Memorial Healthcare System

Shine the Light on the Importance of Audit Controls

Where were you in 2011?

- In the Tech world
  - Steve Jobs died after a long battle with cancer
  - The Guy Fawkes mask, used by Anonymous and LulzSec, became the face of hactivism
  - The iPad put tablets back in demand
- In Healthcare IT Security
  - The ARRA-HITECH impact was being felt
  - Expanding HIE, Preparing for ACOs
  - Always On SSL, BYOD, Cloud Computing, Spam, Phishing, Malware, monitoring Internet activity, encryption and DLP to protect sensitive data

Discovery – Brief Overview

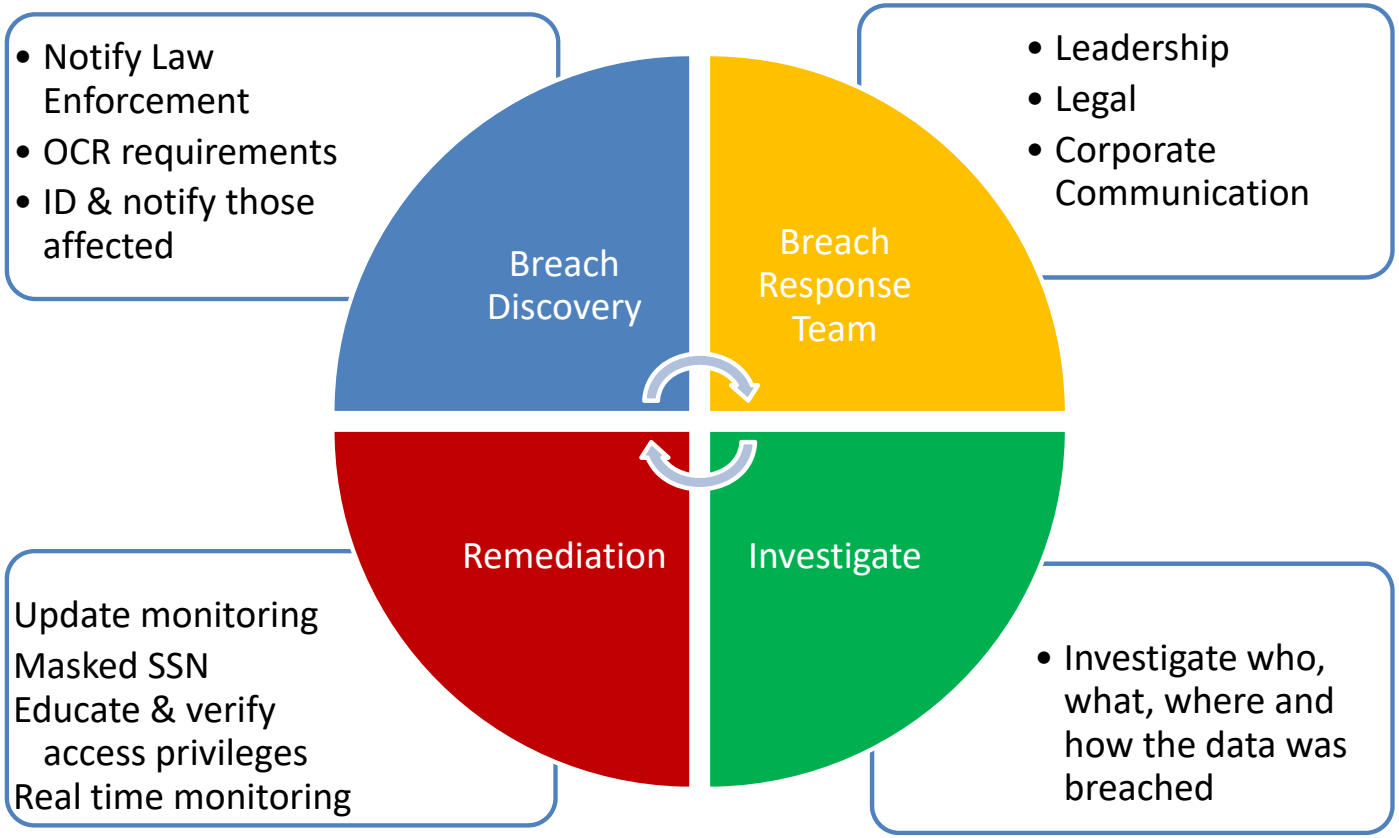
Compliance Hotline Call

- Anonymous Hotline caller
  - Co-worker writing down patient names, SSNs, and DOBs
  - Provided Evidence
  - Just purchased this practice
    - EMR was being converted

Secret Service

- Postmaster intercepted a box of 250 Green Dot cards
  - Secret Service called the names on the cards and learned that a common denominator was that they were patients at Memorial
  - Three names matched to one employee
  - Employee confessed

