Building a Culture of Health Care Privacy Compliance

September 10, 2014

Presented by:

Gerry Hinkley, Partner, Pillsbury
Greg Radinsky, VP & Chief Corporate Compliance, North Shore - LIJ
Wendy Maneval, Sr. Counsel/Privacy Officer, Christiana Care

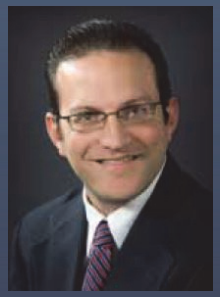
The purpose of this presentation is to inform and comment upon legal and regulatory developments in the health care industry. It is not intended, nor should it be used, as a substitute for specific legal advice inasmuch as legal counsel may only be given in response to inquiries regarding particular situations.

The materials and views expressed in this presentation are the views of the presenters and not necessarily the views of their organizations.

pillsbury

Our Speakers

Gerry Hinkley
Partner
Pillsbury Winthrop Shaw Pittman LLP
gerry.hinkley@pillsburylaw.com



Greg Radinsky
VP & Chief Corporate Compliance Officer
North Shore - LIJ Health System
gradinsk@nshs.edu

Wendy Maneval
Sr. Counsel / Privacy Officer
Christiana Care Health System
wmaneval@christianacare.org

pillsbury

Learning Objectives

- Understanding that the need is to make patient information privacy and security everybody's job
- Learn from the examples of how two leading health care organizations have moved toward a culture of privacy and security compliance
  - North Shore-LIJ Health System
    - Education/awareness
    - Internal organizational structure
    - Internal audit
    - Collaboration
  - Christiana Care Health System
    - Disciplinary structure
    - Training
    - Intra-organizational communication and collaboration

Toward Building A Culture of Compliance – Privacy and Security is *What We Are About!!*

- It starts at the top -
  - Board of Directors/Trustees
  - Chief Privacy Officer
  - Chief Security Officer
- It needs a budget
- It needs a realistic plan and priorities
- Managers need to take responsibility
- Staff need to understand there are consequences
- Physicians lead by example
- Building confidence – internally and externally

pillsbury

Building a Culture of Health Care Compliance

Greg Radinsky

Vice President & Chief Corporate Compliance Officer

North Shore-LIJ Health System

pillsbury

Goals of the Presentation

- Share Examples of Privacy Education and Awareness
- Types of Privacy/Compliance Committees
- HIPAA Audit Practices
- Tips on Collaboration
- Answer Questions

pillsbury

Types of Education and Awareness

- Annual and Pre-Employment Training
- Incorporate OCR Training Examples
- Cartoons
- Security Notices
- Education Campaigns/Intranet
- Patient Rounds

pillsbury

New Government Training Tools

News Release

FOR IMMEDIATE RELEASE
December 12, 2012

Contact: HHS Press Office
202-690-6343

New tools to help providers protect patient data in mobile devices

Launched by the U.S. Department of Health and Human Services (HHS) today, a new education initiative and set of online tools provide health care providers and organizations practical tips on ways to protect their patients' protected health information when using mobile devices such as laptops, tablets, and smartphones.

The initiative is called *Mobile Devices: Know the RISKS. Take the STEPS. PROTECT and SECURE Health Information* and is available at www.HealthIT.gov/mobiledevices. It offers educational resources such as videos, easy-to-download fact sheets, and posters to promote best ways to safeguard patient health information.

"The use of mobile health technology holds great promise in improving health and health care, but the loss of health information can have a devastating impact on the trust that patients have in their providers. It's important that these tools are used correctly," said Joy Pritts, HHS' Office of the National Coordinator for Health Information Technology (ONC) chief privacy officer. "Health care providers, administrators and their staffs must create a culture of privacy and security across their organizations to ensure the privacy and security of their patients' protected health information."

Despite providers' increasing use of using mobile technology for clinical use, research has shown that only 44 percent of survey respondents encrypt their mobile devices. Mobile device benefits—portability, size, and convenience—present a challenge when it comes to protecting and securing health information.

