The Office of the National Coordinator for Health Information Technology

OCPO Update

27 Months in Review

Lucia C. Savage, JD, Chief Privacy Officer

Agenda

- Security Update
- Privacy Update
- We have accomplished a lot!

Security Update

- National Commissions Weigh In On Information Technology Security
  - » President’s Commission on Enhancing National Cybersecurity Report issued December 1, 2016
- Nationwide DHS/FBI Briefing on Cybersecurity, December 30, 2016
- Healthcare Industry Cybersecurity Task Force (HCIC Task Force, under CISA section 405(c)

President’s Commission on Enhancing National Cybersecurity: Genesis and Purpose

- Commission established by Executive Order 13718
- Intended to be recommendations for President Elect
- Charge:

  The Commission will make detailed recommendations to strengthen cybersecurity in both the public and private sectors while protecting privacy, ensuring public safety and economic and national security, fostering discovery and development of new technical solutions, and bolstering partnerships between Federal, State, and local government and the private sector in the development, promotion, and use of cybersecurity technologies, policies, and best practices. The Commission's recommendations should address actions that can be taken over the next decade to accomplish these goals.

- Supported by NIST staff and principals
- Final report issued December 1, 2016

Input to Commission (Healthcare and otherwise)

- Federal Agencies supplied dedicated expert input: NIST, DHS, DOD, Justice, GSA and Treasury.
- Commissioner Ana Anton, currently at Georgia Tech, has some background in secure software for healthcare
- In a series of public meetings, Commissioners took testimony; Robert Booker, Chief Information Security Officer, UnitedHealth Group, provided testimony on August 23, 2016
- Other witnesses in Appendix 2
- Public RFI from NIST resulted in 1100 comments.

Recommendations that Correlate to HHS Current Efforts (not in priority order)

- Incent the sharing of threat information, and how to act on such information, through public/private collaboration (Recommendation 1.2, starts at p. 14),
  - Including pathways for businesses to share threat information without fear of inappropriate legal liability.
  - Information sharing should include threats found in the supply-chain
- Strong identity authentication (recommendation 1.3, starts at p. 16)
  - HHS staff already should be using two factors
  - ONC has accepted a FAC recommendation to move to require multifactor capability for system users in EHRs it certifies.
  - ONC committed to policy guidance on the identity proofing and authentication rigor for consumers to access their own information.
- Develop concrete efforts to support small and medium sized businesses (Recommendation 1.5, starts p. 21)
- Private/public efforts to rapidly improve security in IoT, including through rule-making where appropriate and authorized. (# 2.1, p.25)

Commission Recommendations to Do More

- Improve consumer awareness of cybersecurity in managing their own affairs.
- Agencies should impose cybersecurity standards by rulemaking when appropriate
- Expand qualified cybersecurity workforce
- Improve government management of data assets and procurement, including a more influential role for OMB, using Enterprise Risk Management Techniques
- Collaborate internationally.

President's Commission Summary Key Findings and Notable Recommendations

Note: the report contains 16 recommendations, too lengthy for this presentation. It was intended as a foundational document for the new Administration, and should be read in its entirety as such.

- Economic sector matters less and less as the internet of things causes technical convergence and an inability to segment risk by economic sector: (p. 23)
- Many organizations and individual fail to do the basics of cybersecurity. (p. 7)

Department of Homeland Security/FBI Cybersecurity Briefing December 30, 2016

- Although in the context of nation-state cyber hacking, in this nationwide public (no clearance required) call, the following techniques were recommended to improve cybersecurity prophylaxis
- Data Backups
- Risk Analysis and remediation
- Staff Training
- Vulnerability Scanning & Patching
- Application Whitelisting
- Incident Response
- Business Continuity Planning
- Penetration Testing

Healthcare Industry Cybersecurity Task Force

- Team is hard at work
- Incredibly dedicated group of volunteers
- Assistant Secretary for Preparedness and Response is leading the charge and is main point of contact.

Privacy Update

- Model Privacy Notice
- Public Health Oversight Fact Sheet
- NGA Roadmap for States

Model Privacy Notice: Privacy Policy Snapshot Challenge

- The Model Privacy Notice (MPN) is a voluntary, openly available resource designed to help health technology developers who collect digital health data clearly convey information about their privacy and security policies to their users.
- In 2011, in conjunction with the Federal Trade Commission (FTC), ONC released a MPN focused on personal health records (PHRs), which were the emerging technology at the time.
- Recognizing a need for an updated, broader MPN, ONC with the help of OCR, FTC, and various stakeholders, developed new MPN content and launched the **Privacy Policy Snapshot Challenge**. The challenge provides an award to the creators of the best MPN generator that produces a customizable MPN for health technology developers.
- Submission Deadline: April 10, 2017
- Many ONC Offices are working on this: OCPO, OPOL, and OPRO office of Consumer eHealth, with assistance from OCR and FTC.
- For more information on the Privacy Policy Snapshot Challenge visit https://www.challenge.gov/challenge/privacy-policy-snapshot-challenge/. To view the 2016 MPN visit https://www.healthit.gov/sites/default/files/2016_model_privacy_notice.pdf. The Federal Register Notice announcing the challenge can be viewed here.