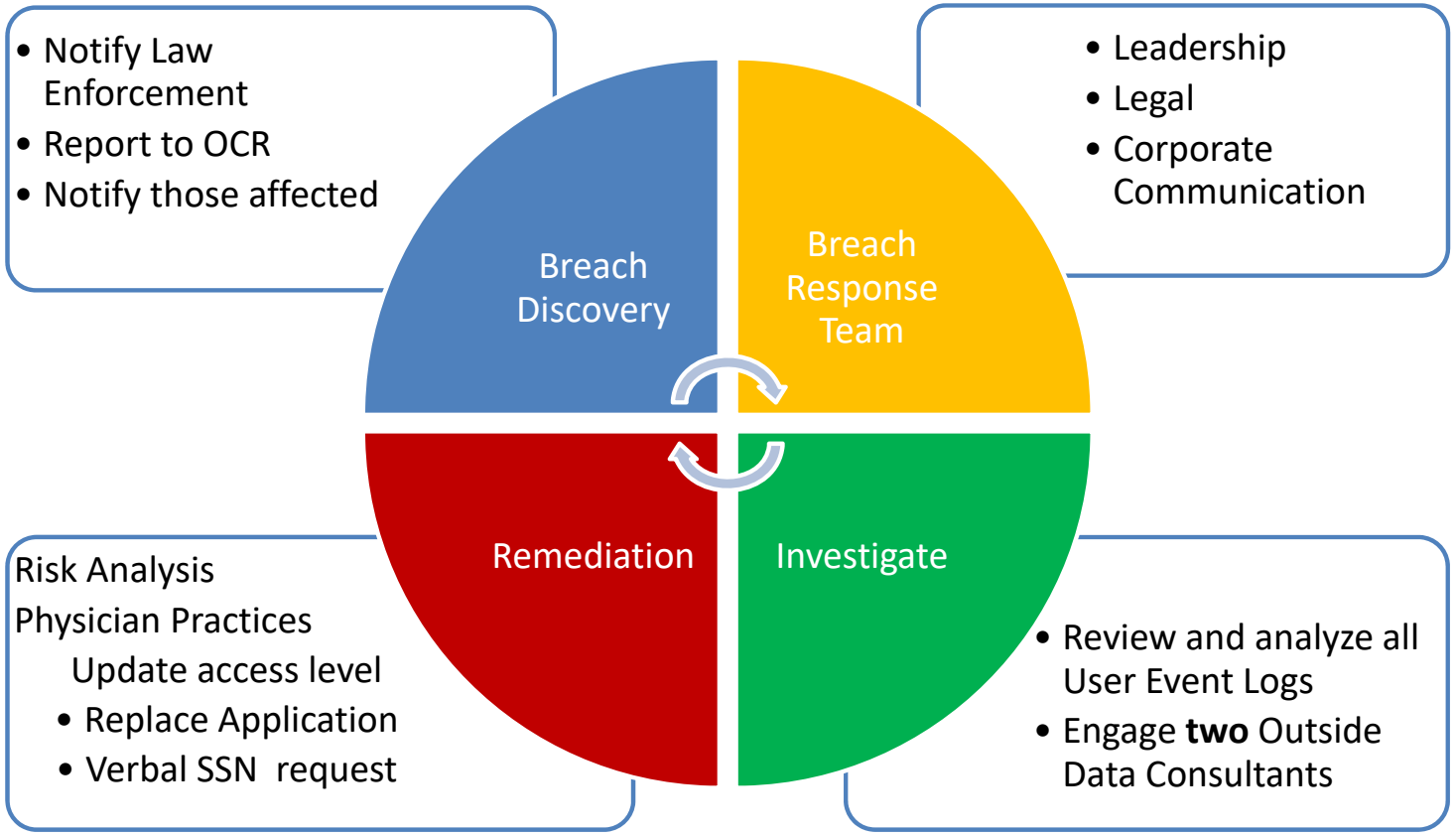
Incident Response



First Report to OCR

- April 2012
- Breach occurred from August 2011 to February 2012 (6 months)
- We reported everyone the employees ever accessed at Memorial
- ~9,500

Breach Detection
The Sweep



Second Report to OCR

- July 2012
- Affiliated Physician Offices
- Breach occurred from January 2011 to June 2012 (18 months)
- ~105,000