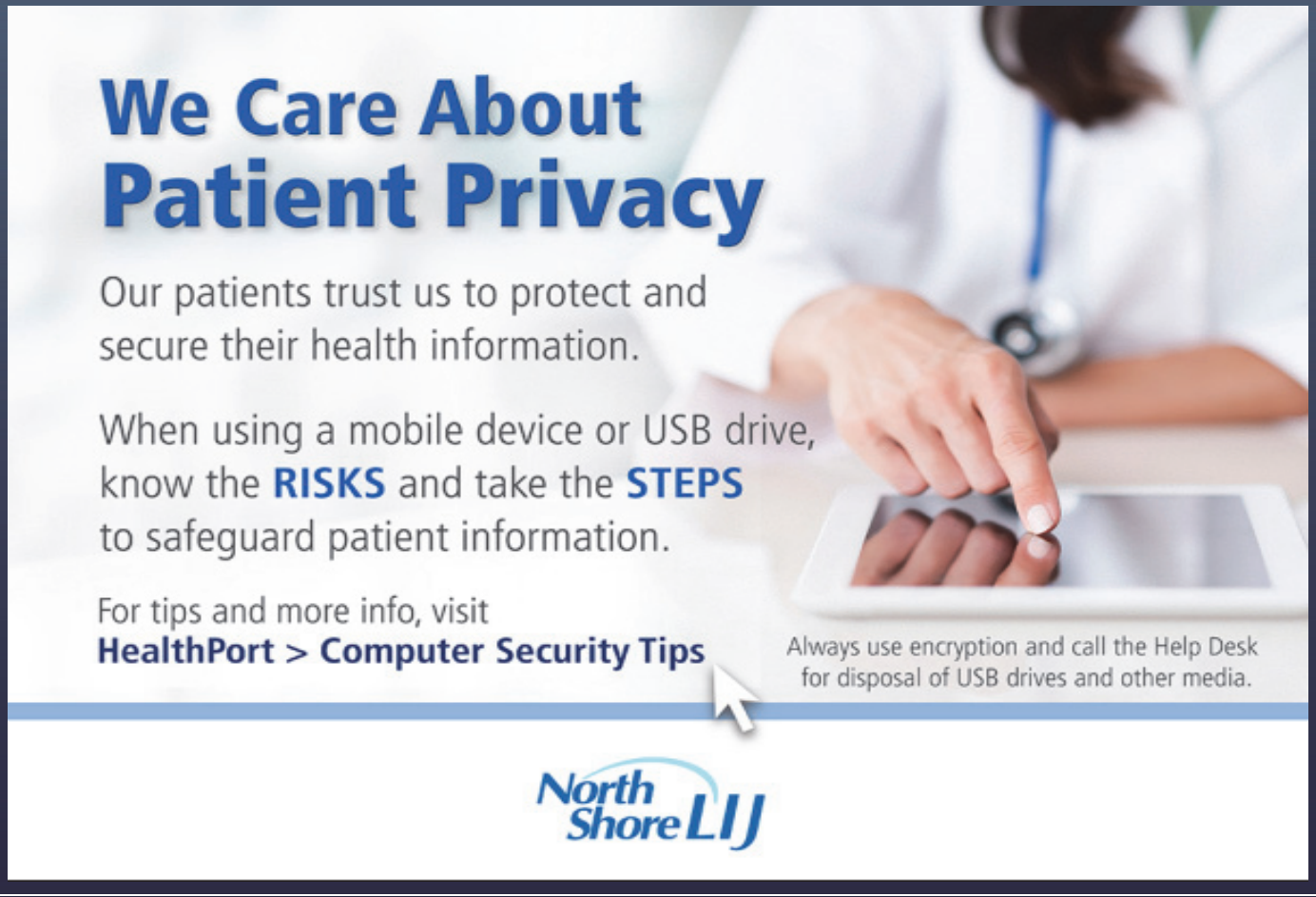
Along with theft and loss of devices, other risks, such as the inadvertent download of viruses or other malware, are top among reasons for unintentional disclosure of patient data to unauthorized users.

