The Office of the National Coordinator for Health Information Technology

ONC Privacy and Security Policy Update

2014 HIPAA Summit

Joy Pritts, JD
Chief Privacy Officer
Office of the National Coordinator
February 6, 2014

Office of the Chief Privacy Officer
The Office of the National Coordinator for Health Information Technology

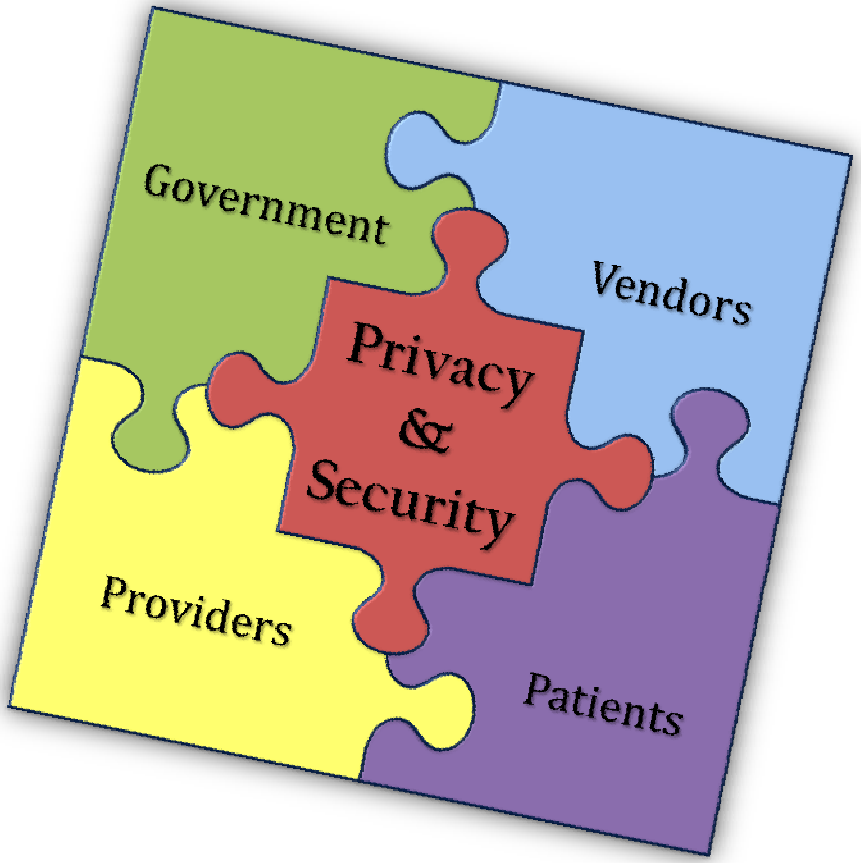
Privacy and Security: A Shared Responsibility

Government: Establish, enforce, coordinate, and communicate affordable and workable Privacy & Security regulations

Providers: Understand Privacy & Security requirements, establish and promote Privacy & Security policies and practices, train and monitor staff, and manage risk

Vendors: Integrate easy-to-use Privacy & Security features into products and provide updates as regulations evolve

Patients: Understand rights and basic means used to secure PHI



HITECH Accounting of Disclosures

The Privacy & Security Tiger Team recommendations under consideration by OCR along with other public comments:

The patient's right to a report of disclosures outside the entity or OHCA.

The patient's right to an investigation of access inside the entity

The need to balance the interest of individuals with administrative burden on covered entities

Future considerations and next steps….

Improving Critical Infrastructure Cybersecurity

- Improving Critical Infrastructure: efforts to mitigate a cybersecurity incident that could result in catastrophic national or regional effects on public health, safety, economic security, or national security
- Healthcare & public health are one of the 16 different industries comprising the critical infrastructure sector (CIS)
- Requires the development of a formal voluntary Cybersecurity Framework

NIST Cybersecurity Framework

- Overall goal is to increase sharing on cybersecurity incidents between public and private sectors
- Work with stakeholders to develop a framework to reduce cyber risks
- Provide a common language for cyber risk that can be used to help identify and prioritize actions for reducing risk

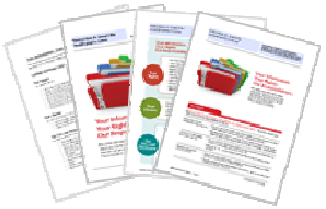
- Not intended to supersede existing sector-specific security standards
- Takes into consideration the impact of cybersecurity on privacy and civil liberties

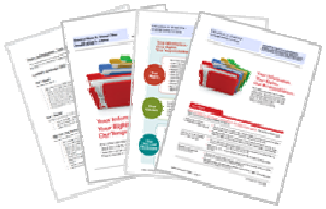
Models of Notice of Privacy Practices

The Office for Civil Rights (OCR) and Office of the National Coordinator for Health Information Technology (ONC) collaborated to develop model NPPs for covered entities to use:

