


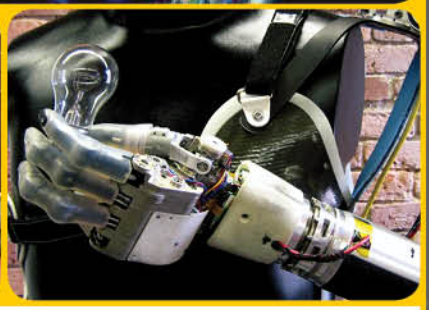

2012 Health Privacy Summit

Synopsis Report

July 2012

U.S.ARMY

TATRC

2012 Health Privacy Summit

Synopsis prepared by

Survivability/Vulnerability Information Analysis Center (SURVIAC)

For the

U.U.S. Army Telemedicine and Advanced Technology Research Center

(TATRC)

July 2012

Table of Contents

Executive Summary

The second International Summit on the Future of Health Privacy ("Health Privacy Summit" or "Summit") was held in Washington D.C. on June 6th and 7th, 2012. The key question: Is there an American Health Privacy Crisis? The resounding message was "yes", we are on the verge of an American Health Privacy Crisis. Opening with the compelling stories of individuals whose privacy has been compromised in the rush to implement electronic health record (EHR) systems, the Summit sought to demonstrate that political and economic gain from technological advances has overtaken a considered and deliberate approach, exposing the critical need for policy and law.

The Department of Defense (DoD) shares concerns with respect to health information privacy generally, and recognizes the need to improve continuity of military medical care. The military medical environment presents unique challenges associated with technical aspects of digital consent, and concerning the management of beneficiary health data. With this in mind, the U.S. Army's Telemedicine and Advanced Technology Center (TATRC) requested a report by the Survivability/Vulnerability Information Analysis Center (SURVIAC) to document findings from the second International Summit on the Future of Health Privacy. This is a synopsis of key discussions and themes that emerged from the Summit; in conclusion, specific opportunities and actions are identified that can be undertaken by the DoD to support information privacy in the context of the Military Health System.

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009 and signed into law on February 17, 2009, is intended to promote the adoption and increased use of HIT by physicians and hospitals. The U.S. government firmly believes in the benefits of using EHR systems and is investing billions of dollars to proliferate their use. Unfortunately, the focus of HIT to date has been primarily to create and advance the electronic exchange of information, with little attention to the need to ensure privacy. Providers observe that many patients are unwilling to provide their full medical histories for fear that the information will be entered into the computer and put at risk.

The Summit raised concern that the overall quality of health care may ultimately be diminished due to loss of trust in health information technology (HIT). Health care providers who attended the Summit reported that they feel caught in a dilemma, forced to follow mandates to adopt EHR systems even as they witness and must explain to their patients the potentially devastating consequences of compromised information privacy. Providers are aware that some patients turn away from necessary and available care based on their fear of EHR systems. For physicians mandated to implement EHRs in the rapidly developing context of HIT, the ethical principle to "do no harm" has become a conundrum. The general consensus at the Summit was that the United States should promptly embrace lessons learned by European countries, recognize privacy as a human right, and re-align our course of action to prioritize information privacy in the development, regulation, and promotion of EHR systems.

Despite the benefits that the Health Insurance Portability and Accountability Act (HIPAA) may provide, the clear consensus at the Summit was that HIPAA is not sufficient to establish the trust that is essential in protecting individually identifiable health information in a health information technology (HIT) environment. Individual privacy that can be compromised in EHR systems does not necessarily constitute a breach of privacy under HIPAA. Moreover, in the rush to implement EHR, patients have not been given an adequate understanding and/or choice about how their health information will be shared. Meta tags and other data segmentation efforts are not yet sufficiently advanced to provide meaningful options for patients who may be willing to share specific data elements in some circumstances.

These and related concerns underscore the need to reset our national strategy with respect to HIT in general, and EHR systems in particular. This presents a potentially valuable opportunity for the DoD to inform the development of national medical privacy policy as a national security priority, and in a manner that recognizes the concerns of military service personnel, veterans, and their families.

Summit Highlights

> *The goal of the Summit is to create the world's premier public forum on health privacy issues by uniting a 'brain trust' of experts – academics, advocates, government, health care, and those in the technology field – who are willing to work together to ensure health privacy is a center-piece of U.S. health care system reforms. We're very pleased with the response to the Summit, from panelists and speakers to sponsors, which no doubt speaks to the importance and urgency of these issues today and into the future.*
>
> *Deborah C. Peel, M.D., Founder and Chairman of Patient Privacy Rights Foundation, May 11, 2011 press release.*

Recognizing privacy as a national security risk, the Department of Defense (DoD) funded the first Health Privacy Summit in 2011. The major issue at that time was the critical need for individuals to understand the flow of information. The lack of a clear "chain of custody" or data flow analyses created concern with the development of EHR systems.