"We know that health care providers care deeply about patient trust and the importance of keeping health information secure and confidential," said Leon Rodriguez, director of the HHS Office for Civil Rights. "This education effort and new online resource give health care providers common sense tools to help prevent their patients' health information from falling into the wrong hands."

For more information, tips, and steps on protecting and securing health information when using a mobile device visit www.HealthIT.gov/mobiledevices.

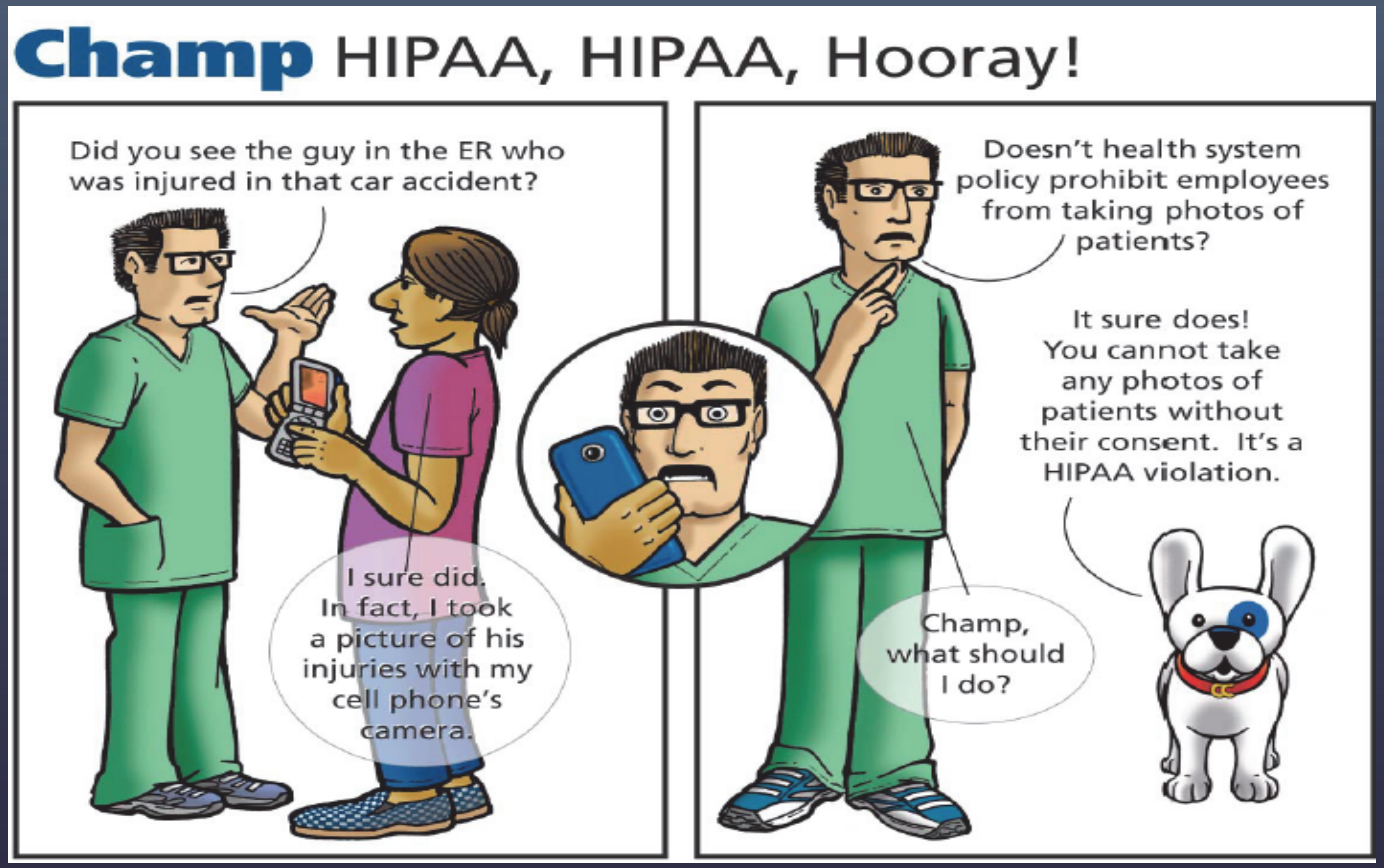
pillsbury

Sample Screensaver



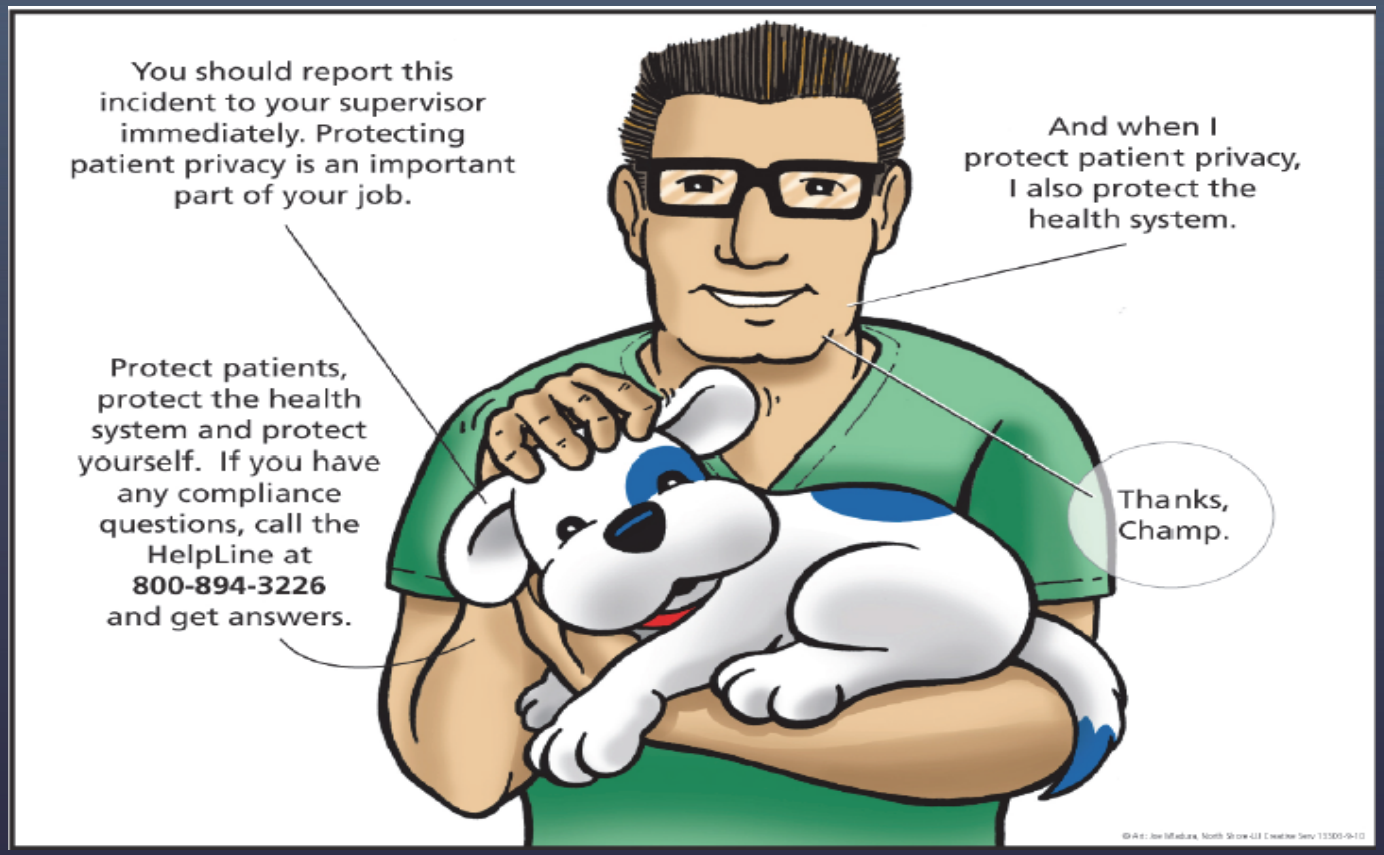
pillsbury

Sample HIPAA Education Cartoon



pillsbury

Sample HIPAA Education Cartoon (cont.)



