Article 29 Data Protection Working Party: "Working Document on the processing of personal data relating to health in electronic health records (EHR)"

Comments from Joan Antokol, Esq., Partner and Head of Privacy and Data Protection Group, Baker & Daniels, LLP, (Formerly Vice President and Global Head of Privacy for Novartis, and Compliance Trainer for NJ Pure Medical Malpractice Insurance Company).

****

The Working Document is very well written and much needed. The Article 29 Working Party and other colleagues who contributed to this effort obviously spent a great deal of time identifying the relevant issues and evaluating possible solutions to protect sensitive patient information in national or regional health databases. I applaud these efforts and consider this document to be a valuable contribution to privacy, security and healthcare. This work can also serve as a basis for countries outside of Europe in addressing privacy and security protections for EHR databases.

Drug Safety/Pharmacovigilance

In addition to the reasons for nationwide EHR schemes provided in the Working Document, the existence of national EHR databases will also likely promote patient safety through enhanced pharmacovigilance. Most experts agree that only a fraction of adverse drug reactions (i.e., 10-20%) are reported to health authorities. National medical records databases would likely contain a great deal of information about patient experiences with pharmaceuticals. If that information were available to health authorities *in fully anonymized form*, it could help them better identify drug reactions and safety signals. The larger quantity of data involving many patients would likely help detect adverse reactions that were not identified by the pharmaceutical sponsor during the clinical trials, such as rare life-threatening reactions, those that occur as a result of interactions with other medications, and those that occur after longer drug exposure. This would, in turn, allow health authorities and other stakeholders to take action more rapidly to ensure patient safety.

Drug Efficacy and Cost Effectiveness

The data in national records databases would also be useful to evaluate and compare the efficacy of different pharmaceutical and non-pharmaceutical approaches to various disease states. An economic analysis using fully anonymized data would make the possible trade offs more visible as health care resources become increasingly constrained.

Encryption

As noted in the Working Document, there are generally very long retention periods for medical records. The data controllers of EHR databases need to evaluate the standards of encryption that will withstand the test of time. The number of bits used several years ago for encryption (i.e., 56 or so) is now easily penetrable by hackers. Currently, encryption standards are in the range of 512 bits. It is likely that the need will arise from time to time to decrypt and re-encrypt data in national databases as additional levels of security become necessary to avoid intrusions.

It is important to anticipate this need (and the related costs), as well as other security measures that may be needed as technology and the sophistication of intrusion both advance.

Portable Electronic Devices

Higher encryption standards generally slow down considerably the transmission of medical data to portable devices, such as laptops and handhelds. In the emergency medical context, the delay in receiving medical information could potentially affect patient care and outcomes. Perhaps there could be varying levels of encryption based upon the risk involved. For example, there could be higher levels of encryption required for transfers of multiple patient files from one large database to another large database, and lower levels of encryption for one doctor requesting one patient's medication history to do a quick review on his/her handheld prior to authorizing a refill prescription. In the lower encryption situations, it might be possible to restrict the viewing period to a short window of time, with “review only” rights (no copying or downloading), to minimize the risk of improper access. Indeed, for access through portable electronic devices, it might be advisable to require in all instances that the log on occur through a Citrix type server, where medical practitioners can view the data in image form only without any data actually left on those devices.

Access by Medical Practitioners and Healthcare Staff

As also noted in the Working Document, it is necessary to identify and authenticate users uniquely and appropriately. The Working Document suggests that authorized personnel of healthcare institutions involved in a patient's treatment may be given a right to access EHR databases, provided that the healthcare professional is actually and currently providing treatment to the patient. While I assume that the intent is for *each* medical practitioner or authorized personnel to obtain his/her own password, it is possible that some sharing may occur, such as between physicians and nurses, hospital staff or ambulance workers who may be assisting them. (There may also be financial incentives to share passwords if each user must pay a separate fee for access.) It will be important to address this situation, including the requirements for medical personnel to obtain their own access rights. It may also be useful to consider whether system users will be permitted to remain connected for extended periods of time, such as a full shift in the medical office or hospital, which may increase the risk that others may obtain access through their connection. If so, it may be useful to have the database's audit trail capture the amount of time that the user has been connected (in addition to other relevant information).

