Multi-Grantee Technical Assistance Meeting: Privacy and Security Considerations for Health IT Research

Prepared for:
Agency for Healthcare Research and Quality
U.S. Department of Health and Human Services
540 Gaither Road
Rockville, MD 20850
http://www.ahrq.gov

Contract No. HHSA-290-2009-00014I

Prepared by:
Booz Allen Hamilton
Massachusetts eHealth Collaborative

Authors
Allyson Miller
Sandy Lesikar
Nalini Ambrose
Seamus McKinsey
Rachel Kell
Barbara Lund

AHRQ Publication No. 13-0048-EF
December 2011

Table of Contents

1. Background

The Agency for Healthcare Research and Quality (AHRQ) Health Information Technology (IT) Portfolio provides ongoing technical assistance to grantees in the form of Webinars, peer-to-peer teleconferences, and one-on-one technical assistance through the National Resource Center for Health IT (NRC). Webinars provide opportunities for grantees to communicate shared experiences, address common challenges, become informed of proven successful research methods, and share other considerations in an open format.

The regulatory environment surrounding the field of health IT is continually evolving. It is imperative for health researchers to stay apprised of the latest legal developments to ensure that research protocols are compliant and that all necessary data security precautions are in place. Health care regulation is complex, and while the Health Insurance Portability and Accountability Act (HIPAA) outlines essential requirements, other applicable privacy protections found in Federal and State law, as well as in contracts and business policies, may call for stronger protection. In addition, data for certain populations, such as minors and patients receiving behavioral health and/or substance abuse services, are subject to increased regulatory protection. Health IT research often necessitates access to patients' protected health information (PHI). PHI is inherently sensitive, and patients and providers alike have valid concerns about PHI being accessed by unauthorized individuals.

This multi-grantee Webinar, titled "Privacy and Security: Considerations for Health Services Research," was held on December 15, 2011, from 1 p.m. to 3 p.m., EST. The objectives of the Webinar are highlighted below:

1. Provide an overview of the privacy and security issues of importance to health IT researchers
2. Outline approaches for researchers to ensure the security of patient data through appropriate policies and procedures governing their team's use of and access to PHI
3. Discuss technical considerations for data use and exchange, particularly as they relate to electronic health records (EHR) and health information exchange (HIE)
4. Share experiences and recommendations among grantees

The Webinar was facilitated by Barbara Lund, M.S.W., M.B.A., of the AHRQ Technical Assistance Team. Presenters for the Webinar were as follows:

- Deven McGraw, J.D., M.P.H., Director of the Health Privacy Project at the Center for Democracy & Technology (CDT)
- Linda Dimitropoulos, Ph.D., Director of the Center for the Advancement of Health Information Technology (CAHIT) at Research Triangle Institute (RTI) International
- Jeff Loughlin, M.H.A., Project Director with the Massachusetts eHealth Collaborative (MAeHC)

2. Meeting Summary

Presentations

The facilitator, Barbara Lund of the AHRQ Technical Assistance Team, provided a high-level introduction to the Webinar's topics, an outline of the event's objectives, and background information on each of the subject matter experts.

Presenter: Deven McGraw, J.D., M.P.H.—Director of the Health Privacy Project at the Center for Democracy & Technology (CDT)
"Policies Governing Uses/Disclosures of Health Information for Research"

Ms. McGraw's presentation focused on policies governing uses and disclosures of health information for research. Her current work focuses primarily on privacy and security issues at a policy level.

The Health Insurance Portability and Accountability Act of 1996

Ms. McGraw began her presentation by providing a high-level overview of the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The HIPAA privacy regulations govern covered entities (most health care providers) and contractors acting on their behalf, also known as business associates. Ms. McGraw noted that the HIPAA privacy rule permits use and disclosure of protected (identifiable) health information (PHI), including both paper and electronic forms of PHI. In contrast, the HIPAA security rule sets forth required and addressable protections for only electronic PHI.