pillsbury

Security Reminders

pillsbury

Security Reminders

pillsbury

Keep It Confidential Campaign

pillsbury

EMR Attestation of Confidentiality

Please read and Acknowledge the statement below.

North Shore – Long Island Jewish Health System ("NSLIJHS")
Electronic Health Record
ACCESS AND CONFIDENTIALITY
USER AGREEMENT

As a physician, provider, employee, student or trainee, affiliate, or volunteer at the North NSLIJHS you may have access to what this Agreement refers to as "Confidential Information" (defined below). The purpose of this Agreement is to help you understand your duties regarding Confidential information. You are required to conduct yourself in strict conformance with applicable laws including NSLIJHS policies governing Confidential information. You are required to read and abide by your principal duties in this area as explained below. If you violate any of these duties you may be subject to discipline, which might include, but is not limited to, termination of your relationship (employment, student, consulting, etc.) with NSLIJHS and to civil and criminal legal liability.

"Confidential information" includes patient information, employee information, financial information, and any other information relating to NSLIJHS, affiliated or sponsored institutions, and information proprietary to other companies or persons. You may learn or have access to some or all of this Confidential Information through the NSLIJHS computer systems to which you have access in order to provide professional care to the NSLIJHS patients (which include but are not limited to the clinical and financial information systems).

Confidential information is valuable and sensitive, and is protected by law and by strict NSLIJHS policies. The intent of those laws and policies is to assure that Confidential information remains confidential – that is, that it will be used only as necessary to accomplish NSLIJHS mission.

I understand that I will have access to electronic, printed or oral Confidential information which may include, but is not limited to information about:

- Patients (such as medical records, conversations, patient financial information, etc)
- Employees (such as medical records, employment records, salaries, etc)
- NSLIJHS facilities, affiliated or sponsored institutions' (such as financial and statistical records, strategic plans, internal reports, memos, peer review information, communications, proprietary computer programs, source code, proprietary technology, etc.)
- Third parties as it relates to NSLIJHS (such as computer programs, client and vendor proprietary information, source code, proprietary technology, etc.)

Accordingly, as a condition of, and in consideration of my access to Confidential information, I promise that:

1. I will use Confidential information only as needed by me to perform my legitimate duties as defined by my relationship (employment, student, consulting, etc.) with NSLIJHS.
a. I will not access Confidential Information for which I have no legitimate need to know (such as for patients whom I am not treating nor have any operational or billing duties); and
b. I will not in any way divulge, copy, release, alter, revise, or destroy any Confidential Information, except as properly authorized within the scope of my relationship with NSLIJHS; and
c. I will not misuse Confidential Information or carelessly handle Confidential Information; and
d. I will not replicate or disclose Confidential Information unless I am explicitly authorized to do so to perform my duties.

2. I will safeguard and will not disclose my access code(s) (e.g., passwords) that allows me to have access to Confidential Information. I accept responsibility for all activities undertaken using my access code(s) and other authorization of my access code. I agree to the following:
a. I will log off computer systems after use; and
b. I will not log on to any information system or access Confidential Information to allow another person access to such information.

3. I will report any suspicion or knowledge that I have that my access code, authorization, or any Confidential Information has been misused or disclosed without NSLIJHS authorization.

4. I will report, consistent with NSLIJHS policies and the Code of Ethical Conduct, activities by any individual that I suspect may compromise the confidentiality of Confidential Information. Reports made in good faith about suspect activities will be held in confidence to the extent possible and appropriate, including the name of the individual reporting the activities.