Reliable Identification of Patients

As noted in the Working document, reliable identification of patients in EHR systems is of crucial importance. This will be a challenge, particularly for patients with common names who move from one location or one treating physician to another. Absent smart card or health card identification and match-up, it would be helpful to explore further how new patient records, particularly those reflecting a different address or those from a different treating physician, will be added to an existing patient's record. Will the new physician be included in the review of the patient's historical records to evaluate whether it is in fact the same patient? Will the patient be contacted for input, with the risk that patient records may be inadvertently exposed? Will employees, an oversight board, or external experts make the final decision? What will happen to those records that cannot with any degree of certainty be assigned to an existing patient? How will duplicate names be merged into one patient?

User Authorization and Authentication – Submission of EHRs

It would be helpful to explore further how submitting EHRs to the databases will work. Will all medical practitioners (once authenticated) automatically be allowed to submit patient records, or will there be limitations, such as confirmation of ongoing actual treatment of the patient? Will the physician's or hospital's staff be allowed to submit information? How about transcription services, laboratories, medical clearinghouses, pharmacies or insurance companies?

Legitimate Basis for Access to Patient Records

In the US, a number of the 20,000+ HIPAA Privacy Rule complaints that have been filed to date involve healthcare workers who did not have a legitimate basis to review a patient's record, but nevertheless did so out of curiosity or snooping. For instance, there have been reports where hospital employees became aware that their ex-spouse, an ex-spouse's new partner, a neighbor or a co-worker was undergoing treatment. The hospital employee accessed the patient's information out of curiosity, and was later terminated when the violation was reported and investigated. Similarly, medical staff members who became aware that a celebrity or public official received treatment have occasionally accessed the person's records without a legitimate basis for doing so. These situations could also occur with a national medical records database, and may be identified through an audit trail on the system.

Genetic Data

Some people believe that genetic data is even more sensitive than other types of health data because (a) it theoretically encompasses all types of health conditions and predispositions including but not limited to psychiatric problems; and (2) it very likely will provide information about other family members. Will the Working Document standards also apply to genetic data stored in EHR databases? If so, does the Working Document supplement genetic data laws that exist in certain countries? Has anyone evaluated whether there are any perceived conflicts between those laws and the Working Document?

Law Enforcement

There are likely to be situations where law enforcement will seek access to medical records, such as to obtain home addresses of individuals wanted in connection with crimes, to confirm blood alcohol or illegal drug use after car accidents, to evaluate HIV/AIDS or other diseases of attackers in connection with rapes. Some thought should be given to these issues.

Other Interested Stakeholders

As noted in the Working Document, insurance companies and others involved in claims reimbursement may seek access to patient information in EHR national databases. Employers may also seek access to the data. Of course, the individual should have the right to decide who has access to his/her data.

US Approach

Because the HIPAA Privacy and Security Rules only apply to "covered entities", and because the Federal Trade Commission does not have jurisdiction over all industries, the US would likely require new laws to impose national standards for electronic health records databases. (Even if the HIPAA Privacy and Security Rules, or the FTC requirements did apply, those laws do not contain the level of specificity in the Working Document, such as layered consents or sealed envelopes.)

The US Food and Drug Administration has just announced that it will issue a proposed rule to regulate electronic health records transferred directly to a database from a medical device. The FDA plans to exercise its jurisdiction to do so by determining that the medical records become part of the device. In its comments relating to this proposed rule, the FDA's Chief Information Officer, Tim Stitely, advised that he was not sure whether any federal organization would regulate electronic health records, but that with their growing popularity, he thought they would fall under the Office of the National Director for Health Information Technology's purview, rather than the FDA. It is possible that various stakeholders, such as the American Medical Association or the American Hospital Association, might also want to issue best practice guidelines.

Medical Identity Theft

In the US and elsewhere, identity theft is a huge issue. In some situations, it involves not only theft of financial identity, but also theft of an individual's medical identity, such as for insurance coverage purposes. While the numerous privacy and security protections described in the Working Document will likely protect against this threat, it is important to remain vigilant as the threat continues to evolve.

****

Please do not hesitate to contact me if I can provide any clarification of my comments, or to discuss further.