OCR – Initial Data Request

- December 2012

OCR – Second Letter

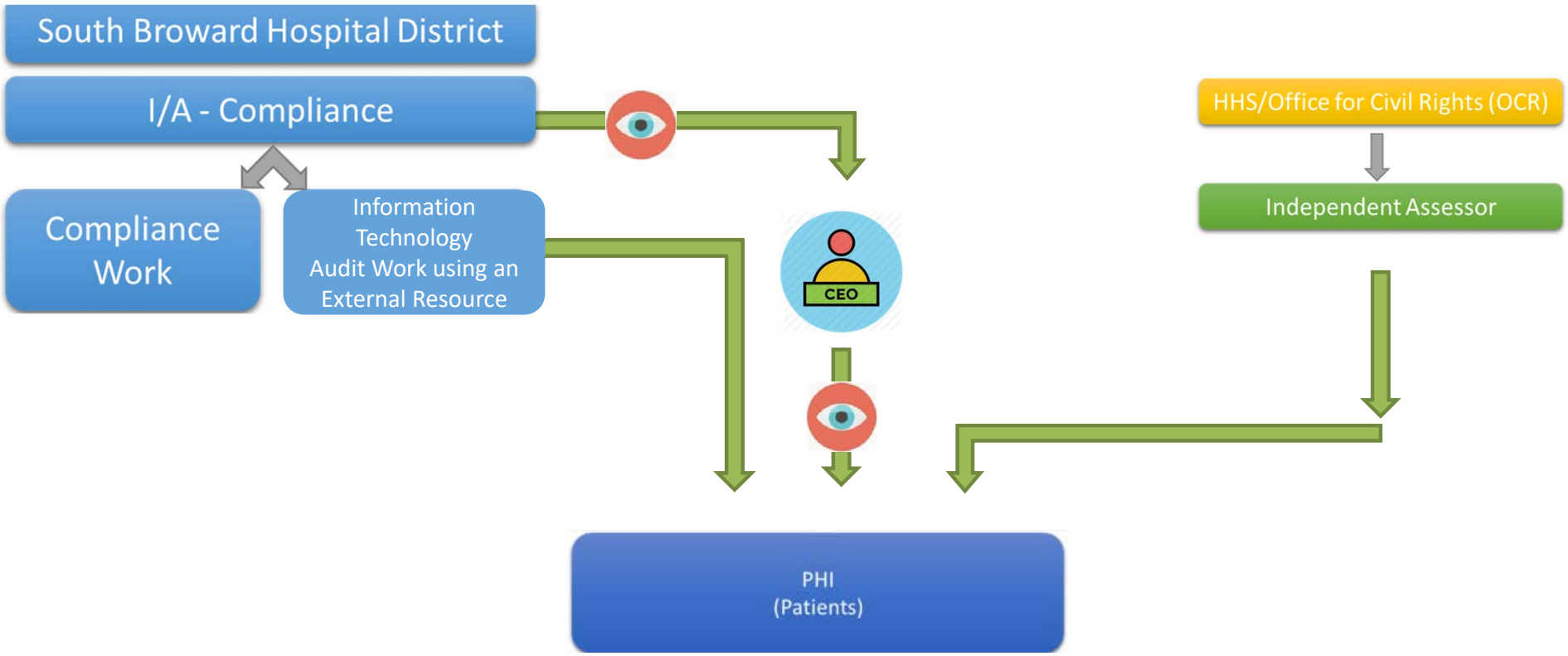
- September 2013

…

OCR – Last Letter

October 2016

Compliance's Role



MEMORIAL HEALTHCARE SYSTEM

I got this email…

Thu 2/16/2017 2:51 PM

OCR HIPAA Privacy Rule information distribution <OCR-PRIVACY-LIST@LIST.NIH.GOV> on behalf of OS OCR PrivacyList, OCR (HHS/OS) <OCRPrivacyList@HHS.GOV>

$5.5 million HIPAA settlement shines light on the importance of audit controls

To OCR-PRIVACY-LIST@LIST.NIH.GOV

You forwarded this message on 2/17/2017 10:14 AM.

HHS Office for Civil Rights in Action

February 16, 2017

$5.5 million HIPAA settlement shines light on the importance of audit controls

Memorial Healthcare Systems (MHS) has paid the U.S. Department of Health and Human Services (HHS) $5.5 million to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules and agreed to implement a robust corrective action plan. MHS is a nonprofit corporation which operates six hospitals, an urgent care center, a nursing home, and a variety of ancillary health care facilities throughout the South Florida area. MHS is also affiliated with physician offices through an Organized Health Care Arrangement (OHCA).

MHS reported to the HHS Office for Civil Rights (OCR) that the protected health information (PHI) of 115,143 individuals had been impermissibly accessed by its employees and impermissibly disclosed to affiliated physician office staff. This information consisted of the affected individuals' names, dates of birth, and social security numbers. The login credentials of a former employee of an affiliated physician's office had been used to access the ePHI maintained by MHS on a daily basis without detection from April 2011 to April 2012, affecting 80,000 individuals. Although it had workforce access policies and procedures in place, MHS failed to implement procedures with respect to reviewing, modifying and/or terminating users' right of access, as required by the HIPAA Rules. Further, MHS failed to regularly review records of information system activity on applications that maintain electronic protected health information by workforce users and users at affiliated physician practices, despite having identified this risk on several risk analyses conducted by MHS from 2007 to 2012.