Public Health Oversight

- Another in ONC/OCR series on the “permitted uses” of HIPAA
  - Circumstances in which PHI and ePHI can be shared identifiably without first obtaining the individual’s written consent.
  - Treatment and Health Care Operations released February, 2016
- Public Health Oversight released December 8, 2016. Examples include
  - Collecting protected health information to monitor, prevent, and track disease and vital statistics such as birth and death records; engaging in public health interventions; and other responsibilities of authorized federal, state, or local public health agencies
  - Collecting information about the health of children who have experienced lead poisoning and tracking their neurological development over time
  - Supporting the notification of people who may have been exposed to a communicable disease that the public health department is tracking
  - Enabling employers to meet health safety reporting requirements
  - Participating in state-sponsored cancer registries

Illustrated Example, Public Health Oversight Sharing

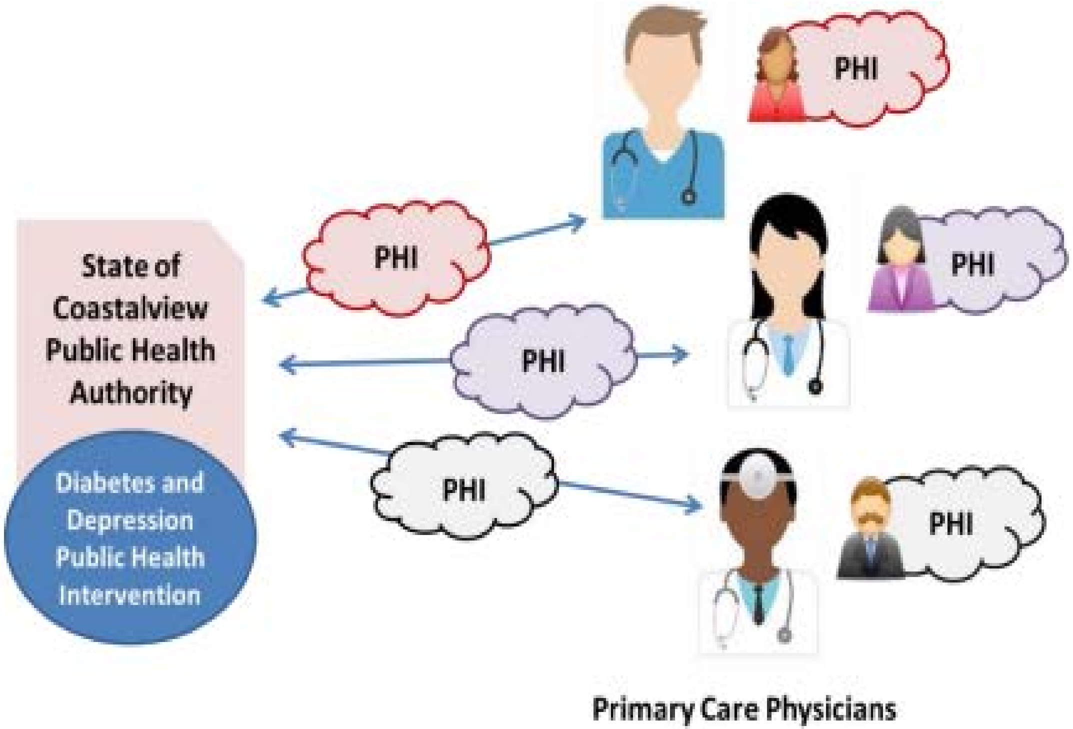

State of Coastalview Public Health Authority
Diabetes and Depression Public Health Intervention
PHI
PHI
PHI
PHI
PHI
PHI
Primary Care Physicians

Figure 5: Public Health Interventions Scenario 2

NGA Interoperability Roadmap for States

- NGA interviewed more than 90 state health policy officials, health information organizations, vendors, provider organizations and payers,
- NGA convened 30 officials and stakeholders from the federal, state and industry sectors to discuss the problem for two days
- Resulting NGA road map helps states
  - evaluate their own legal and regulatory privacy landscapes,
  - identifies best practices states can learn from each other, and
  - enables states to take decisive steps to improve the availability of electronic health information while simultaneously protecting patient privacy.
- In addition, NGA also found that key market issues are negatively impacting whether health information exchange is occurring.
- Phase 3 is currently under way. NGA will provide technical assistance to 3 states, selected competitively, who want to apply the NGA roadmap in their own environments. States are: Michigan, Illinois and Louisiana