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

The Office of the National Coordinator for Health Information Technology

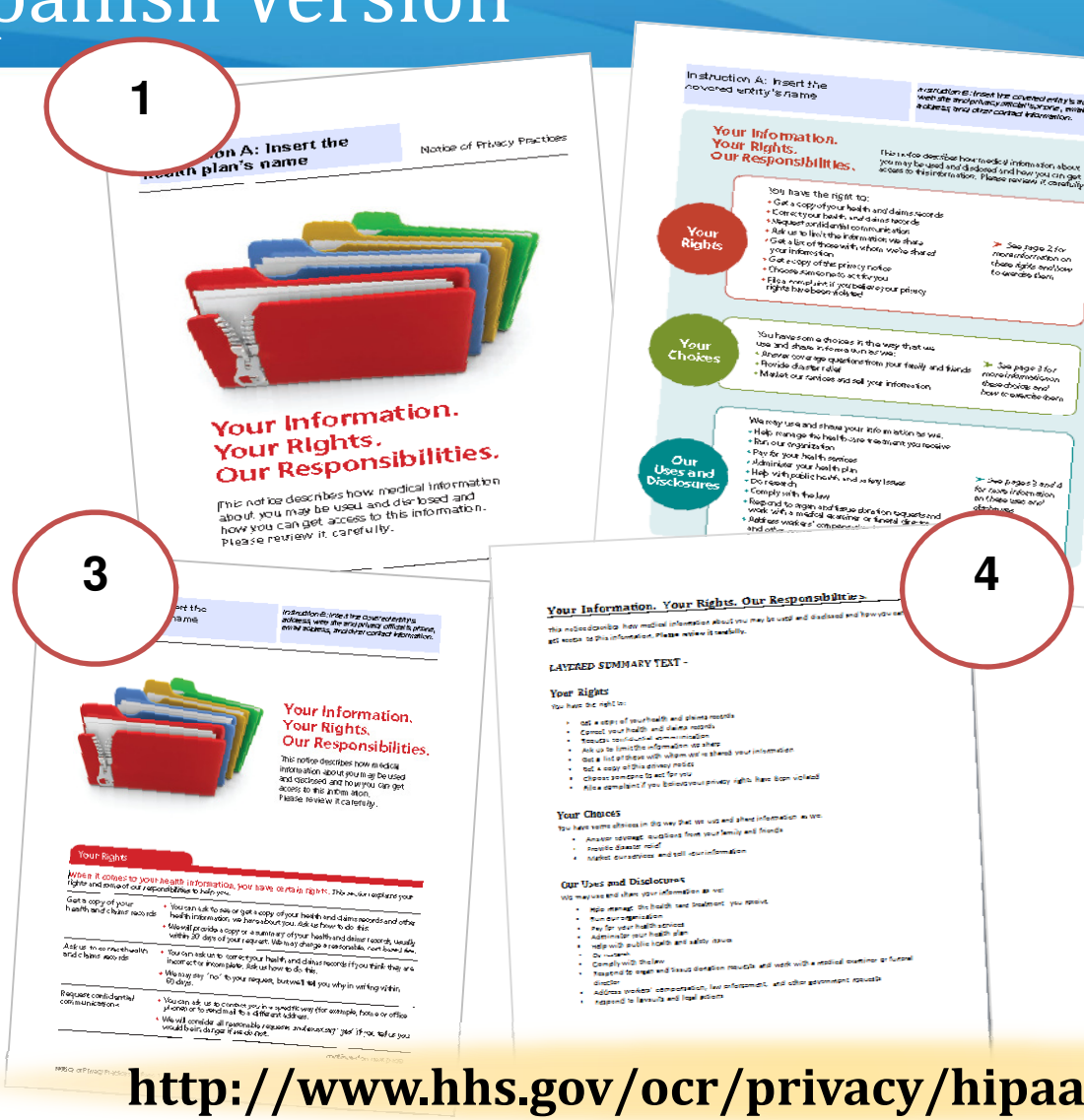




✓ One set for health plans

✓ One set for health care providers

Types of Notices Available: Coming Soon - Spanish Version



1. **Booklet**
2. **Layered Notice**
3. **Full Page**
4. **Text Only**

http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html

Cybersecure: Contingency Planning

The latest training game focuses on disaster planning, data backup and recovery and other elements of contingency planning.

Meaningful Consent Website

- Geared toward providers, health information exchange organizations (HIEs), and other health IT implementers
- Gives background on meaningful consent and ONC's eConsent Trial Project
- Provides customizable tools and resources to help you enable patients to make meaningful consent decisions

www.HealthIT.gov/meaningfulconsent

Coming Soon - Security Risk Assessment Tool

- Downloadable Risk Assessment Tool designed to guide providers through the Risk Assessment process.
- The tool includes resources to
  - understand the context of the question,
  - examples of potential impacts to PHI if requirements aren't met,
  - and includes actual safeguard language from the HIPAA Security Rule

www.HealthIT.gov/security-risk-assessment

We are all responsible for creating a culture where privacy and security are respected and valued.

Office of the Chief Privacy Officer
The Office of the National Coordinator for
Health Information Technology

HealthIT.gov