The Resolution Agreement and Corrective Action Plan may be found on the OCR website at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/memorial

OCR offers helpful guidance on the importance of audit controls and audit trails at https://www.hhs.gov/sites/default/files/january-2017-cyber-newsletter.pdf

To learn more about non-discrimination and health information privacy laws, your civil rights, and privacy rights in health care and human service settings, and to find information on filing a complaint, visit us at http://www.hhs.gov/hipaa/index.html

THE PRIVACY AND SECURITY RULES
ENFORCEMENT AND PENALTIES FOR NONCOMPLIANCE

The Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) and the Security Standards for the Protection of Electronic Protected Health Information (Security Rule) establish a set of national standards for the use, disclosure, and safeguarding of an individual's health information – called protected health information – by covered entities. The Privacy Rule sets standards for the use and disclosure of protected health information by covered entities and also sets standards for providing individuals with privacy rights to understand and control how their health information is used and disclosed. The Security Rule's standards specify a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information. The Department of Health and Human Services, Office for Civil Rights (OCR), is responsible for administering and enforcing these standards and may conduct complaint investigations and compliance reviews.

Consistent with the principles for achieving compliance provided in the Privacy, Security, and Breach Notification Rules , OCR will seek the cooperation of covered entities and may provide technical assistance to help them comply voluntarily with the Privacy, Security, and Breach Notification Rules. Covered entities that fail to comply voluntarily with the standards may be subject to civil money penalties. In addition, certain violations of the Privacy, Security, and Breach Notification Rules may be subject to criminal prosecution. These penalty provisions are explained below.

Civil Money Penalties. OCR may impose a penalty on a covered entity for a failure to comply with a requirement of the Privacy, Security, and Breach Notification Rules. Penalties will vary significantly depending on factors such as the date of the violation, whether the covered entity knew or should have known of the failure to comply, or whether the covered entity's failure to comply was due to willful neglect. Penalties may not exceed a calendar year cap for multiple violations of the same requirement.

	For violations occurring prior to 2/18/2009	For violations occurring on or after 2/18/2009
Penalty Amount	Up to $100 per violation	$100 to $50,000 or more per violation
Calendar Year Cap	$25,000	$1,500,000

A penalty will not be imposed for violations in certain circumstances, such as if:

- the failure to comply was not due to willful neglect, and was corrected during a 30-day period after the entity knew or should have known the failure to comply had occurred (unless the period is extended at the discretion of OCR); or
- the U.S. Department of Justice has imposed a criminal penalty for the failure to comply (see below).

Lessons Learned

- Calendar year cap $1.5 m for *Willful Neglect*
- OCR will ask for your financial statements
- Keep a diary
- OCR will hold you to today's expectations
- You will not have an opportunity to verify accuracy of the News Release
- First big action from the OCR Atlanta, GA Office

Memorial Healthcare System

Resolution Agreement

Factual Background and Covered Conduct

On April 12, 2012, MHS submitted a breach report to HHS indicating that two MHS employees inappropriately accessed patient information, including names, dates of birth, and social security numbers. On July 11, 2012, MHS submitted an additional addendum breach report to notify HHS that during its internal investigation, it discovered addition impermissible access by 12 users at affiliated physician offices, potentially affecting another 105,646 individuals.[2] Some of these instances led to federal charges relating to selling protected health information (PHI) and filing fraudulent tax returns.

Factual Background and Covered Conduct (cont.)

MHS impermissibly disclosed the PHI of 80,000 individuals in violation of the Privacy Rule (*See* 45 C.F.R. §§160.103 and 164.502 (a)) when it provided access to such PHI to a former employee of an affiliated physician practice from April 1, 2011, to April 27, 2012.

From January 1, 2011, to June 1, 2012, MHS failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports, as required by 45 C.F .R. §164.308(a)(l)(ii)(D); and

From January 1, 2011 until June l, 2012, MHS failed to implement policies and procedures that, based upon MHS's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process, as required by 45 C.F.R. § 164.308(a)(4)(ii)(C).

Resolution Agreement

Terms and Conditions

- No Admission/No Concession
  - No admission of Liability
- Payment
  - $5.5 million
- Corrective Action Plan

Memorial Healthcare System

Corrective Action Plan

Corrective Action Plan

- Choose a designated Compliance Representative
- Internal Monitoring Plan
  - Approved by HHS
- Select and engage an Assessor
  - Third party to review our compliance with the CAP

Corrective Action Plan

Obligations

1. Risk Analysis and Risk Management Plan
2. Revision of Policies and Procedures
3. Adoption and Distribution of Policies and Procedures
4. Monitoring
5. External Assessments
6. Internal Reporting
7. Annual Reports

Memorial's Patient Privacy Video