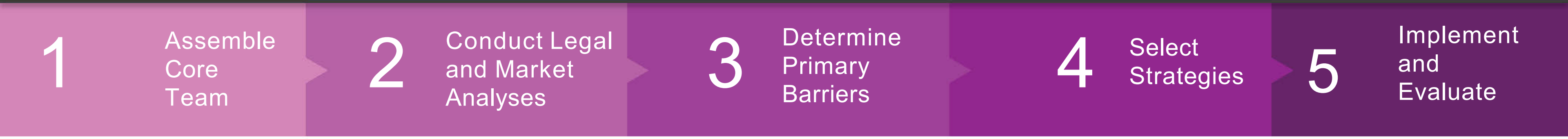
NGA Interoperability Roadmap for States

- Conundrum:
  1. Definitely a source of confusion, even w/in states
  2. Enacted for important protections for special populations
  3. Not up-to-date with Health IT
- NGA Role
  - » Grant from ONC to develop an Interoperability Roadmap for states with special attention to state privacy law and confusion
  - » Validates 1, 2 and 3, above
  - » Identifies sources of lack of interoperability as privacy confusion and market barriers.
  - » Shares tactics and strategies from successful state-based work

State Roadmap Steps and Strategies: National Governors Association (NGA)

Developed to help states evaluate and implement changes to achieve better health, better care and lower costs by increasing the flow of clinical information between providers while protecting patient privacy as a step toward nationwide interoperability.

Steps States Can Take to Increase Information Flow Between Health Care Providers


1 Assemble Core Team

2 Conduct Legal and Market Analyses

3 Determine Primary Barriers

4 Select Strategies

5 Implement and Evaluate

State Strategies to Address Legal and Market Barriers and Increase Information Flow Between Health Care Providers

State Strategies to Address Legal Barriers

Fully Align State Privacy Laws With HIPAA
Pass a law that supersedes all more restrictive state privacy laws to allow providers and hospitals to exchange information in accordance with HIPAA.

Partially Align State Privacy Laws With HIPAA
Amend select statutes to allow certain types of information, such as information exchanged electronically, to be exchanged in accordance with HIPAA.

Create Standardized Consent Forms
Create a standardized consent form that provides a "one stop" approach to gaining patient permission for sharing information.

State Guidance and Education
Issue guidance and provide education to providers about how to comply with state and federal law, including clarifying legal intent and addressing common misconceptions.

State Strategies to Address Market Barriers

Create Meaningful Economic Interests That Encourage Exchange of Health Information Create or adjust payments to incentivize exchange of health information or penalize lack of exchange.

Use Legislative, Regulatory and Contracting Authority to Bolster Exchange of Information Pass laws or issue regulations that expressly prohibit information blocking or require information exchange.

Set the Vision and Hold People Accountable
Set statewide vision for interoperable exchange of health information and use bully pulpit to elevate best practices and place pressure on those lagging behind.

Serve as Convener
Bring key stakeholders to the table to work together toward interoperable exchange of health information.

The Office of the National Coordinator for
Health Information Technology

Slide Reproduced from NGA Roadmap

Additional Information

- Full Roadmap
  - » https://www.nga.org/files/live/sites/NGA/files/pdf/2016/1612HealthCareRightInformation.pdf

  Johnson, K., Kelleher, C., Block, L., Isasi, F. (2016), National Governors Association Center for Best Practices.

- ONC Blog Post
  - » https://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/roadmap-states-addressing-privacy-policy-barriers-availability-flow-electronic-health-information

27 Months in Review

2014	October	• Chief Privacy Officer (CPO) is sworn in.
2015	January	• ONC publishes whitepaper on electronic consent management, which concludes it was not the technology. • ONC publishes 2015 Report to Congress on Information Blocking, which includes an example of a hospital refusing to comply with a patient's written request to transmit her data to another hospital.
	February	• ONC publishes revised Guide to Privacy & Security of Electronic Health Information; laid groundwork for fact sheets.
	March	• 2015 Edition of the Notice of Proposed Rulemaking (NPRM) proposes data segmentation to improve privacy compliance and reduce holes in the data.
	April	• Draft Interoperability Roadmap describes a clearer approach to consent at a policy level.
	June	• Privacy & Security Working Group (PSWG) finalizes Health Big Data Recommendations report.
	September	• ONC awards co-op funds grant to National Governors Association (NGA) to develop an interoperability roadmap for states with an emphasis on state laws on privacy.
	October	• The finalized 2015 Edition NPRM includes Data Segmentation for Privacy (DS4P), read-only Application Programming Interfaces (APIs), and right of individuals to choose unencrypted email when requesting Protected Health Information (PHI) be emailed to them. • ONC finalizes Interoperability Roadmap.
	December	• Office for Civil Rights (OCR) releases new Frequently Asked Questions (FAQs) on consumer access to their own data.
2016	February	• ONC and OCR release fact sheets on sharing PHI for Treatment and for Health Care Operations
	April	• Federal Trade Commission (FTC) releases four-agency Mobile Health Apps Interactive Tool that helps health app developers know what regulations they need to comply with (original idea was ONC's).
	June	• ONC and OCR release three videos on consumers' rights to get, share, and use their own PHI. • Joint Task Force on API work concludes.
	July	• ONC releases report to Congress on Non-Covered Entities.
	September	• ONC releases an updated Security Risk Assessment Tool.
	December	• NGA releases its interoperability roadmap for states. • ONC releases fact sheet on sharing PHI for Public Health Oversight.

The Office of the National Coordinator for Health Information Technology

@ONC_HealthIT

HHSONC

HealthIT.gov