One year later, the 2012 Health Privacy Summit focused on individual patient privacy as critical to the successful adoption of EHR systems. Summit participants came from a wide range of backgrounds, including providers, attorneys, vendors, government agency officials, consultants, academicians, and researchers. The atmosphere of the Summit promoted healthy and interactive dialogue by addressing current challenges and critical needs for the successful development and meaningful use of EHR systems. The Summit provided panel discussions and specialized breakout sessions aimed at addressing the critical privacy issues shared by patients who have been victimized through the current use of EHR systems. Discussions included highlights from European privacy efforts and overviews of innovative technologies designed to protect the privacy and security of health data. Overall, the Summit was dynamic, interactive, and motivational. It raised insightful questions and considerations in an effort to pave the way for health information technology (HIT) in the years ahead.

SUMMIT CONCEPTS AND THEMES

- Trust and Transparency
- Technology is Moving Faster than Policies and Laws
- Stakes are High with EHRs and Privacy – Risk of Irreparable Damage
- Privacy by Design, as Opposed to Technology by Design
- Consumer Education
- Big Data and Disclosures

Main Discussions and Themes

The 2012 Summit was opened by keynote speaker Dr. Farzad Mostashari, who serves as National Coordinator for Health Information Technology within the Office of the National Coordination (ONC) at the U.S. Department of Health and Human Services. Dr. Mostashari established the focus of Summit discussions with his address entitled, *Creating a Culture of Privacy and Security Awareness*. Privacy is an American value; this was true in 1977 in the United States Supreme Court case of

Whalen v. Rowe, and it is still true today. Unfortunately, privacy has not been identified as a priority in the urgency to advance HIT.

The ONC recognizes the critical need for patient-centered considerations through privacy policy, technology, and culture. ONC's Office of the Chief Medical Officer and Office of Consumer eHealth have identified three A's for focusing their efforts: Access, Attitudes, and Actions. All consumers, including patients and providers, need *access* to health information to ensure proper and comprehensive care. *Attitudes* toward healthcare and HIT need to change; patients need to be empowered to ask questions and to participate in their care, while providers need to be confident in the care they provide without fear of law suits. *Actions* are necessary to ensure the security and protection of information as it is uploaded, downloaded, and transferred among electronic systems.

Four general sessions highlighted several key concepts and themes for the successful development and expansion of EHR systems:

- "First Do No Harm. Does Technology Harm Patients?"
- "Is There Too Much or Too Little Regulation? Will States or Congress Regulate?"
- "Docs and EHRs. How is the Physician-Patient Relationship Affected?"
- "Big Data – Finding the Healthy Balance Between More Information and More Risks"

Trust and Transparency

There is a sacred bond of trust between patients and their health care providers. It is this trust that can be leveraged for the successful development and expansion of EHR systems. Providers are more likely to adopt and make meaningful use of EHR systems that they trust, and likewise they will encourage patients to embrace the use of trusted EHR systems. However, trust depends on the assurance of privacy. Summit speakers cautioned Americans against trading off privacy to accommodate the push for efficiency and expediency afforded by EHR systems. Although EHR systems can and do offer tremendous value in the promise of improved and enhanced quality care, loss of privacy can cause long- term quality of care to diminish. Patients who fear the loss of their privacy may stop trusting their health care providers and turn away from the health care system entirely.

ELECTRONIC HEALTH RECORDS
WHY WE NEED THEM

- Efficiency and Expediency
- Complete Medical History
- Streamline Health Care for Geographically Dispersed and Isolated Areas
- Instant Access to Medical Information, especially in an Emergency
- Significantly Improved Quality of Care
- Enhancing Research and Moving Science and Medicine Forward
- Increased Patient Knowledge and Empowerment

Transparency promotes trust. Patients want to know how their health information will be used; providers should be able to answer this question clearly and correctly, with confidence that patients' health information is protected from misuse. As transparency fosters trust in HIT generally, EHR systems can expand more successfully toward the goal of enhanced health care through improved efficiency and expediency, instant access to complete medical histories,

delivery of care to patients in isolated areas, the advancement of medical science, and improved patient education.

Technology is Moving Faster than Policies and Laws

Joy Pritts, Chief Privacy Officer for ONC, emphasized that technology is developing faster than laws and policy can be written to safeguard patients. The health care market is not prepared to keep up with the pace of EHR technology because standards have not yet been developed for its use. EHR systems are tools that have the potential to play a powerful and positive role in healthcare, but appropriate laws, policies, and safeguards are critical in order to protect the essential interests of all stakeholders.

The time-consuming process of creating effective and relevant laws and policies is particularly challenging in the continually advancing world of HIT. Several speakers at the Summit argued that HIPAA, and in particular the HIPAA Privacy Rule, is inadequate to withstand the challenges created by HIT. The focus of HIPAA has been on compliance and breaches, missing the bigger issue of the harm created by data loss, unnecessary data sharing, and identity theft. The HIPAA Privacy Rule does not define individual privacy. Moreover, HIPAA allows for uses and disclosures of health information for purposes of treatment, payment, and health care operations (TPO) without patient consent or knowledge and without being subject to HIPAA's minimum necessary standard. "HIPAA Privacy" is at risk of becoming an oxymoron as we face the challenges associated with promoting and expanding EHR systems.

Although it is certainly possible to write patient-centric privacy policies and laws to regulate HIT, this has not yet been achieved. Unfortunately, EHR systems are being adopted without regulation and guidance. There is concern that the current adoption of EHR systems in an effort to keep up with the fast pace of HIT may jeopardize trust in the healthcare system overall. Although the development of effective privacy policies are slow, it is important to consider that when such policies are finally in place, they can be used to encourage public acceptance (trust) and thus support the ultimate success of EHR systems in health care.

