The Office of the National Coordinator for Health Information Technology

Office of the Chief Privacy Officer Update

June 23, 2016

Lucia Savage, JD, Chief Privacy Officer, ONC

ONC OCPO Update

- Security and Cybersecurity
- Next round of fact sheets: Sharing for Public Health purposes
- Clarifying about Opting in and Opting Out

Cyber Information Sharing Act of 2016

Internal Analysis and Reporting	(b)(1)) Report.— (1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretary shall submit to the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Energy and Commerce of the House of Representatives a report on the preparedness of the Department of Health and Human Services and health care industry stakeholders in responding to cybersecurity threats.
Threat Sharing Task Force	(c) Health Care Industry Cybersecurity Task Force.—(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary, in consultation with the Director of the National Institute of Standards and Technology and the Secretary of Homeland Security, shall convene health care industry stakeholders, cybersecurity experts, and any Federal agencies or entities the Secretary determines appropriate to establish a task force to—
Security Standards Task Force	(d) Aligning Health Care Industry Security Approaches.—(1) IN GENERAL.—The Secretary shall establish, through a collaborative process with the Secretary of Homeland Security, health care industry stakeholders, the Director of the National Institute of Standards and Technology, and any Federal entity or non-Federal entity the Secretary determines appropriate, a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that

Ethical Hacking

- According to Politico Cybersecurity May 12, 2016:
  - Defense Secretary Ash Carter said he was impressed by the "Hack the Pentagon" program, the first phase of which ends today. More than 1,400 hackers signed up for the bug bounty pilot initiative targeting Pentagon websites, with more than 80 bugs discovered that qualified for payouts so far. "All of this is helping us be more secure, at a fraction of the cost that exhaustively diagnosing ourselves would take," he said. "And we believe this approach, effectively crowd-sourcing cybersecurity, has great potential for us, as it does for a number of you around the table." ‘
- If ethically hacking the Pentagon is helpful, how could this help security in the healthcare sector? Why does this not occur more?

Public Health Activities (sample)

- Example from 45 CFR 164.512(b) A covered entity may use or disclose protected health information for the public health activities and purposes described in this paragraph to
  - (i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions . . .
  - (iv) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or

Basic Choice: When is Opting required by law and what are the implications of such a requirement?

- **New research is helpful: Downing, et al, "***Health information exchange policies of 11 diverse health systems and the associated impact on volume of exchange***" Journal of AMIA, June 17, 2016, http://jamia.oxfordjournals.org/content/early/2016/06/14/jamia.ocw063**
- **Objective:** to examine the relationship between electronic exchange of patient health information across organizations and organizational HIE policy decisions. We focused on 2 key decisions: whether to automatically search for information from other organizations and whether to require HIE-specific patient consent.