5. I understand that my obligation under this Agreement will continue after termination of my relationship with NSLIJHS.

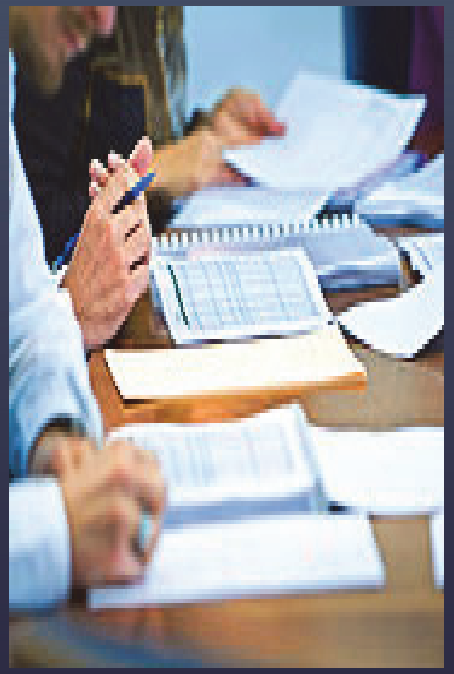
6. I understand that I have no right or ownership interest in any Confidential Information referred to in this Agreement. NSLIJHS may at any time revoke my access code, other authorization, or access to Confidential Information. At all times during my relationship with NSLIJHS, I will act in the best interest of NSLIJHS.

7. I will be responsible for my misuse or wrongful disclosure of Confidential Information and for my failure to safeguard my access code or other authorization to access Confidential Information. I understand that my failure to comply with this Agreement may also result in my loss of relationship with NSLIJHS, other disciplinary action including termination, and to personal civil and criminal legal liability

pillsbury

HIPAA Related Committees

- Board Committees
- Executive Audit and Corporate Compliance Committee
- IT Risk Governance Committee
- PHI Committee
- Patient Privacy Committee



pillsbury

Types of HIPAA Audits

- HIPAA Rounding Audits
- HIPAA Security Audits
- EMR Access Audits (e.g., investigation, VIPs)
- FairWarning® Audits

pillsbury

Sample HIPAA Education Rounding Questions

Executive Summary		
	Criteria	Risk Factor High, Medium to Low, None
1	Staff are not observed discussing confidential patient information among themselves in public areas.	
2	The patient receives and acknowledges receipt of the Notice of Privacy Practice as required.	
3	The Notice of Privacy Practices is posted in appropriate areas.	
4	Computer monitors are positioned away from public areas to avoid observation by unauthorized individuals.	
5	Paper records are stored or filed in such a way as to avoid observation by patients or visitors, or casual access by unauthorized staff.	
6	Confidential patient information is not left unattended in a printer, photocopier or fax machine, unless these devices are in a secure area. Physical access to fax machines and printers is limited to authorized staff.	
7	Patient lists, with information beyond date/address, are not readily visible by visitors.	

pillsbury

Sample HIPAA Education Rounding Questions (continued)

Executive Summary		
	Criteria	Risk Factor High, Medium to Low, None
8	Unattended Computer systems (including Computers on carts or MOWs) are appropriately logged off when not in use.	
9	Compliance Helpline Poster is posted in the area.	
10	Staff are wearing badges and badges are visible.	
11	Selected staff spoken with know whom to contact about a privacy/security complaint.	
12	Observation of paper PHI being disposed of properly in dedicated secure receptacles.	
13	Computer passwords are not visibly posted and there is no evidence of password sharing.	
14	Observation of unattended portable media devices (e.g., jump drives) in unsecure areas.	
15	Observation of Employees inappropriately requesting Social Security numbers and/or making copies of any type of photo identification.	
16	Proper disposal of electronic media devices and hardware containing PHI.	
17	Employee awareness of e-mail encryption.	