The Stakes are High with EHRs and Privacy – Risk of Irreparable Damage

"Electronic technology is a game changer," said James Pyles, co-founder and principal of the law firm of Powers, Pyles, Sutter & Verville, PC. This statement appeared to have a powerful impact on Summit attendees after hearing testimonials of patients whose individually identifiable health information had been compromised through the use of EHR systems. Technology has outpaced policy and the law; the potential privacy implications are alarming. Unlike paper records, electronic records cannot be physically retrieved. In the absence of legal and policy protections, electronic health data can be misused causing irreparable damage.

ELECTRONIC HEALTH RECORDS
WHY WE FEAR THEM

- Snooping/Unauthorized Access
- Criminal Misuse
- Data Loss
- Secondary Uses
- Medical Identity Theft
- Potential to Destroy Quality of Life
- Life-threatening Consequences

In addition to the risks that intimate health data can be lost or shared inappropriately, electronic data creates a

potential currency for fraud. Data in EHRs systems can be used to commit identity theft and are vulnerable to other forms of organized criminal misuse. Such data are potentially valuable for false income tax returns, fraudulent use of medical insurance, fraudulent claims for treatment that was not actually performed, and wrongful billing. Unlike financial data, no single agency controls the use or investigates the abuse of health data. Individuals most vulnerable to abuse of health data are the deceased, children, HIV patients, the elderly, the desolate, and patients receiving long-term care. Military patients express added concern about the global sharing of their identifying health information.

Privacy by Design, as Opposed to Technology by Design

"Privacy by Design" is a patient centric concept that is gaining momentum in HIT to help address the current challenges of EHR systems. The premise here is that technology should be used to facilitate a process, not create it. The current national strategy is to incentivize use of iEHR systems through meaningful use requirements; this approach is based on a framework that starts with the end in mind (improving patient health) and works backwards from available technology. By contrast, Privacy by Design recognizes the need to work forward from privacy as a critical objective for the utilization of technology. The long-term success of EHR systems depends on providers embracing meaningful use not for incentives, but because they truly believe in EHR systems and can trust them, passing that sincere belief to their patients. By this approach, meaningful use requirements for providers should be coupled with meaningful choices by patients. Data flows should be mapped using a model with defined controls and building a methodology that is based on meaningful choices to be made by individual patients.

Basic opt-in and opt-out models are simplistic, after-the-fact attempts to layer privacy on technology. As such, they are inadequate to support meaningful choice. Better potential for meaningful choice rests with the use of meta tags, which can be used to provide a viable means of protecting sensitive data by segmenting designated data elements. Meta data tagging involves coding specific entries of a patient's health record to allow for more control over sensitive data. However, meta tags are neither perfect nor widely used because there are no currently recognized standards for tagging. Tagging also raises a difficult challenge when trying to account for the vast individual differences in the levels and amounts of identifying information patients are willing to share in various circumstances. Tagging data and interpreting those tags in a uniform and consistent manner is a complicated process, but it is an essential objective in Privacy by Design.

CULTURAL PERSPECTIVES ON RELIGION AND PRIVACY

- A Muslim nurse, Jewish Rabbi, and Catholic Academician presented their views on privacy based on their religious faith and heritage
- What makes a person a person is free will, and if you take that away, you take away humanism
- Privacy is of critical importance to the individual; it is part of the heart and soul of individuals, that which makes us human

Consumer Education

In addition to developing patient-centered policies and laws and building privacy directly into HIT, the future success of EHR systems also depends on consumer education. This includes education for all stakeholders, including providers, patients, those who collect and maintain data, and those who maintain and/or manage EHR systems. Comprehensive education is an enormous challenge, particularly because most people currently have inadequate information about potential threats to privacy in general.

More education is critical, not only concerning the use and value of EHR systems, but also to promote the need for meaningful choice and how it can be built into HIT as technology moves forward. Ideally, EHRs should be presented not only as a means of improving the quality of care and scientific/medical research, but also as a means to empower patients through greater knowledge about their health information and meaningful choices in protecting their privacy. Training should include information about how policies, law, and technology are applied to protect privacy. It should also communicate the transparency of EHR systems in order help build trust and overcome the current barriers that prevent their successful expansion.

It is a challenge to educate multiple audiences in a balanced way. Vulnerable populations may not wish to give consent because they have never before been asked for it. A presumption that must be overcome is that it may be too difficult to explain primary and secondary uses of information to multiple audiences. However, with education and new understanding, many patients will likely agree to both primary and secondary uses of health information once they are given meaningful choice in a trustworthy and transparent EHR system.

Big Data and Disclosures

A wealth of learning can be obtained from large providers such as the Mayo Clinic and Kaiser, as well as from large integrated delivery networks. Proponents of big data are excited over the

mass of data that can be made available through EHR systems. These data can be used to study associations and test hypotheses to improve medical science and the quality of healthcare. Big data are also considered essential for serving aging populations and geographically dispersed patients.

Although there is validity to the value of big data, there are currently no regulations in place to control data mining as relates to patient privacy. The value of big data will remain limited and risky as long as EHR systems are unregulated and patients are not given an understanding and meaningful choice concerning the use of their electronic health information.