Ms. McGraw discussed when consent is needed to collect PHI in research. Under the privacy rule, quality assessment and improvement activities are part of "health care operations," and therefore consent is not required for use and disclosure of PHI. However, it is important to note that if the primary purpose of the research is not to contribute to "generalizable" knowledge, then the research does not fall under the category of health care operations and consent is needed. When research activities do not fall within this scope, authorized consent is required. Ms. McGraw noted that under the HIPAA privacy rule, using less identifiable information, such as limited data sets (removal of certain categories of identifiers) and de-identified data (removal of more categories of non-PHI identifiers), allows for less risk and fewer regulations. However, she reported that this suggestion is made primarily from a legal perspective; researchers should be aware that there may be institutional policies that researchers are required to follow that are not necessarily embedded in the law.

Federal Common Rule

The Federal Common Rule governs most federally funded health care research and pertains to both clinical research and research on individual level data. HIPAA and the Federal Common Rule have the same definition of "research" as it applies to acquiring consent for collecting and using PHI. Ms. McGraw discussed how Institutional Review Board (IRB) approval is required if research involves clinical data.

Ms. McGraw noted that HIPAA and the Federal Common Rule are two laws that are important and of which any researcher should be aware; however, she noted that researchers should also be

familiar with several other applicable laws and policies. These include State medical privacy laws, health information exchange (HIE), Federal or State grant funding conditions, the Genetic Nondiscrimination Act, and Federal Substance Abuse Confidentiality Regulations.

Future Developments To Watch

Ms. McGraw spoke about several upcoming developments of which researchers should be aware. She added that, while these are not legal changes in effect today, it would behoove researchers to watch for these changes because they might have an impact on researchers in the future. She highlighted the governance rule for "Nationwide Health Information Network," expected to go into effect in early 2012. This rule is being issued by the Office of the National Coordinator for Health IT (ONC) and will likely provide regulations pertaining to or governing HIEs, including access, use, and disclosure of identifiable information. Ms. McGraw also included the following additional developments in her presentation: ONC QueryHealth Initiative, potential changes to the Federal Common Rule, finalization of Health Information Technology for Economic and Clinical Health (HITECH) changes to HIPAA privacy rule, and the proposed rule for Stage 2 Meaningful Use and the beginning discussions for Stage 3 Meaningful Use.

Presenter: Linda Dimitropoulos, Ph.D.—Director of the Center for the Advancement of Health Information Technology (CAHIT) at Research Triangle Institute (RTI) International
"Privacy and Security Requirements Governing Research with Clinical Data: Some Considerations for Health Services Researchers"

Dr. Dimitropoulos focused her presentation on privacy and security requirements governing research with clinical data and highlighted some considerations for health services researchers. She noted that access to electronic clinical information is critical to advancing health services research. In addition, balancing the needs of researchers for access to data with the needs of patients for privacy can, and continues to be, a challenge. Dr. Dimitropoulos began her presentation by providing an overview of the research studies conducted by RTI International. The Health Services Research Team at RTI primarily conducts studies designed to learn more about the quality and cost of health care, patient safety, payment reform, and health care utilization. The studies are evidence-based and are geared toward assisting health care decision makers make changes to improve the quality of care.

Dr. Dimitropoulos provided a high-level overview of additional regulations and guidance under the privacy and security rules. These included The Privacy Act of 1974, HIPAA Privacy and Security Rules, International Privacy Laws, the Confidential Information Protection & Statistical Efficiency Act of 2002 (CIPSEA), and the Federal Information Security Management Act of 2003 (FISMA). She followed by providing examples of different types of projects that typically require higher levels of data protection. Examples included any project designated by the funding agency as having a moderate security level, projects involving data files that include any type of identifiable information (e.g., social security numbers), any project with direct identifiers and very sensitive information, projects requiring a Business Associate Agreement, and projects involving classified information.

Personally Identifiable Information (PII) vs. Protected Health Information (PHI)

PII is defined as information that can be used to uniquely identify a single individual or information that can be used with other sources to uniquely identify a single individual. Dr. Dimitropoulos highlighted data considered to be PII, including a person's full name, home address, telephone number or email, social security number, biometric records, as well as any other identifying numbers (e.g., driver's license number, credit card numbers, medical records number). Researchers also need to be aware of PHI, which, under HIPAA, is defined as PII that relates to a person's health, medical treatment, or payment and that was obtained from a "covered entity" (health care provider, health plan, or health care clearinghouse).

