Briefing on Report: *Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA* 
ONC Joint Health IT Committee 

July 27, 2016 

Lucia Savage, JD, Chief Privacy Officer, ONC 
Devi Mehta, JD, MPH, Privacy Policy Analyst, ONC
Agenda

• Non-Covered Entity Report Findings
  » Identification of the Problem
  » Legal Scope of HIPAA and Non-Covered Entities
  » Why this Report at this time

• Cybersecurity Initiatives
Non-Covered Entity Report Findings


- Report demonstrates continued gaps in policies around access, security, and privacy. In addition and as a result of these gaps, confusion persists between HIPAA regulated entities and those not regulated by HIPAA among both consumers and innovators.

- Report identifies the lack of clear guidance around consumer access to, and privacy and security of, health information collected, shared, and used by non-covered entities (NCEs).
Non-Covered Entities Defined

• **Non Covered Entities (NCEs)** are technologies managed by businesses that collect electronic heath information about individuals and are NOT covered by HIPAA as a “covered entity” or a ‘business associate”. Includes:
  
  » **mHealth technology**, such as entities that provide direct-to-consumer mobile health applications, remote health monitoring devices, or wearable health tracking devices.

  » **Health social media**, including social networking websites for health purposes, which might be accessed on computers or smart phones and other mobile devices.

  » **PHRs not hosted by covered entities**.

• **Out of scope for report**: Products, services, and data sources where health information is derived from other data, e.g.

  » GPS data

  » Pollen counts connected to zip codes

  » Casual social media disclosures (compared to social media sites that are health-focused)
Identification of the Problem

• Consumers believe HIPAA protects their data when it may not—HIPAA protection does not apply to all health information everywhere it is collected, accessed, used or stored.

• HIPAA has specific prohibitions against the use of identifiable data for marketing; this rule does not apply to NCEs.

• NCEs are not required by law to adhere to minimum security practices, whereas HIPAA provides minimum security standards.

• NCEs are not required by law to give consumers access to their health information, or to send it (disclose it) as the consumer wishes, whereas HIPAA guarantees this right.

• Lack of clear rules may be delaying economic growth.
What Protections Exist?

• HIPAA, enforced by OCR and state Attorneys General, provides nationwide privacy, security & breach notifications for health information accessed, used, disclosed or held by Covered Entities and their Business Associates.

• The Federal Trade Commission
  » has a well-developed body of law enforcing privacy and security practices that are unfair and deceptive, including taking action against an organization that adopts a code of conduct, but does not adhere to that code.
  » Uses its authority to bring enforcement actions against companies that fail to have reasonable and appropriate data security practices regarding consumer data, including health data.
  » The FTC has also used its authority under Section 5 in cases where, for example, the Commission has reason to believe that a business made false or misleading claims about its privacy or data security procedures.

• HHS through the Food & Drug Administration oversees the safety of medical devices, including those that act through apps that are within the FDAs authority.
Why This Report Now?

• Growth in mobile health technologies beyond 2019
• Precision Medicine Initiative
• Consumer engagement a necessary component of Delivery System Reform
• Consumers have gone mobile
Important Components of ONC Efforts

• Findings support and underscore the recommendations from the API Task Force

• Identify legal gaps important to understand if consumers are to take advantage of
  » 2015 Edition provisions
    – Open Read-only API
    – Transmission via unsecured email
  » Focus on consumer rights of access

• For consumers and policy-makes it compliments the content of
  » the FTC developer guidance webpages
  » OCR’s App developer guidance
Cyber Security Update

• CISA 405(c) task force, the Health Care Industry Cyber Task Force
  » Met July 21
  » Next in person meeting October 26, location TBD
    – More info available on http://www.phe.gov/preparedness/Pages/default.aspx

• Improving Cyber threat sharing in the Health and Public Health Sector.
  » July 20, ONC published a funding opportunity for to help improve cyber threat sharing;
  » July 25, Assistant Secretary for Preparedness and Response (ASPR), the sector specific agency, published a funding opportunity for a Sector Information Sharing and Analysis Organization (ISAO)
    » Read the joint ONC/ASPR blog

• Fulfills commitment C.3.3 in Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap version 1.0
Questions?

Lucia Savage, JD, Chief Privacy Officer, ONC
Lucia.Savage@hhs.gov 202-690-3955

Devi Mehta, JD, MPH, Privacy Policy Analyst, ONC
Devi.Mehta@hhs.gov 202-205-4411