The Office of the National Coordinator for
Health Information Technology

ONC Update

HIPAA Summit
Washington DC, September 16, 2016

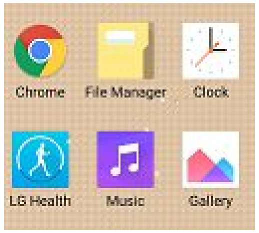
Lucia C. Savage, JD, Chief Privacy Officer, Office of the National Coordinator for Health IT,

Agenda

1. APIs, Apps, and Access
2. mHealth and Health Social Media
3. HIPAA Basics, Phase II
4. Its Cybersecurity Month
   - Neighborliness in the Cyberhood
   - Other Current Work
5. Advancing computable privacy through
   - Identity Proofing
   - Electronic Consent Management
   - State Privacy Law Discussions

APIS, Apps, and Access

EHR APP



American patients are embracing digital health information

- 80% say it is “very” or “somewhat” important that their doctors use online medical records.
- More than 70% say it is “very” or “somewhat” important that they be able to access their
  - Labs
  - Medication histories
  - General health history
  - Physician’s notes.
- Yet, same polling shows that only 40% said the data they wanted (see above) was available to them.

Source: http://kff.org/health-costs/poll-finding/kaiser-health-tracking-poll-august-2016/

How ONCs 2015 Edition Rule on certified EHR Technology Automates Patient Access and Information Exchange

Under HIPAA

- Advances Congress' requirements in HITECH sec. 13405(e) that Patients **right to send a copy (transmit) elsewhere; see also** 45 CFR 164.524
- have the **right to an electronic copy** of their PHI, if the records are stored electronically, and
- *and* PHI can be **shared for permitted uses (TPO); APIs can facilitate**

MU Stage 3 Requirements

Patient must be given electronic access to portal within 24 hours in order to

- **view online, download and transmit** their health information
- **AND access to an API** that can be used by 3rd party apps

Related CEHRT Requirements

- **API functionality** including
  - lookup and retrieve whole or partial patient record
- **API security** measures
- A **"transmit" option that includes unencrypted email**

The Office of the National Coordinator for Health Information Technology

Summary of Key Recommendations from Collaborative Federal Advisory Committee Task Force on Privacy & Security of APIs

- Continue outreach on the fact that HIPAA does not limit what types of apps a patient can use. The only relevant concerns should be:
  - technical compatibility (i.e. app works with the API technical specifications);
  - patient choice.
- Advance the idea of self-registration of apps
  - Registration should not become a barrier to patient choice.
- Encourage a voluntary market in app endorsement.
- Encourage Transparent Disclosure Privacy Practices of apps through Model Privacy Notice and other efforts.
- Work to improve the "privacy literacy" of consumers
- Help providers have confidence that an app is authorized to act on behalf of a particular patient.
- Ensure that providers understand how to protect the security of their systems from malicious technology, and have confidence to discuss security with their patients, without the patient's security choices being a barrier patients choosing apps that work for them.
- Take advantage of an API's ability t provide auditable data on access to create transparent information for consumers.

API, Apps and Access: Educating Stakeholders

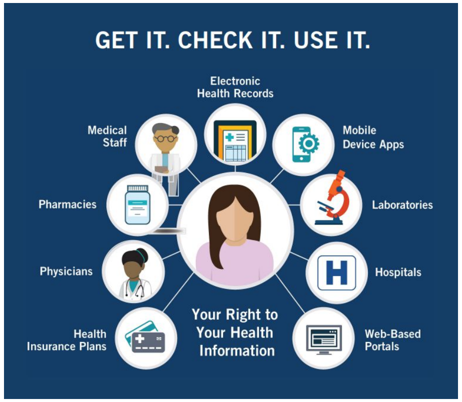
- Implementation Guides available on healthit.gov
  - See section 170(g)(7), (8), and (9) at https://www.healthit.gov/policy-researchers-implementers/2015-edition-test-method
- API Privacy & Security Task Force Recommendations to ONC
- Videos for consumers and providers on individual's right to access their data: https://www.healthit.gov/access

mHealth and Health Social Media

- New ONC Report Exploring Privacy & Security of mobile health technology compared to HIPAA: https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf
- Key Findings
  - Differences in individuals' right to access or transmit data collected about them.
  - HIPAA has a security floor; outside of HIPAA, there is no particular security regulation, although security must be fair and not misleading.
  - HIPAA regulates whether data can be sold or used for marketing; outside of HIPAA, this is governed by terms of use, fairness and being not misleading.
  - Consumers are generally familiar with HIPAA, and think it applies where it does not.
  - Developers are confused as well, and confusion may be impeding innovation.
  - New study of which mobile health apps, like fitness trackers, have transparent privacy polices (not evaluating the caliber of the policy itself).