It is important to note that PHI and PII are not the same thing—PHI applies only to research projects that are covered and fall within the parameters of HIPAA. The types of research projects that are typically subject to the HIPAA parameters include research that uses existing PHI and research that includes the treatment of research participants. However, under HIPAA, health information that is de-identified is not considered PHI and thus is not covered under the privacy rule. Dr. Dimitropoulos highlighted two accepted de-identification methods. The first method, called Safe Harbor, entails the removal of the 18 HIPAA-specified data elements from the data set. Dr. Dimitropoulos noted that researchers often do not find this particularly useful because one cannot readily link the data to other data sets or stratify them by geographical locations. The second method is called Statistical Verification and requires using statistical methods to de-identify a data set and typically involves an expert statistician who will note that there is a "very

small risk" of reidentification. In addition, the covered entity must have no actual knowledge of a method by which an individual could be reidentified.

Obtaining Authorization To Use or Disclose PHI

The privacy rule does allow covered entities to use or disclose PHI for research either with or without obtaining authorization from the research participant. Dr. Dimitropoulos outlined what should be included in an authorization form when obtaining consent from a participant to use or disclose his or her PHI. She reported that the forms are generally provided by the covered entity that is involved with the project. Dr. Dimitropoulos stated that under HIPAA, researchers could use one of four options to eliminate the need to obtain authorization: 1) obtain an IRB or Privacy Board waiver, 2) provide documentation that PHI will be used only for activities "preparatory to research," 3) provide documentation that the research will involve only decedents' PHI, or 4) use only a "limited data set" for research, public health, or health care operations. Dr. Dimitropoulos reported that the two most popular and frequently used options are obtaining an IRB or Privacy Board waiver and using limited data sets.

Dr. Dimitropoulos noted that using a limited data set can be useful, especially if the study involves secondary data analysis or if there is no direct contact with any of the study participants. Researchers find this to be more useful than using completely de-identifiable data. Limited data sets require that the research team enter into a Data Use Agreement (DUA) with the covered entity releasing data to the research team. A DUA establishes the permitted uses/disclosures of the data set by the recipient and identifies who is permitted to use or receive the data set. Dr. Dimitropoulos also presented that the DUA must provide that recipients will not use or further disclose the information outside the purposes stated in the agreement, will use safeguards to protect the data, and will report any use/disclosures outside the agreement to the covered entity. Additionally, recipients will ensure that others to whom it releases data set abide by same conditions and will not identify or contact the individuals.

Dr. Dimitropoulos concluded by offering suggestions and considerations for health services researchers. She noted that some covered entities would require researchers to use their IRB or Privacy Board. Researchers should consider incorporating authorization language into consents or use separate authorization forms. State-level privacy laws might be more stringent than HIPAA and must be followed, and researchers should always be prepared for compliance audits.

Presenter: Jeff Loughlin, M.H.A.—Project Director with the Massachusetts eHealth Collaborative (MAeHC)
"Protecting Patient Data: Privacy and Security of Electronic Health Records (EHR)"

Mr. Loughlin focused his presentation on issues surrounding the protection of patient data and the privacy and security of electronic health records (EHRs). He noted that there has been an increase in the use of EHRs, which provided a much greater and improved ability to combine clinical and billing information. In addition, he reported that richer data sets are available because of the use of EHRs.

A number of different programs and regulatory drivers are increasing both the requirement and the desire for structured quantifiable data elements within EHRs. These drivers include the American Recovery and Reinvestment Act (ARRA) and, within ARRA, HITECH and Meaningful Use; payment reform through the Patient-Centered Medical Home and Accountable Care Organizations; the National Quality Strategy through Quality Improvement Initiatives; and the Million Hearts Campaign.