There are also concerns about the proper scientific use of such data. There is a tendency for researchers and providers to request more data than may be necessary or appropriate. This raises the issue of large "dirty" data sets versus marginal structured data sets, and results in increased risks to privacy. In EHR systems, free text fields are not regulated and the process for de-identification of this information is not fool-proof. These considerations should be addressed in the development of patient centric policies and laws and in the advancement of technology.

European Trends

Since World War II, health privacy has been recognized as a human right in Europe. Relative to the United States, Europe is more advanced in HIT; European programs are smaller, more homogeneous, and more simplistic. Factors that drive centralization are greater in Europe than in the United States. By comparison, programs in the United States are larger, more diverse and fragmented. The larger the scale of EHR sharing, the greater are the potential risks to privacy. There are, however, valuable lessons learned from Europe that can be considered to inform the development of privacy standards in the United States. (See Table 1, below.) Generally, electronic health records in Europe are more advanced, and therefore, problems have become more evident there.

Table 1: Sampling of Privacy Cases from Europe by Country

Country	Design and Impact
Iceland	▪ Centralized EHR used to research genetics; ▪ Records to be 'de-identified' by encrypting the social security number, but would be linked to genetic, family data ▪ Patients in Iceland objected Argument was for de-identification, but , in practice, it was easy to re-identify ▪ The court ruled that patients must have the ability to opt-in. The project died
Finland	▪ European law based on s8 ECHR right to privacy, clarified in the I v Finland case ▪ A nurse in the hospital was HIV positive; All employees could see her patient records ▪ Court said that the hospital had a duty to restrict information to providers ▪ Human Rights Law

	▪ Not a consent law, rather a Health Privacy Veto Law ▪ The right to restrict personal health information to the clinicians providing care
United Kingdom	▪ Centralized EHR system: replace all IT systems with standard ones over ten years, giving access to information to everyone with a "need to know" ▪ Providers had professional autonomy ▪ Project was a disaster; lack of focus resulted in billions wasted ▪ Multiple problems and issues o Move from servers to hosted systems 100 miles away o Focus on money versus patient care ▪ Opt-out disaster ▪ 5 million records in 1 database, no penalty to punish wrong-doers
Netherlands	▪ System proposed in 2010 for national electronic patient record to allow data transmission between care providers ▪ Electronic health interchange, centralized system, e.g. HIEs[1] and RHIOs[2]Problem: staff at the center were given read access to everything (pull model, not push) ▪ Uniformity enabled centralization ▪ Campaigners have persuaded the Senate to block the system

As in many European countries, consent rules in the United States are controversial and often confusing. Guidelines must be formulated to determine whether consent is needed, the breadth of that consent, and the choices to opt-out, especially in relation to research. If a Veto Law is enacted, patients would be identified as opt-in by default, unless they specifically veto a particular use or disclosure. This approach would force developers and providers alike to consider the risks inherent in their program designs.

As we develop systems and services in the United States, we need to consider problems encountered in Europe. The "National Programme for IT" was introduced in 2002 as part of the National Health System (NHS). The program was a colossal failure; billions were spent, suppliers dropped out, and the resulting software did not work. A Summary Care Record (SCR) was introduced as part of this initiative to make medication and allergy information available to emergency or unscheduled providers. The Scottish version of this software leaked the records of politicians, sport stars, and other notable personalities. When the public was surveyed on a central records database, most adults reported they did not want wide information sharing or the use of their records for research without their knowledge or consent.

These issues changed the United Kingdom's approach to electronic records. The children's' database -- designed to share data between health care providers, schools, probation agencies and social workers -- was replaced by a targeted child-protection system. Despite this victory, secondary issues have been raised as a potential risk to privacy. As part of a larger 'open data'

[1] Health Information Exchanges
[2] Regional Health Information Exchanges

initiative on public-sector data, a new policy has been drafted to make “anonymised’ data available to academic and commercial researchers (Royal Society report due June 21). Anonymised data are thus still data at risk.

The United States has a valuable opportunity to learn and benefit from the experiences and challenges faced by other countries, and to avoid repeating their mistakes. While there are many factors that favor centralized records, these same factors also favor higher risks. The United States has many additional risks and policies to examine before it can successfully promote EHR systems and/or universal EHRs. EHR systems are vulnerable to technical as well as political attack. As a fundamental premise, Americans need to learn from Europe that the successful development and expansion of EHR systems depends on putting patient privacy and education at the forefront of HIT design, policy, and law.

Best Privacy Technologies of 2012

Innovative capabilities for privacy and security were recognized at the Summit for their achievements in providing the best privacy technologies of 2012. Awards were giving to:

- Jericho Systems for enabling patient privacy controls, including meaningful consent, and encouraging patient choice as well as allowing the patient to control all requests
- Trend Micro Deep Security, a global cloud security leader, for leveraging technology without compromising privacy
- RADAR, ID Experts for minimizing harm when breaches occur and accelerating breach response and patient notice

Work Groups

During the Summit, participants were encouraged to identify problems and concerns and to collaborate on potential solutions. They were also invited to participate in work groups where members from various professions gathered to brainstorm and act upon the issues presented. Three work groups have been formed, covering the three key areas that need to be addressed in the success of EHR systems: Principles, Technology, and Consumer Education (Outreach).