HIPAA Basics, Phase II

- Phase I: HPAA Supports Exchange for
  - Treatment
  - Health Care Operations
  - OCR Guidance on Individuals’ Right to Access their Own PHI
  - ONC/OCR videos and infographic
- Phase II:
  - HIPAA Supports Exchange for Public Health Activities
  - HIPAA Supports Exchange for Health Oversight



October is Cybersecurity Month

- Improving security in the Cyberhood
  - Why:
    - In an ***interoperable, interconnected health system***, an intrusion in one system could allow intrusions in multiple other systems.
  - How: Grants to expand threat sharing
  - Security Risk Assessment Tool update
  - HHS Healthcare Cyber Information Sharing Task Force
    - Blogs available
    - We need your input
  - HHS Health & Public Health Sector Coordinating Council:
    - Contact Steve.curren@hhs.gov
  - DHS guidance on information sharing by private sector:
    - https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf
    - OCR Guidance on sharing cyber threats

CyberhoodWatch

We immediately report all suspicious activities to our Healthcare Neighbors

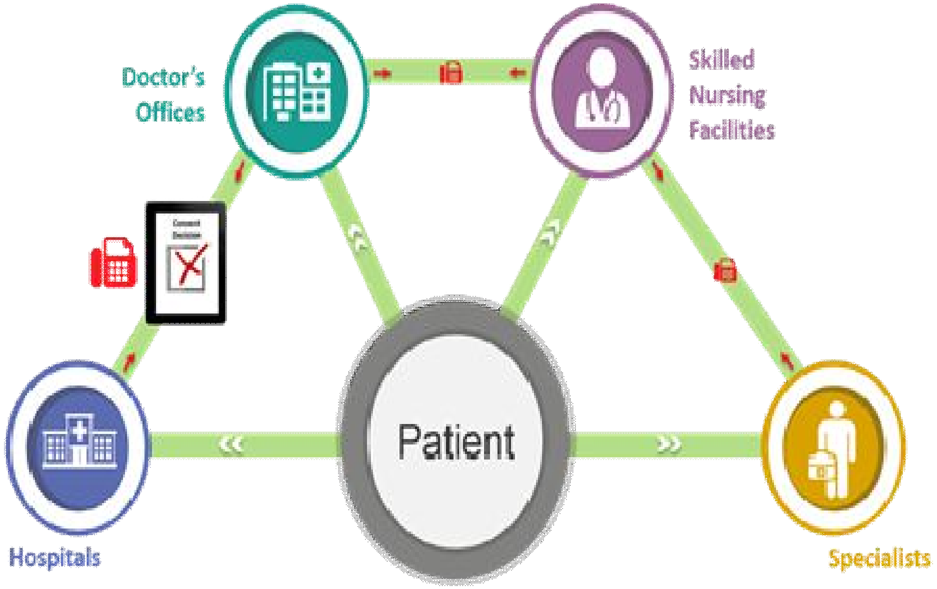
Hot off the presses

Improving Security Hygiene in Healthcare

- Some other stuff we’re working on
  - Updates to our Security Risk Assessment Tool
  - Ethical Hacking
  - Security Engineering and APIs
    - API Task Force concluded that security issues for read-only, open-specification API in healthcare are *the same* as security issues for existing read-only, open-specification APIs, such as made available in other sectors: Internet commerce, banking, energy

Computable Privacy

- What is it: Making Privacy less reliant on paper



- More information at Computable Privacy In Action

Advancing Computable Privacy

- Identity Proofing
  - » Individuals Accessing their own PHI
  - » National Standard for Trusted Identities in Cyberspace, (NSTIC) pilots in healthcare and social services
    - – http://nstic.blogs.govdelivery.com/2016/08/25/citius-altius-fortius-announcing-6-new-pilot-projects-across-10-states-and-d-c/
- Capturing and electronically documenting Individual’s privacy choices
  - » http://confluence.siframework.org/display/PATCH/The+Patient+Choice+Technical+Project+Homepage
- State Privacy Law

The Office of the National Coordinator for Health Information Technology

Questions?

Lucia Savage, JD

Chief Privacy Officer

www.healthit.gov

PrivacyAndSecurity@hhs.gov

@savagelucia

@ONC_HealthIT

@HHSONC

HealthIT.gov