FOUR HOT TOPICS IN HEALTHCARE TECHNOLOGY 2014-2015.

Kathryn Coburn, Committee Co-Chair


   **A. Privacy Advocates claim:**

   1. The $30 billion/year industry in sales of “de-identified” protected health information (without the patients' consent and authorization), is creating mistrust of the confidentiality of medical information transmitted electronically.

   2. The sale of “de-identified” health information is obstructing the federal Framework for secure, free flow and electronic exchange of Protected Health Information (PHI) for treatment of patients, payment of insurance claims, health care operations that benefit patients, healthcare providers and health plans, reduce costs and promote better outcomes.

   3. The reasons are:
   (a) **There is no regulatory oversight of the de-identification process, which frequently results in inadequate de-identification of PHI** and often enables re-identification of the PHI by the purchaser.
   (b) “De-identified” information is re-identified for a variety of unregulated uses by purchasers of the health information, vitiating patient confidentiality rights.

   **B. Data Brokers who buy and use “de-identified’ health information and sell “re-identified” health care information argue:**

   1. The sale of “de-identified” health information is legal under federal law, namely, the Health Insurance Portability and Affordability Act of 1996 (HIPAA) and the HIPAA Privacy Rule and regulations.

   2. “De-identified” health information is not “protected health information”.

   3. Data brokers who acquire “de-identified” health information are not subject to HIPAA and therefore not forbidden to re-identify the health information they have purchased.
II. HIPAA Privacy and Security Audits.

1. The Office of Civil Rights (OCR) plans to enhance HIPAA enforcement capabilities, using a new website to perform Privacy and Security Compliance Audits.

2. OCR has published a stringent and comprehensive Audit Protocol, which will be used to perform both desk and onsite audits.

3. HIPAA fines levied by OCR, if the healthcare provider or health plan or business associate of either, fails the audit, will be placed in a fund to support further HIPAA compliance audit activities.

4. Last year, audits showed that the most common HIPAA violation was a failure to document a periodic security risk assessment.

5. Entities that fail the OCR HIPAA audits will be required to pay fines, comply with the HIPAA privacy and security standards, implement HIPAA privacy and security procedures, including risk assessments, perform HIPAA remediation activities and submit to OCR HIPAA monitoring for up to 20 years.


1. Who owns the data a consumer places on the healthcare app? Data ownership rights may be acquired by contract or they may exist as a matter of law. Is the app connected to a Website? Is there a license agreement that clearly describes the rights of the consumer and the rights of the app owner in the data?

2. Apps are frequently used as a mechanism for consumer adherence to treatment and for monitoring health outcomes of consumers. What can the app owner do with the information the consumer places on the app?

3. Who is responsible for meeting privacy obligations when the data are collected by another entity and not stored on the user’s personal device?

4. Is there a healthcare provider or a health plan or business associate of either who is accessing the information? If so, on whose behalf is the owner of the app providing services, on its own behalf or on behalf of the provider, health plan or business associate?
IV. Regulation of Artificial Intelligence in Healthcare.

1. Government regulation of medical devices, robots and drones used in healthcare and healthcare operations is expanding at lightning speed.

2. Under a recent case, November 17, 2014, the Federal Aviation Administration (FAA) regulates drones as unmanned aircraft, no matter how small or inexpensive the drone. (See Huerta v. Pirker, National Transportation Safety Board, Docket CP-217).

3. The Federal Communications Commission (FCC) regulates wireless medical devices, as does the Federal Trade Commission (FTC) in certain cases.

4. Surgical robots are regulated by the Department of Health and Human Services (HHS) and by the FTC.

The Healthcare Technology Committee welcomes commentary from other SciTech Committees interested in any of these Hot Topics. We would like to collaborate with you on presentations and webinars. Please call 424.238.4501.