Principles Work Group

Findings of the Principles Work Group included the observation that the HIPAA Privacy Rule is outdated and unable to withstand the challenges of advanced HIT. Covered entities under HIPAA are held to a federal "floor", setting baseline minimum privacy and security standards. Although covered entities have the option to require greater protections and individual rights than the law provides, they are hard pressed to do so, in that they will increase their risk to liability.

ESSENTIAL PRINCIPLES FOR A CONSUMER HEALTH PRIVACY BILL OF RIGHTS

- Individual control
- Transparency
- Respect for Context
- Security
- Access & Accuracy
- Focused Collection
- Accountability
- Applicability
- Enforcement

The current health privacy crisis is due to the fact that HIT is a "game changer". There are millions of reported breaches, not to mention unreported data losses causing harm that are not otherwise considered breaches under HIPAA. In a matter of seconds, millions of patients can be harmed. Unlike paper records, data loss within EHR systems can occur instantaneously, making it impossible for patients to recover or restore their health privacy. The Privacy Rights Clearinghouse (www.privacyrights.org) has documented more than 22 million medical/health information privacy breaches since 2005. It is little wonder that 60% of the American public lacks confidence in the confidentiality of electronic medical records (Helman, Greenwald, & Fronstin, 2008). Many states have enacted data breach notification laws in response to public concern, but these laws do nothing to prevent data privacy breaches.

The Principles Work Group is currently focused on creating a business case for and drafting a "Consumer Health Privacy Bill of Rights". These efforts are on the heels of action by the White House, on February 23, 2012, issuing a Consumer Privacy Bill of Rights "without delay" based on privacy principles recognized internationally in Europe and Asia. The purpose of the Consumer Privacy Bill of Rights is to "provide a baseline of clear protections for consumers and greater certainty for companies" with respect to the collection and use of electronic data about individuals, which is "essential" for the trust necessary for obtaining public acceptance of networked technologies. However, to avoid interference with HIPAA, the Consumer Privacy Bill of Rights *specifically exempted health care*. The Policy Work Group is seeking to lobby for the issuance of a Consumer Health Privacy Bill of Rights "without delay", building from the same principles determined to be essential for developing trust and acceptance of electronic technology in other markets.

Technology Work Group

Technology works in the manner in which it is designed. Privacy problems presented by EHR systems are not due to limitations of technology itself, but rather to the wide range and number of EHR systems developed and how they are implemented in the health care system without adequate requirements for privacy protection. Ironically, one of the original goals of HIPAA was to standardize transaction code sets, yet there is no federal standardization of EHR systems. To date, EHR systems are implemented at the state or provider level, resulting in a "fractured state of understanding EHRs."

TECHNOLOGY WORK GROUP'S LIST OF NECESSARY ACTIONS AND AWARENESS FOR HIT ADVANCEMENT

- Identify Current Technological Solutions for EHR Systems
- Coordinate Efforts by Agreeing on Action Items and Available Experts Aligned to Support Each Action
- Central Messaging
- Socialize Progress Made for Building Privacy into Technologies and Work Toward Standardized Goals for EHR Systems
- Build Awareness with ONC and Policy Makers

In addressing the current HIT challenges, the Technology Work Group recognizes the need to bring together a collaborative group of expert volunteers to set and define goals and determine the best options for data segmentation. These needs raise further fundamental needs for funding and engineering. In addition to focusing on technological solutions, the Technology Work Group also recognizes the need to work in tandem with policy makers. As it currently stands, private industry and federal agencies are independently driving EHR systems, and there is no clear standard for where innovation should begin or how it should proceed. Technology and policy experts need to work together and agree upon the initiatives, actions, and directions that each can take in support of the other, with the mutual long term goal of successfully designing privacy into EHR systems and promoting their success.

Consumer Education/Outreach Work Group

The challenge of consumer education for the purpose of promoting understanding and use of EHR systems is two-fold:

(1) The target audience is a diverse population; they have diverse needs and an inconsistent understanding of the issues at hand.
(2) Existing policies and laws are too general and too vague to adequately regulate and standardize EHR systems. It is difficult to determine where and how to begin an awareness campaign or where such a campaign would make the biggest impact.

While most people have at least heard of HIPAA, few fully understand it and even fewer understand how HIPAA standards are implemented. Now, almost a decade after enforcement of the HIPAA Privacy Rule, confusion remains and individuals are wrongfully denied access to their medical records. This problem is compounded by a lack of privacy policy and law and by the need for privacy by design within

electronic technology. As the demand for technology and instant access continues to grow, privacy breaches, unauthorized use, and data loss/misuse continue to escalate with even more damaging and devastating consequences. Those who are least informed -- the poor, underinsured, and uninsured -- are the most vulnerable. Consumer education is critical, but it is difficult to know where and how to begin due to the complexity of current challenges.

CONSUMER EDUCATION WORK GROUP ACTION PLANNING

- Who is the audience?
- What is the message?
- What doesn't the audience know that they should know?
- How do we educate on the benefits of EHR systems versus the potential and realistic consequences?
- What is the best media for each audience?