Building a Culture of Health Care Compliance

Wendy Maneval

Sr. Counsel / Privacy Officer

Christiana Care Health System

pillsbury

Designing Appropriate Sanctions for Violations

Administrative Safeguards include Workforce Training and Management (45 CFR § 164.308):

"A covered entity must provide for appropriate authorization and supervision of workforce members who work with e-PHI. A covered entity must train all workforce members regarding its security policies and procedures, and must have and apply appropriate sanctions against workforce members who violate its policies and procedures."

Audit Requirements – OCR expects organizations to adopt policies regarding sanctions for violators.

Guidelines for Sanctioning Violators

- Discipline policy should reflect the goals of the organization (to punish, deter, prevent, reform)
- *Proportionality*: “Punishment should fit the crime”
- *Uniformity*: Discipline policy should treat similar violations similarly
- *Consistency*: Violators should not be treated differently because of their role.

Many Approaches

- Zero Tolerance for Privacy Violations
- Considerations of Patient Harm
- Application of “Just Culture” Principles

pillsbury

Application of Just Culture Principles

- Emphasis on behavior choices not outcome or harm
  - Human Error → consolation
  - At-Risk Behavior → punish to deter, re-educate
  - Reckless Behavior → termination

Opportunities

- Sanctions in gray areas (when the violation is not clear)
- Failure to follow policy versus violation of regulatory requirements
- Difficulty in proving that violation occurred or the identity of violator
- Physicians versus everyone else…
- Non-employees

Defining the Scope of Access to Records and Other Medical Information

- Treatment, Payment and especially Healthcare Operations (New developments and situations that diminish the ability to recognize when they apply…)
- Who is included in the treatment team?
- Business Associates
- Minimum Necessary
- Decision-makers and Family
- Research
- Education (future providers, publications, other organizations)

Training and Refresher Courses for Employees

- Privacy Rule – 45 CFR § 164.530:

  "A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information … as necessary and appropriate for the member of the workforce to carry out their functions within the covered entity."

Training: Implementation Standards

- To each member of the workforce no later than the compliance date for the covered entity.
- Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the workforce.
- To each member of the workforce whose functions are affected by a material change in a policy or procedure – within a reasonable time after the change becomes effective.

pillsbury

Example of a Training Program: Large Organization

- New Hire Orientation Training – General education on HIPAA requirements and policies of organization.
- Confidentiality Agreement – to be signed by any individual provided with access to electronic health information – prior to first access and annually thereafter.
- Annual Electronic Training – highlighting priority issues based on experience.
- Spot Training – Training to department/unit/service regarding issue or concern that needs to be addressed.
- Regular Training – in-person training to department/unit/service regarding specific needs of workforce.
- Remedial Training – for re-education of violators – if possible, related to the violation and impact of the violation.

Fostering Communication with Employees and Departments

How to enhance the likelihood of reporting of privacy concerns:

- Improve access to Privacy Office
  - Hotline (answered by member of the Privacy Office)
  - Website
  - Email Address
  - Incident reporting system
  - Regular meetings with colleagues in Patient Relations, HIMS, Social Work, Emergency Department, etc.
- Training opportunities

Privacy is a "Team Sport"

Regular collaboration with (for example):

- Senior Leadership
- IT
- Security
- HR
- HIMSS
- Patient Relations
- Public Safety
- Social Work
- External Affairs/Communications
- Clinical Departments
- Academic Affairs
- And the rest of the organization…

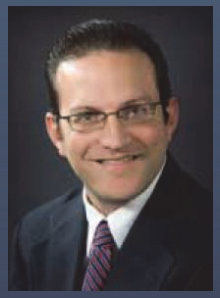
pillsbury

Questions and Answers

pillsbury

Our Speakers

Gerry Hinkley
Partner
Pillsbury Winthrop Shaw Pittman LLP
gerry.hinkley@pillsburylaw.com



Greg Radinsky
VP & Chief Corporate Compliance Officer
North Shore - LIJ Health System
gradinsk@nshs.edu

Wendy Maneval
Sr. Counsel / Privacy Officer
Christiana Care Health System
wmaneval@christianacare.org

pillsbury