HITECH and Meaningful Use

Mr. Loughlin highlighted different aspects of the HITECH and Meaningful Use initiatives. One important aspect is the changes in data requirements for EHRs. Mr. Loughlin discussed these changes; examples included increases in patient demographics, structured data and problem list (ICD/SNOMED), use of electronic prescribing, increase in use of laboratory results, and increased documentation of other testing and procedures. There is also a rise in data exchange, reporting, and sharing of information through EHRs.

Meaningful Use outlines the requirements for providers for privacy and security. Specifically, the objective is to protect electronic health information created or maintained by certified EHR technology through the implementation of appropriate technical capabilities. The requirements pertaining to privacy and security for EHRs involve conducting a security risk analysis, implementing security updates as necessary, and correcting identified security deficiencies discovered as part of the risk management assessment. Mr. Loughlin noted that providers should be aware of audits and compliance issues. In smaller practices, providers must ensure that they are compliant with all HIPPA regulations as well as Meaningful Use requirements. Moreover, those providers new to using EHRs are also focusing on the physical security of hardware and devices. Mr. Loughlin highlighted additional policies and procedures that all providers using EHRs must be aware of, including password management and role-based access, network security and data encryption, and data backup and the disaster recovery process.

Another driver within Meaningful Use is making patient data available to the patient. Providers are required to allow patients access to their personal information/data via an EHR. The objectives are to provide patients with an electronic copy of their health information (i.e., via CD or USB drive) and to provide clinical summaries for patients for each office visit (paper or electronic).

Health Information Exchange

Mr. Loughlin reported that the objective for HIE is to provide the capability to exchange key clinical information (e.g., Continuity of Care Documents [CCD]) electronically among providers of care and patient-authorized entities. He explained that under Meaningful Use, practices are required, at a minimum, to test their capability of exchanging data via EHRs. As providers adopt

and implement EHRs, it is essential to perform a test to ensure data can be sent back and forth. Providers can use a variety of different electronic transmission methods, including encrypted winzip and Simple Mail Transfer Protocol (SMTP), secure File Transfer Protocol (FTP), secure Socket Layer (SSL) Web Interface, Simple Object Access Protocol (SOAP), and Representational State Transfer (REST).

Mr. Loughlin concluded his presentation by highlighting some of the concerns expressed by large and small practices using EHRs. Specifically, he noted the following concerns: breach notification and HIPAA requirements pertaining to patient and public disclosure requirements, patient consent for HIE, PHI access audit capabilities and requirements, and an increased focus on technical safeguards.

2. Questions and Answers

Question 1: *What if the purpose of one's research is quality assessment and to improve knowledge in a more generalizable way?*

Ms. McGraw replied that it is her understanding that when a person is performing a quality assessment and, if at least one of the purposes of the project is to contribute to generalizable knowledge, then the project falls under and must adhere to research privacy and security rules.

Question 2: *If an internal university climate survey is conducted, but then a completely de-identifiable summary of the results is posted, have you crossed over (re: from a quality assessment to research)?*

Ms. McGraw stated that if the researcher intended to do something strictly internal but then looked at the data that were collected and thought they might be used to contribute to generalizable knowledge, then she would conclude the researcher's initial intention was to perform an internal quality review, and this can be considered operations. Ms. McGraw followed up by saying that if the researcher then reached a point where he or she looked at the data and thought that there might be some value that could be generalized, then the researcher might need to apply the research privacy and security rules to the data at that point. However, posting de-identifiable data is considered to be in the realm with the fewest restrictions within a research context.

The Webinar participant clarified the question and asked about the idea that even if one is not treating it as research but then make it public by, for example, posting it to a university Web site where the public has access to it, is it then considered to be more generalizable public knowledge even if it is not research per se?

Ms. McGraw replied that if the researcher is publishing results that apply only to the specific university's quality and are not generalizable to other institutions, then it is still considered operations. In this situation, the information could be made public as long as the data are presented in a de-identified way.