In working to identify a plan of action, the Consumer Education Work Group identified many considerations. Education and outreach efforts will need to reach many different stakeholders, including providers, patients at varying educational levels, insurers, regulators, technology experts working with EHR systems, and many others. Different types of campaigns will be required, supported by clear, basic messaging. The benefits and risks of EHR systems will need to be clearly conveyed, as well as the likelihood of risks and what protections can be taken to avoid and mitigate risks. Different and varying types of media must also be considered for each campaign and audience, including considerations as to social media, broadcast media, focus groups, and small face-to-face classes. Collectively, informed and knowledgeable stakeholders can guide the success and further the successful promotion of EHR systems.

Specific Topic Sessions

The Summit further offered five specific issue breakout sessions that were repeated twice during the afternoon of the second day, enabling each attendee to participate in two sessions of greatest interest to them.

"How do Ideal Patient-Centered, Ethically Based Health IT Systems Address Privacy?"

On the surface, it appears easy to define the requirements for EHR systems. The system should be accessible for every provider who serves an individual patient. Patient records should be stored electronically. Electronic records should allow a provider to garner the information they need to treat the patient effectively. For any additional access, patient consent should be required in order to permit access.

A "one size fits all" approach to EHR systems, however, does not allow for differentiation between records or between types of data and does not recognize that some types of data have different requirements for use and disclosure. For example, mental health and substance abuse records should not be combined with general health records. Furthermore, providers do not always need to have access to the full record.

Access and "need to know" guidelines should be the basis for a complex EHR model. An EHR should have multiple sections with multiple access levels depending on need to know. Some hard questions should be asked: Who needs to know the information contained in the record? Should every provider have access to every section of the record? What are the secondary

uses of the record (payment, research, administration, etc.)? And, is it feasible or practical to have more than one type of EHR for every patient? Furthermore, different patients will feel differently in terms of consenting to various types of disclosures and the data elements that can be disclosed in various instances.

Under HIPAA, the clinical use of an EHR is not difficult to understand or design in light of the fact that HIPAA allows for uses and disclosures of individually identifiable health information for TPO purposes without patient knowledge, consent, or authorization. If the record contains mental, behavioral health, or other highly sensitive information, additional access rights should be implemented for those sections, while other sections, most notably laboratory and pharmaceutical information, are routinely made available for all providers.

There are, however, ethical issues that should impact EHR systems development when considering secondary uses of a record. Although not mandated under HIPAA, several providers require a patient to consent to records being sent to health insurance companies for payment purposes. Health insurance companies are also regulated by HIPAA in protecting the records, but they have other reasons for wanting to use health records in their possession in order to monitor and control overall health care costs. Lobbyists and other special interest groups also seek access to health data. Researchers claim they would benefit from full access to the big health data, but this benefit is frequently overstated. Not all research is good, and it is important to avoid the practice of "stalking" data records to gain other information for alternatives uses.

A PROPOSAL FOR AN IDEAL ETHICAL EHR

- Allow access to appropriate providers
- Create mechanisms to aggregate data for secondary use, especially research
- Allow for the patient to veto any part of the record
- Coordinate maintenance of the EHR between the individual patient and the designated provider

Ideally and ethically, EHR systems should focus first and foremost on the patient and his or her privacy concerns. This approach will necessitate the development and implementation of some complicated technology architecture to protect different parts and different data elements in different ways. It will also require thoughtful policy to provide useful guidance and regulate the use of the EHR systems. These are the objectives of patient-centered privacy by design.

"Health Information Privacy & Health IT – Where Are We Going and How Did We Get There?"

As early as 1890, Louis Brandeis (later a Supreme Court Justice) co-authorized a Harvard Law Review article, entitled "The Right to Privacy." He defined privacy as "the right to be left alone," which has become a well-known premise.

Privacy is not defined in the HIPAA Privacy Rule, and it is not the central focus of HIPAA or the HITECH Act. HIPAA permits multiple uses and disclosures of a patient's health information without patient consent or knowledge. Furthermore, HIPAA does not restrict disclosures and uses of health information for TPO purposes to a minimally necessary standard, which potentially places significant amounts of patient health information at risk of inappropriate exposure and loss. HIPAA is not equipped to regulate EHR systems.

In 2009, the U.S. government set aside $20 billion in stimulus funds for incentives and penalties to encourage health care providers (hospitals and physicians) to adopt EHR systems. When medical data are breached, however, the incalculable additional cost is weakened public trust in the very patient-provider relationship that is so essential to effective care, and to the adoption and expansion of the EHR systems that are intended to enhance quality of health care overall. In a 2012 study by the Ponemon Institute, 83% of respondents felt organizations that fail to protect their personal information are untrustworthy (2012 Consumer Study, 2012).

RECOGNIZING PRIVACY AS A VALUE IN HIT STATEMENT BY PRESIDENT BARACK OBAMA

One thing should be clear, even though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion that privacy is an outmoded value. It has been at the heart of our democracy from its inception, and we need it now more than ever.

