People also often frequently copy data into Microsoft Excel files which of course can easily be spread and are usually not encrypted. Another analysis found that 10% of all hard drives sold by secondhand retailer in Canada had remnants of personal health information that people have stored on them easily accessible.

**SLIDE 9**

What is the role of governments in the protection of privacy? While in the United States and the European Union, various privacy regulations have been developed. In the United States there are the HIPAA regulations. And actually HIPAA includes both the privacy rule and a security role. The privacy rule is more focused on policies and defining when information can or cannot be disclosed with or without the patient's consent. In particular information that is used in the treatment, payment and operations or TPO does not require consent from the patient for disclosure for those purposes. The security rule specifies required protections around security. In the European Union there is European commission directive 9546 EC. This has very stringent rules about data processing allowing it only with the individual's consent or under highly specific circumstances such as legal obligation or public necessity.

**SLIDE 10**

There are many more issues related to medical privacy. One of the most fundamental issues as who

owns medical information. Certainly back in the era of paper charts we always believed that the individual who owns the paper owns the information on it. But as we have growing development of personal health records with patient data distributed in different places, there is a growing view really that the patient owns the information. And this actually has a number of economic implications because sometimes patient data is used for various economic purposes. Another concern is compelled disclosures. Sometimes we are compelled to disclose health related information for nonclinical care reasons. This has the potential to disclose and allow unauthorized access to health-related information. Another concern is the growing advances in the area of genomics. One's DNA, one's genome is probably the ultimate personal identifier that distinguishes a person as an individual. As we'll see in the coming slides even when data is de-identified, it may actually be identifiable and thus can compromise privacy. When we start to look at the genome of a family member we can identify siblings. We can learn things about family members whose authorization for disclosure we don't explicitly receive. And with the growing number of genome-wide association studies that look at genome data and its correlation with clinical data, we may have disclosure of information about individuals from those sorts of studies, especially if the data from them is released into public repositories.

**SLIDE 11**

We often hear that de-identifying data makes it more secure; taking out the information that identifies individuals. Well it turns out we shouldn't be overconfident in this area. One of the experts in this area is Dr. LaTonya Sweeney who has noted for example that 87% of the US population can be uniquely identified by just three pieces of data: a 5 digit zip code, gender, and date of birth. She also undertook a study that used readily available public information sources even though the health-related source was supposedly de-identified to actually identify the medical records of the governor of the state of Massachusetts. She took the health insurance database for state employees which was de-identified and then purchase the voter registration list from the city of Cambridge Massachusetts where the governor lived and by linking zip code, gender, and date of birth was able to identify in the so-called de-identified database who the governor was. As I mentioned in a previous slide, genomic data can aid re-identification of individuals in research studies and some research has shown that Social Security numbers in the United States can be predicted from public data and once an individual's Social Security number is obtained then a great deal more information about them can be obtained as well.

**SLIDE 12**

Here's how Gov. Weld was the identified. Again all name address other obviously identifying information was removed leaving behind a great deal medical information things like ethnicity, visit, dates, diagnosis, procedures, medication, and charges. The database still had in it zip code data, birth, and gender which then from the voter registration database was easily able to be mapped to name and address and that is

how the governor was identified in the health-related database.

**SLIDE 13**

In addition to concerns about privacy are concerns about security of information. We'll see that there are many points of potential leakage of information and of course we'll also note that this is a problem for paper medical records that it doesn't just exist for electronic records. I will also talk about some the consequences of poor security and medical identity theft.

**SLIDE 14**

Healthcare information flows. It's mostly captured in the direct patient care environment, but then it flows to things like support activities of those who pay for healthcare, those who do quality reviews, and sometimes that information even makes it into commercial uses. There are also social uses of information such as insurance eligibility, public health, and medical research. As data flows from one source to another there are, many potential points for it to leak and compromise one's privacy.

**SLIDE 15**

We tend to think of security of medical records only problem for electronic records, but we must step back and think about security for healthcare organizations that still use paper records. The security problems for paper records are just as bad if not worse. For example, most people's records sit on shelves or in carts or lie on the counters of healthcare institutions. We have no idea who's looked at them. You can't have an audit trail of a paper chart like you can with an electronic chart. There's also quite a bit of faxing of medical records that goes on. Fax machines often sit out in easily accessible locations and people can look at the paper that comes out of them. In paper-based healthcare settings we also do a fair amount of photocopying of records. People might move to a new healthcare provider, we may have some requirements from the insurer that data be provided so reimbursement for services can be made, and paper records also get abstracted for a variety of purposes, things like research, quality assurance. Individuals copy data out of the paper record. Paper records as well as electronic records are also used to prevent insurance fraud. In the United States such information flows to the Health Information Bureau, a company that has records on many million Americans and its database is a huge source of information that could potentially compromise one's privacy.

**SLIDE 16**

We've known for many years that the poor security of health information has consequences for patients. Patients may avoid seeking healthcare. They may lie about information. Healthcare providers, if they're concerned that information may fall into the wrong hands, might avoid entering sensitive data or devising workarounds to processes that aim at improving the security of information. A survey from the California healthcare foundation in 2005 found that 13% of consumers admitted to engaging in privacy protected

information that might put their health at risk because the proper information doesn't go into the medical chart; things like asking the doctor to lie about the diagnosis, paying for a test out-of-pocket because they didn't want to submit a claim, and avoiding seeing their regular doctor so that information about the condition they were seeing a doctor about would not go into their regular medical chart.