Question 3: *If there is an honest broker between PHI data and the investigator, which option for waiver applies?*

The speakers asked the questioner to elaborate on the definition of an "honest broker." The grantee stated that an honest broker, within the context of his question, is a person who is not associated directly with the research team whose role and responsibility is to consume and initially view the highly identifiable data. (He or she could see the PHI and the complete data set.) The honest broker's role is then to convert that data by replacing identifiers and then hand them off to the research team. So, PHI is being manipulated by someone who is usually inside the covered entity, and the resulting data are then given to the investigator.

Ms. McGraw cautioned that it could be complicated, but a researcher must start by first thinking about the types of data that the researchers would be able to access, in what ways the identifying data has been masked, and if this masking is sufficient to qualify as a limited data set or de-identified data. If the data meet the requirements of a limited data set or de-identified data, then a waiver is not required. In addition, the researcher needs to think about how the honest broker is being regulated. Is the honest broker potentially a business associate of the covered entity, is he or

she preparing research data sets on the covered entity's behalf, or is the honest broker essentially part of the research team?

Question 4: *In reference to one of the slides titled, "Limited Data Sets and DUAs [from Dr. Dimitropoulos' presentation]," you mention the link code being allowed in a limited data set. Taking into consideration that the link code can take a subject ID and reidentify it back to an individual, we have some mixed signals regarding whether or not you absolutely and positively have to destroy that link table immediately after using it or whether the covered entity can keep the link. What are your thoughts on this topic?*

Dr. Dimitropoulos reported that if the link table remains with the covered entity, then she does not think an IRB would have an issue with it. A researcher would have to specify whether or not he or she planned to go back to access it, and because it is not residing with the researcher's institution, Dr. Dimitropoulos did not feel that the link table would have to be destroyed. She clarified that she was unsure what the situation would be if the table remained with the covered entity.

Ms. McGraw then replied that she was quickly searching through the HIPAA regulations to find language pertaining to this situation, specifically, whether the link table was allowed to be passed along to the data recipient in order for the data to qualify as a limited data set. Ms. McGraw suggested that to be on the "safe side," the key link should stay with the covered entity and should not be passed along. She suspects the request or need to immediately destroy the link is not necessarily a legal issue (and does not recall seeing this under HIPAA) but might instead be an institutional practice and requirement to avoid risk.

Question 5: *Can you provide any guidance on the best ways to stay apprised of what is going on with regulations, especially as they apply to health services research?*

Ms. McGraw replied that it is a great practice to stay involved in professional associations that served researchers or are composed of researchers. These associations tend to track what is going on as it pertains to researchers, especially at the Federal level. A second approach is to talk to compliance officers within your institution. It is the compliance officer's job to be aware of all the different regulatory changes, especially those at a State level.

Question 6: *You referenced a couple of the agreements that have to be in place as researchers are working with different entities. Do you have more to say about agreements? I sometimes have seen researchers stumble on the use of agreements. Could someone speak to the best practices for using agreements when performing this type of research? Are there resources available?*

Ms. McGraw and Dr. Dimitropoulos agreed that researchers reach out to their peers working on similar projects for examples of agreements. Ms. McGraw reported that it could be useful if they are able to share their agreements. In addition, sometimes institutions have templates that they use and can provide to researchers.

Dr. Dimitropolous also suggested visiting the Centers for Medicare & Medicaid Services' (CMS') Web site for examples of good model agreements and reported that AHRQ might also have some resources or models to provide. The CMS Web site can be found at http://www.cms.gov/.

Question 7: *What have you seen in the field regarding educating providers about privacy and security regulations that have been released? When working with providers, researchers want to be confident that the providers have been educated.*

Mr. Loughlin suggested that smaller providers might benefit from joining professional societies and associations as a means of educating themselves. He also suggested that providers should join the Regional Extension Centers (REC) within their State. Mr. Loughlin also reported that many organizations are trying to build on peer networks and are encouraging providers to engage with one another.