"Consumer Data Privacy In A Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," White House, February 2012

"HIEs: What We Know and Don't Know, Data Segmentation & Patient-Centered Options"

As we face the potential enormity of privacy breaches in HIT, many patients justifiably fear that they may be stigmatized or otherwise compromised by misuse of their electronic health information. This fear can create a barrier to care. The only way to address this problem is through data segmentation and patient-centered design. To date, the primary focus of EHR development has been on how to design systems to communicate with each other. These systems have not been developed so that the pulling and pushing of data across the health information exchange (HIE) is in accordance with patient consent. What we do not know is how to effectively offer and obtain meaningful consent. Now is the critical time and opportunity to address this problem, and to reconsider current laws and create policy that can regulate the use of EHR systems accordingly.

"Is Genetic Privacy Threatened?"

It is important to recognize that genetic privacy is different than health privacy. Currently, there are genetic privacy concerns pertaining to bio banks, genetics research, forensic DNA databases, consumer based genetic testing, newborn screening, and surreptitious testing. With an increase in the number of genetic testing companies, the problem is compounded in that companies are accepting genetic information without consent. Genetic information is also being offered to employers when they are not otherwise requesting the information.

More awareness and education are needed to protect genetic privacy. This session set forth an overview of current law, its implications, and the increased visibility and understanding that is needed to protect genetic information.

The Genetic Information Nondiscrimination Act (GINA) was introduced in 1995, and passed and signed into law in 2008. It specifically addresses the protection of genetic information, including family health information of all kinds. GINA protects individuals from the misuse of genetic information by health insurers and employers. There are six narrow exceptions regarding employment discrimination under GINA**:**

- Inadvertently obtaining genetic information through casual conversation with employees or similar means (“water cooler” exception)
- Offering qualifying health or genetic services, including such services offered as part of a voluntary wellness program
- Acquiring genetic information for use in the genetic monitoring of the biological effects of toxic substances in the workplace
- Requesting family medical history to comply with the certification provisions of the Family and Medical Leave Act (”FMLA”) or state or local family and medical leave laws
- Acquiring genetic information from documents that are commercially and publicly available; however, an employer may not research medical databases or court records for the purpose of obtaining genetic information about an individual
- Conducting DNA analysis for law enforcement purposes that require genetic information of its employees, apprentices, or trainees for quality control purposes to detect sample contamination

Exceptions also exist regarding employer disclosure of genetic information under GINA and regarding health insurer discrimination under GINA. Use and disclosure of genetic information by health insurers is further regulated by HIPAA.

GINA does not pre-empt state law; 48 states have prohibitions against genetic discrimination in health insurance laws. However, state laws are generally more limited in scope than GINA. State laws may offer a larger potential recovery, but they are also limited by other civil rights statutory limits.

The greatest challenge is not with regard to the limitations of or exceptions to GINA, but rather the fact that consumers, including patients, providers, and research reviewers alike, do not know about GINA. Most people are not aware GINA privacy protections exist; there is no general education program to promote awareness. With the development and expansion of EHR systems, consumers especially need to know that there are laws in place to protect their genetic information. This type of consumer awareness will build consumer confidence in the benefits of genetic research.

Genetic research promises to improve patient health and decrease human suffering; it will likely drive the future of patient care. Studies conducted on genomes to date have reduced the cost of a single genome from three billion dollars 15 years ago, to an average of ten thousand dollars today, and it is anticipated that the cost will continue to be reduced with further studies. However, there is great risk when studies are not appropriately identified as providing or leading to genetic testing. Institutional Review Boards (IRBs) conduct ethical reviews of proposed research under the Federal Policy for the Protection of Human Subjects. However, IRB members may not be trained in how to identify genetic testing or how to protect genetic privacy. The benefits of genetic testing/research are huge, but as with EHR systems, we risk losing trust in promoting and expanding genetic research where genetic privacy is not understood and built into HIT systems. Awareness campaigns are needed in which clear, standard language is used to build consumer awareness and confidence, such that provider-patient relationships can be further leveraged and trust can be built to endorse the core tenets established in GINA.

"How do Social Media, Mobile Devices, Medical Devices, and Implants, Online 'Health Websites,' and Clouds Threaten Health Privacy?"

Social media has become a way of life. Social media, medical devices, implants, websites, and cloud computing are potentially useful to patient education and care, but by their very nature these tools are also vulnerable to misuse. While they afford users convenience and instant information, they also present potentially enormous privacy risks.

"Digital gaps" and "dumb systems" (systems that do not communicate effectively with one another) create additional risks. Existing regulation applies in sectors; when data crosses over into another or multiples sectors, it increases privacy risks. Mobile devices present the opportunity to track user-entered information and everything a user does with that information. Medical devices can capture information for use in unanticipated ways. For example, disease and toxicology screenings may unknowingly be applied to a blood test, and an implant for monitoring blood pressure may be used to track a patient's whereabouts. In general, consumers are not well-informed about cyber security risks. Younger populations may be especially casual in their willingness to place personally identifiable information, including health information, on the internet. Cloud storage and cloud computing present additional risks to information privacy. Digital forensics cannot be applied to a cloud system to identify the culprit or cause when a breach occurs or information is wrongfully shared.

All of these developments in electronic technology bring great promise for efficiency and expediency, but they also present significant risk to privacy and potentially irreparable harm to individuals. This is a collective action problem, in that policymakers, technology developers, and educators alike need to work together to address the problem with a patient-centered privacy focus. Transparency of data mapping is critical to establish trust; patients and providers alike should know where their health data are, where they are going, and how they can and will be used.

