The Office of the National Coordinator for Health Information Technology

Briefing on Report: ***Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA***
HL7 Mobile Health Workgroup

September 21, 2016

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
  - Next Steps

Non-Covered Entity Report Findings

- Report entitled, ***Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA,*** released on July 19, 2016. (https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf)
- This Report demonstrates that large gaps in policies around access, security, and privacy continue. 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.
- The 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, such as:
  - 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 retarding economic growth.

What Protections Do 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 (FTC) Enforcement Mechanisms:
  - » 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 as a necessary component of Delivery System Reform
- Consumers have gone mobile

An Important Component of ONC Efforts

- Findings support and underscore the API Task Force Recommendations.
- Identify legal gaps that are important to understand in light of:
  - 2015 Edition (CEHRT Rule) provisions:
    - Open Read-only API
    - Transmission via unsecured email
  - Focus on consumer rights of access
- Information complements the content of:
  - FTC Mobile Health App Developer Tool (https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool)
  - OCR's mHealth Developer Portal (http://hipaaqsportal.hhs.gov/)

The Office of the National Coordinator for Health Information Technology

Questions?

Devi Mehta, JD, MPH, Privacy Policy Analyst, ONC

Devi.Mehta@hhs.gov, 202-205-4411

@ONC_HealthIT @HHSONC HealthIT.gov