Question 8: *Can you refresh us on what key pieces of legislation or initiatives researchers should be focusing on that may have an impact on them?*

Ms. McGraw reported that, within HITECH, researchers should focus on rules that make business associates accountable to authorities for violations of the privacy and security rules. This has passed in statute but, without regulations, these statutes are not effectively being enforced. She noted that some people are holding off on finalizing business associate agreements until specific regulations are put in place. Researchers need to be aware of when a true business associate relationship exists and when it does not. In addition, the HITECH provision rule will have an impact on researchers regarding the prohibition on the sale of PHI. It is unclear how the exception for research will be interpreted within the rule. Aside from HITECH, the governance rule for the Nationwide Health Information Network is also important for researchers to pay attention to if the researcher regularly deals with an HIE to obtain data.

Comment: A grantee said: I think all of us on the call were required to write a security plan when submitting our grants; a security plan is different than a data monitoring plan. Writing this plan was a condition for submitting an AHRQ grant proposal under health IT. Because I had never seen a security plan before, I was unsure of how to draft the plan. It would have been helpful if AHRQ could have provided a model security plan as an example.

Response: AHRQ will consider providing a template for a security plan for grantee applicants.

Appendix: Presenter Bios

Presenter: Deven McGraw, J.D., M.P.H.—Director of the Health Privacy Project at the Center for Democracy & Technology (CDT)

Deven McGraw is the drector of the Health Privacy Project at the CDT, where she promotes policies that protect individual privacy as personal health information is shared electronically. Ms. McGraw serves on the Health Information Technology (HIT) Policy Committee run by the Department of Health and Human Services and established in the American Recovery and Reinvestment Act, chaired by the Office of the National Coordinator for Health Information Technology, and chairs its Privacy and Security Workgroup. The HIT Policy Committee is a Federal Advisory Committee that makes recommendations to the National Coordinator for Health IT on a policy framework for the development and adoption of a nationwide health information infrastructure, including standards for the exchange of patient medical information. Ms. McGraw is a magna cum laude graduate of the Georgetown University Law Center and received her Master of Public Health from The Johns Hopkins University.

Contact email: deven@cdt.org

Presenter: Linda Dimitropoulos, Ph.D.—Director of the Center for the Advancement of Health Information Technology (CAHIT) at RTI International

Dr. Linda Dimitropoulos is the director of the Center for the Advancement of Health Information Technology (CAHIT) at RTI International. The Center brings together a multidisciplinary group of clinical informaticians, policy analysts, researchers, and clinicians focused on improving health care delivery through the effective use of health IT. Dr. Dimitropoulos is a social psychologist with expertise in attitude change, measurement, and persuasive communications with applications to consumer behavior and decisionmaking. She has 18 years of experience designing and managing health services research studies and currently leads several key Federal contracts, including the AHRQ Technical Assistance to Implement Health IT and HIE in Medicaid and CHIP contract. She serves as the program director for the National Resource Center for Health IT contracts, also funded by AHRQ. Dr. Dimitropoulos led the Privacy and Security Solutions for Interoperable Health Information Exchange and the Health Information Security and Privacy Collaboration (HISPC) contracts for AHRQ and ONC, which studied the variation in Federal and State health information privacy laws and policies governing electronic health information exchange.

Contact email: lld@rti.org

Presenter: Jeff Loughlin, M.H.A.—Project Director with the Massachusetts eHealth Collaborative (MAeHC)

Mr. Loughlin is a project director with the Massachusetts eHealth Collaborative (MAeHC) and currently serves as the director for the Regional Extension Center of New Hampshire, working with providers, practice leaders, and medical and administrative staffs to ensure successful adoption and Meaningful Use of EHR technology in the medical office environment. He has worked with the Collaborative for 6 years, providing a variety of consulting services to practices and community-based EHR and HIE initiatives. Prior to joining MAeHC, Mr. Loughlin served as an IT consultant at Boston Medical Center, providing EHR implementation and training services for the outpatient medical departments. Before moving to the IT team, he spent several years as a

Practice Manager in a variety of outpatient settings at Boston Medical Center, Harvard Vanguard Medical Associates, and Boston City Hospital. Mr. Loughlin is a U.S. Army veteran with more than 23 years of military service and is currently serving with the Massachusetts Army National Guard as a Medical Service Corps Lieutenant Colonel. He holds a master's degree in Healthcare Administration from Simmons College in Boston.

Contact email: jloughlin@maehc.org