Creating privacy by design is a process that requires multidisciplinary experts. Government is an important participant in this process, but is not the single answer. An open line of communication needs to be built between vendors and technology developers, providers and patients, policy makers and others. All stakeholders need to be explicitly included in the process of creating solutions.

Conclusions and Recommendations

A recent poll by the U.S. Centers for Disease Control found that as of 2011, 55 percent of U.S. doctors had adopted an electronic health record system as part of their routine practice (Mozes, 2012). However, current EHR technology does not adequately protect the confidentiality and privacy of medical and health information (see also Win, 2005). HIT systems now make it possible to breach the medical privacy of millions of patients in an instant without physical access. Threats and vulnerabilities stemming from inadvertent loss to malicious criminal activity are well-documented (Johnson, 2009; Johnson & Willey, 2010) and can have potentially devastating consequences for patients and their families. Recent incidents reported by the media include a 2011 breach that left millions of military TRICARE insurance patients vulnerable

after a Pentagon contractor left computer tapes containing private medical data in the back seat of her car.

Based on the themes and discussions emerging from the Summit, SURVIAC offers the following recommendations for consideration by TATRC:

- Participate in writing policy and law for the regulation of EHR systems that recognize the unique concerns of military beneficiaries and veterans
    - Review and contribute to the draft Consumer Health Privacy Bill of Rights and participate in the Policy Work Group to assist in creating health privacy law and policy
    - Utilize work on the Virtual Lifetime Electronic Record and iEHR initiatives as well as participation in the Nationwide Health Information Network as platforms in drafting policy and creating meaningful choice for military patients
    - Identify lessons learned, costs and benefits of military health systems to inform the development of privacy policy as a national security priority
- Ensure that patient privacy and legal experts within DoD are identified and involved early on in the process and have an active voice in the design of electronic technology. Further ensure that these experts are actively engaged in the workings of the Interagency Program Office and are able to develop and effectively communicate DoD's position on critical privacy issues and can collaborate and consider similar and/or alternative positions offered by Veterans Affairs
- Consider projects that focus on meta data tags and a system for the uniform and consistent interpretation of meta data tags and data segmentation. These are needed to support patient-centric EHR systems and to provide meaningful choices that can be offered to patients concerning the use of their health information
- Embrace the challenges of consumer education
    - Develop awareness among military beneficiaries
    - Provide education about current EHR systems and risks, and about patient-centered efforts to set the future course and development of EHR systems
- Promote awareness and a solid understanding of GINA within the Office of the Under Secretary for Personnel and Readiness OUSD (P&R) Human Research Protection Program and DoD IRBs in order to ensure that genetic research is properly identified and genetic privacy is appropriately reviewed and protected
- Broadly disseminate information about the Health Privacy Summit and the Policy, Technology and Consumer Education Work Groups throughout DoD. Increase attendance and visibility at the Summit and encourage participation in the work groups
- Coordinate efforts for policy writing, technology design and military consumer education, staying focused on the further development of patient-centered EHR systems and the need to build trust and transparency for all stakeholders

References

(2012). *2012 consumer study on data breach notification.* Traverse City, MI: Ponemon Institute. Retrieved from http://www.experian.com/assets/data-breach/brochures/ponemon-notification-study-2012.pdf

Fact sheet: Plan to protect privacy in the internet age by adopting a consumer privacy bill of rights. (2012, February 23). Retrieved from http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b

Helman, R., Greenwald, M., & Fronstin, P. (2008). The 2008 health confidence survey: Rising costs continue to change the way Americans use the health care system. *EBRI Notes,29(10),*2-13. Retrieved from http://www.ebri.org/pdf/notespdf/EBRI_Notes_10-2008.pdf

Johnson, M. E. (2009). *"Data hemorrhages in the health-care sector," lecture notes in computer science.* In Dingledine, R., Golle, P. (Eds.), *Financial Cryptography and Data Security* (pp. 71–89). Berlin, Heidelberg: ICFA/Springer-Verlag. Retrieved from http://fc09.ifca.ai/papers/54_Data_Hemorrhages.pdf

Johnson, M.E., & Willey, N. (2010, May). *Healthcare data hemorrhages: Inadvertent disclosure and HITECH*. Paper Presented at IEEE Symposium on Security and Privacy, Oakland CA. Retrieved from http://digitalstrategies.tuck.dartmouth.edu/cds-uploads/research-projects/pdf/JohnsonEA.pdf

Mozes, A. (2012, July). U.S. doctors embracing electronic health records: survey. *Medline Plus*. Retrieved from http://www.nlm.nih.gov/medlineplus/news/fullstory_127314.html

Press release for health care privacy summit 2011. (2011, May 11). Retrieved from http://patientprivacyrights.org/2011/05/press-release-for-health-privacy-summit-2011/

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193-220. Retrieved from http://www.jstor.org/stable/i256795

The White House, (2012). *Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy*. Retrieved from The White House website: www.whitehouse.gov/sites/default/files/privacy-final.pdf

Win, K. T. (2005). A review of security of electronic health records. *Health Information Management,* 34(1), 13-18. Retrieved from https://www.cs.uwaterloo.ca/twiki/pub/Main/MaxwellYoung/Review_Win.pdf