

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

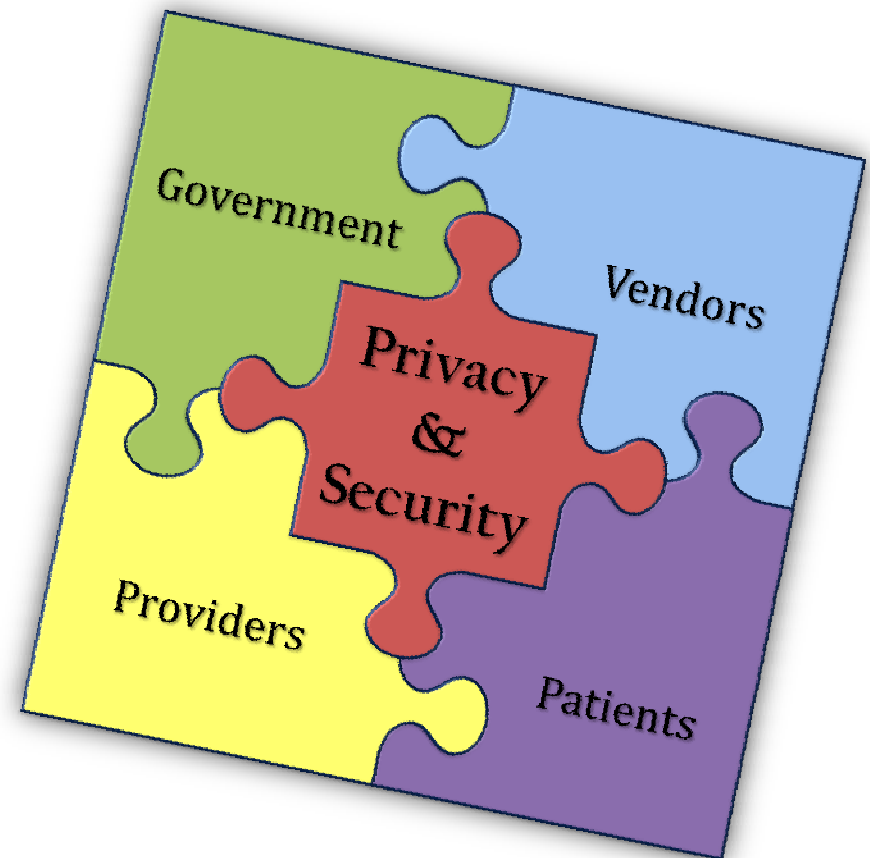


**Government:** Establish, enforce, coordinate, and communicate affordable and workable Privacy & Security regulations

**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



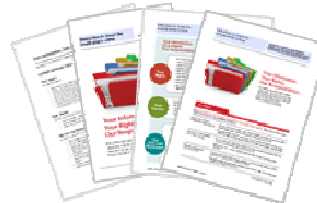
The Office for Civil Rights (OCR) and Office of the National Coordinator for Health Information Technology (ONC) collaborated to develop model NPPs for covered entities to use:



The Office of the National Coordinator for Health Information Technology



✓ One set for health plans



✓ One set for health care providers

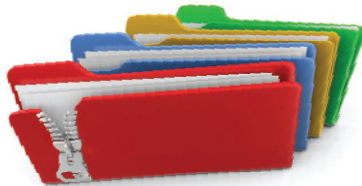


# Types of Notices Available: Coming Soon - Spanish Version



1

Instruction A: Insert the covered entity's name  
 Notice of Privacy Practices



## Your Information. Your Rights. Our Responsibilities.

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

2

Instruction A: Insert the covered entity's name

Instructions: Insert the covered entity's name in the appropriate areas marked with asterisks.

## Your Information. Your Rights. Our Responsibilities.

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

### Your Rights

- You have the right to:
  - Get a copy of your health and claims records
  - Contact your health and claims records
  - Request and limit certain information
  - Ask us to limit the information we share
  - Get a list of those with whom we share your information
  - Get a copy of this privacy notice
  - Choose whether we will notify you if we discover that your privacy rights have been violated

See page 2 for more information on these rights and how to exercise them.

### Your Choices

- You have some choices in the way that we use and share information about you:
  - Share certain information with family and friends
  - Provide disaster relief
  - Market our services and sell your information

See page 3 for more information on these choices and how to exercise them.

### Our Uses and Disclosures

- We may use and share your information to:
  - Help manage the health care we provide you
  - Run our organization
  - Pay for your health services
  - Administer your health plan
  - Help with public health and safety issues
  - Do research
  - Comply with the law
  - Respond to legal and law enforcement requests and other government requests
  - Address workers' compensation, law enforcement, and other government requests
  - Respond to lawsuits and legal actions

See page 3 for more information on these uses and disclosures.

3

Instruction A: Insert the covered entity's name

Instructions: Insert the covered entity's name in the appropriate areas marked with asterisks.



## Your Information. Your Rights. Our Responsibilities.

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

### Your Rights

When it comes to your health information, you have certain rights. This notice explains your rights and what our responsibilities are to help you.

- Get a copy of your health and claims records**
  - You can ask to see or get a copy of your health and claims records and other health information we have about you. Ask us how to do this.
  - We will provide a copy or summary of your health and claims records, usually within 30 days of your request. We may charge a reasonable cost-based fee.
- Ask us to limit the health and claims records we share**
  - You can ask us to limit your health and claims records if you think they are incorrect or incomplete. Ask us how to do this.
  - We may say "no" to your request, but we'll tell you why in writing within 60 days.
- Request confidential communications**
  - You can ask us to contact you by a specific way (for example, text or email) or to avoid us by a different address.
  - We will consider all reasonable requests and we may not be able to do all of your requests.

4

## Your Information. Your Rights. Our Responsibilities.

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

### LAYERED SUMMARY TEXT -

#### Your Rights

- You have the right to:
- Get a copy of your health and claims records
  - Contact your health and claims records
  - Request and limit certain information
  - Ask us to limit the information we share
  - Get a list of those with whom we share your information
  - Get a copy of this privacy notice
  - Choose whether we will notify you if we discover that your privacy rights have been violated
  - Ask a complaint if you believe your privacy rights have been violated

#### Your Choices

- You have some choices in the way that we use and share information about you:
- Share certain information with family and friends
  - Provide disaster relief
  - Market our services and sell your information

#### Our Uses and Disclosures

- We may use and share your information to:
- Help manage the health care we provide you
  - Run our organization
  - Pay for your health services
  - Administer your health plan
  - Help with public health and safety issues
  - Do research
  - Comply with the law
  - Respond to legal and law enforcement requests and other government requests
  - Address workers' compensation, law enforcement, and other government requests
  - Respond to lawsuits and legal actions

<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.

**Cybersecure Contingency Planning**

We aren't located in a flood plain or where there are a lot of hurricanes. We don't have to worry about any other kinds of risks, do we?

**20**  
Your Score

**make decision**

**Cybersecure Contingency Planning**

No, you only have to plan to respond to natural disasters, like tornadoes, floods and wildfires.

Not if you have insurance.

No, why waste your time planning for something that is not likely to happen.

Yes, if you don't plan for threats like fire, vandalism, or power outages, your information may be vulnerable to loss or damage.

**20**  
Your Score

**Cybersecure: Contingency Planning**

**Play the Game Now**



# 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](http://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](http://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   
12