Privacy and Security: A Shared Responsibility

Health Care Providers
- Understand Rules
- Protect and Secure Information
- Educate Staff and Patients

Government
- Promotes Trust
- Develops Policies
- Fairly Enforces Rules

Patients
- Understand Rights
- Protect Personal Information
- Be Engaged

Technology Vendors
- Embrace Privacy by Design
- Provide Convenient Technology
- Implement Standards
ONC Goal:
Inspire Confidence and Trust

Promote the Secure Use of Health IT

Information Assurance

Coordinate Development of Privacy and Security Policy

Patient Direct Access to Lab Report (CLIA)

Meaningful Use

Educate and Empower Patients and Providers

Improved Access to Health Information

View and Download Health Records

Patient Education

Enhanced Understanding of Patients

Provide Technical Assistance

Interactive Security Training

Data Segmentation for Privacy

Notice of Privacy Practices

eConsent Trial
Mobile Devices: Tips to Protect and Secure Health Information

- Use a password or other user authentication.
- Install and enable encryption.
- Install and activate wiping and/or remote disabling.
- Disable and do not install file-sharing applications.
- Install and enable a firewall.
- Install and enable security software.
- Keep security software up to date.
- Research mobile applications (apps) before downloading.
- Maintain physical control of your mobile device.
- Use adequate security to send or receive health information over public Wi-Fi networks.
- Delete all stored health information before discarding or reusing the mobile device.
Protecting Patients Rights: New OCR Resource Center at Medscape.org

Video Programs module imbedded into page for dynamic interest

OCR Educational Links, Including Mobile Device Content

HIPAA/OCR Poll Question Updated Quarterly

http://www.medscape.org/sites/advances/patients-rights
The latest training game focuses on disaster planning, data backup and recovery and other elements of contingency planning.

http://www.healthit.gov/providers-professionals/privacy-security-training-games
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:

- One set for health plans
- One set for health care providers
Types of Notices Available

1. **Booklet** – Presents the material in booklet form with design elements

2. **Layered Notice** – Presents a summary of the information on the first page, followed by the full content on the following pages

3. **Full Page** – Has the design elements found in the booklet, but is formatted for full page presentation

4. **Text Only** – Provides a text-only version of the notice

[http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html](http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html)
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
Contingency Plan

A contingency plan is a way to establish strategies for making sure you don't lose your ePHI, should your organization experience an emergency or a system failure. A contingency plan also outlines how you can restore your data. If you do suffer a data loss.
A Risk Analysis is seen as one of the most important security tasks. Performing a Risk Analysis will help you identify when and where there is a risk…

A risk where...

- Someone can compromise the **confidentiality** of your ePHI
- Someone might inappropriately alter or delete your ePHI (which affects its **integrity**), or
- Your ePHI might not be **available** when you need it

Coming Soon - Security Risk Assessment Tool

Coming Soon - Security Risk Assessment Tool

Coming Soon - Security Risk Assessment Tool

Coming Soon: Security Risk Assessment Tool

Coming Soon - Security Risk Assessment Tool

Coming Soon - Security Risk Assessment Tool

Coming Soon - Security Risk Assessment Tool

Coming Soon - Security Risk Assessment Tool

Coming Soon - Security Risk Assessment Tool

## Coming Soon - Security Risk Assessment Tool

![Security Risk Assessment Tool](image)

Coming Soon - Security Risk Assessment Tool

Providing Feedback.....

Security Risk Assessment

Comments

How can I provide comments?

ONC is asking users to provide comments regarding their use of the Security Risk Assessment (SRA) Tool. These comments will be used to improve future versions of the SRA Tool.

Comments will be accepted from Friday, March 28th to Monday, June 2nd.

[*] denotes required fields

Security Risk Assessment Tool Web Event

It's been about a month since HHS released the Security Risk Assessment (SRA) Tool on March 28th of this year. Since then ONC has received many suggestions, comments and questions. This webinar is designed to review the current state of the tool, discuss some of the known issues and ONC’s plan to address those identified issues and answer questions from users across the country.

ONC is looking forward to hearing from the SRA Tool's user community.

Register here and join us at – on April 29th 2014 from 2 – 3:30 pm EDT.
Feedback Review

• Risk Assessment versus Risk Analysis
• Windows 8.1 download issues
• Unknown publisher/digital certificate issue
• More context on likelihood and impact
• No Mac version or other platforms
• Language is unclear
• X issue on glossary
• Needs Multi-site functionality
Everyone has a role in protecting and securing health information
Download the Full Infographic Today!

http://www.healthit.gov/policy-researchers-implementers/everyone-has-role-protecting-and-securing-health-information