**SLIDE 17**

There are a number of tools for protecting health information. A nice framework for thinking about these tools comes from a book that is over a decade old now, but it was one of the seminal volumes that led medicine to think more about the privacy and security of health information. So even though the discussion in this book about the specific techniques available is somewhat dated, the framework that it provides is still quite valid and many of the tools it identifies are still important. This report by the Institute of Medicine called *For The Record Protecting Electronic Health Information* was commissioned by the National Library of Medicine. It actually informed the HIPAA legislation in the United States. The report looked at the practices then of six institutions, recommending immediate and future best practices and again, although the content is dated the framework is still quite valuable and thinking about protecting health information.

**SLIDE 18**

The report begins by classifying the various threats to security. It notes that there are threats inside the healthcare organization. There are threats when information flows out of the healthcare organization for mostly legitimate secondary use and then, of course, there is information that is accessed from outside the institution. This report noted back then, and it's probably still the case now, that these latter breaches get a lot of press, but are actually lower in number than particularly insiders who have access to information often for legitimate patient care reasons, but then use that information in inappropriate ways.

**SLIDE 19**

There are many technologies to secure information from the report, many of which are in routine use now. Deterrents don't actually prevent individuals from accessing data, but just remind them, provide a deterrent, that they should only access appropriate information. So alerts when a protected record is entered, such as a hospital employee, and audit trails, the users of electronic health record systems knowing that all data they look at is kept track of so the organization can go back and look and see who has access what. There are many things organizations can do for system management in precaution of information being disclosed so managing software, making sure that the most up-to-date versions are being used, and analyzing vulnerability of the system for outsiders to break into it. There are also obstacles -- everything from authentication, i.e. passwords or other means for people to identify that they are authentically allowed into information resources, authorization, so establishing authorization of who can look at what data, integrity management in the organization making sure that the appropriate people

are looking at the appropriate data and no more. Things like digital signatures required to get in to look at specific data, encryption so protecting data that's transmitted across networks so it can't be intercepted by others, and we'll talk about that more in a moment. Firewalls that keep things like rogue computer programs off of computers. And then rights management a process for deciding who has access to what data

**SLIDE 20**

Encryption is an important part of information security. It's necessary, but it's not the only thing that organizations must do to protect information. Certainly any information that goes over any sort of public network should be encrypted so any information that goes out over the public internet, any health-related information that we want to protect, should be encrypted. The way that encryption works is scrambling of that information so that is not understandable by a human and then unscrambling on the other end so that it can be used by the appropriate users. The scrambling and unscrambling is usually done using some sort of key that works in a mathematical formula to scramble and unscramble information and there is different types of encryption, symmetric and asymmetric. Asymmetric encryption, also called public-key encryption, can be used for things like digital certificates and electronic signatures. There are different trade-offs between the types of encryption that are beyond the scope of this unit.

**SLIDE 21**

The *For The Record Report* also describes a number of best practices for security and it breaks these down into organizational practices and technical practices. Many of these are now done by healthcare organizations. On the organizational side we have things like confidentiality and security, policies and committees, education and training programs, sanctions of individuals when data is accessed inappropriately and allowing patient access to audit trails of their data. On the technical side things like authentication of users and audit trails which all are routinely done. Paying attention to physical security of computer hardware and disaster recovery when things go wrong. Protecting remote access points and external communications is an essential part of best practice. Software distance plan and ongoing system vulnerability are also important practices.

**SLIDE 22**

Let's talk more about authentication and passwords. Authentication is the process of gaining access to a secure computer system. The usual approach to authentication is a password, but secure systems may also add other requirements, like some sort of physical entity. So we talked about authentication being at least what you know, but sometimes what you have. Some of the devices that people have to have that are used in authentication are things like biometric devices, so some characteristic of an individual such as thumbprint or retinal scan, or some physical device, like a smartcard or some other physical key, and so these physical entities of what you have can be paired with the password to provide more protection.

Passwords are growing challenge as we have access to more and more secure systems. The ideal password, of course, is one that you as an individual can remember, but no one else can guess. That can often be challenging. It even gets more complicated with the typical Internet user in this day and age who has many sites for which he or she must use a password. In many organizations including healthcare organizations there is clamoring, appropriately so, for single sign-on so individuals just have to authenticate once. Of course the downside is that if single sign-on is used and someone is able to authenticate to a whole array of systems that potentially compromises privacy and security.

**SLIDE 23**

I like to think of health information security as a trade-off. When we think of the spectrum of security of information we think one end of the spectrum such as public web pages where there's no security, we want everyone to be able to look at them, and then the other end is total security that we often see with government agencies need to protect highly classified information. Healthcare probably fits into some sort of happy medium. That is we do want to protect individuals, but we also don't want to make systems overly difficult for healthcare professionals to use. If we have to go through layers and layers of security, like one does with intelligence agencies, it makes the delivery of healthcare more difficult. It interrupts the workflow. So we have to ideally find some sort of happy medium where information is still rigorously protected, but the ease of access for appropriate users is maintained.

**SLIDE 24**

Let's close this discussion by considering other issues about privacy and confidentiality. There are no right or wrong answers here. There are questions of opinion and personal values and so forth. But just think about these questions – Who, for example, owns health information? How do we best implement informed consent for its use? When does the public good for disclosure of information exceed personal privacy? Does the public good exceed personal privacy for public health? for research? for law enforcement? What conflicts are there with business interests and individual privacy? and How do we let individuals opt out of healthcare information systems? What are the costs of doing so? When do we override this ability? These are all issues to think about for privacy and confidentiality of health information.

**SLIDE 25**