BEAUTY & THE BREACHES

“ONE ORGANIZATION’S JOURNEY TOWARDS A CULTURE OF CONFIDENTIALITY”

PRESENTED BY
MEREDITH R. HARPER, MHSA, CHC, CHPC. HCISPP, ITIL, CISM

TRANSFORMATIONAL LEADER | INSPIRATION BROKER | SPEAKER | ADVISOR
THE ECOSYSTEM

- $6 Billion in Revenues
- $200 Million in uncompensated care
- 6 Acute Care Facilities (Approx. 2500+ beds)
- 60+ Physician Practices
- Substance Abuse & Behavioral Health Facility
- Research Program
- Specialty Centers & Institutes
- Approx. 31,000 workforce members
- 1300+ Member Medical Group
- 1000+ Member Physician Network
- 30+ Primary Care Centers
- Health Plan
- Home Health & Hospice Division
- Retail Pharmacy Division
- Optical Care Division
- Occupational Health
- Long Term Care Facility & Extended Care Division
OUR CULTURE OF CONFIDENTIALITY

Technology

Process

People

Executive Leadership & Board Commitment
BREACH #1 (2010)

PHYSICIAN’S ASSISTANT LEAVES OFFICE DOOR OPEN SO HIS SECRETARY CAN GET PEANUTS TO SNACK ON WHILE HE WAS AT A MEETING. HIS UNENCRYPTED NON-IT PURCHASED LAPTOP WAS STOLEN ALONG WITH THE PATIENT INFORMATION OF APPROXIMATELY 3000 PATIENTS.
OUR RESPONSE

• Reported this incident to the CEO, COO & Board alerting them that this will be a media reportable data breach

• Pulled together loosely developed teams to respond to the data breach with no external breach support

• Conducted a Root-Cause Analysis to determine the program gaps and support necessary to strengthen the privacy & security program

• Effectively shared with the Executive Leadership that this is more “cultural” than it is “procedural”
RESTRUCTURED PROGRAM

Information Privacy Services

Privacy & Security Risk Management Services

Information Privacy & Security Office

Network & Information Security Services

Identity & Access Management Services
RESTRUCTURED PROGRAM

Information Privacy Services
- HIPAA privacy education & training
- Investigations
- Privacy monitoring & audits
- Third party privacy risk assessment & mitigation
- Business Associate Program Management
- Enterprise wide internal consultants on HIPAA/HITECH regulations and their application in the HFHS environment

Information & Network Security Services
- Security advisory services
- Security requirement definition
- Network security reviews & configurations
- Technical security assessments
- Security risk exception approvals
- PCI compliance operations & sustainability
- Security advisory services
- Incident response & forensic investigations
Privacy & Security Risk Management Services
- Social Engineering Program & Penetration Testing
- 3rd party risk assessments
- Meaningful use assessments
- PCI assessments (project, process and IT risk assessments)
- Risk exception reviews, assessments
- Risk convergence reporting & management
- GRC administration & governance
- Internal audits, external audit coordination & risk advisory services

Identity & Access Management Services
- Lifecycle management of user identity objects
- Creation, modification & termination of user logon accounts for systems and services across the enterprise
- Participates in audits, risk reviews, and testing
- Intake an entitlement of Access Requests
- Governance over all user identity objects
Any routine investigations and incidents that may result in a breach must be forwarded to the IPSO for a Code A(ssessment) and potential Code B(reach) Alert.

Investigations are led by the IPSO in conjunction with operational management and Human Resources.

All investigative documentation (i.e., notes, interview transcripts, audit logs, etc.) should be stored in our centralized repository to ensure the ability for metric reporting and auditing.

Corrective Action always recommended by the IPSO in accordance with the outcome of the investigation.

Re-education required for the entire department within 30 days of investigation closure not just the offender.
Enterprise Privacy & Security Council

- The oversight council that approves System policies and procedures related to privacy & security regulations

Code B Alert Team

- The rapid-response workgroup established to centrally respond and manage all System data breaches

Office for Civil Rights Response Team

- Reviews all OCR data requests related to privacy & security violations and respond on behalf of the System and/or specific business unit
BREACH #2 (2011)

PHARMACY RESIDENT LOST HIS UNENCRYPTED FLASH DRIVE IN THE MCDONALD’S PARKING LOT. THE FLASH DRIVE STORED A SPREADSHEET OF COMPILED PATIENT INFORMATION OF APPROXIMATELY 4000 PATIENTS.
OUR RESPONSE

• Reported this incident to the CEO, COO & Board
  • Compared the list of affected patients to see any patients were impacted by the first breach…we did!
  • Immediately called the COO and informed him that he will have the pleasure of calling these patients directly, along with my support.

• Realized that we needed help and contacted an external breach response partner that assisted in decreasing our response and notification time: **56 days to 18 days**

• Conducted a Root-Cause Analysis to determine the program gaps

• Reinforced with the Executive Leadership that this is more “cultural” than it is “procedural”
**CODE B(REACH) ALERT PROGRAM**

**Issued & managed by the IPSO for all media reportable data breaches or data breaches with significant risk**

**Branded communication plan consistently utilized throughout the system and managed corporately instead of at the business unit level**

**External:** Includes the notification to the prominent media outlets, OCR or any other external agencies

**Internal:** Typically includes a copy of the communication to the patients, FAQs about the breach and instructions for forwarding patient inquiries to toll-free call center

**Requires immediate attention by all System leadership and should be shared with staff for a 90 day period**

**Code A(assessment) Alert**

**Alerts issued by the IPSO led by the CIPSO**

**Limited to the IPSO, PR, Legal Affairs, Risk Finance & Insurance**

**Provides a summary and initial analysis of potential data breach**

**Includes initial data analysis culminating in an official breach risk assessment to determine if an actual breach has occurred**
ICOMPLY PROGRAM

Branded System wide program coordinated by the IPSO to safeguard “system” information

• Phase I: Targeted portable storage devices
• Phase II: Targeted “culture” through educational modules
• Phase III: Focused on reducing our “unsecured” printer footprint
• Phase IV: Targeted the culture again to reinforce HITECH/Omnibus
• Phase V: BYOD & Mobile Device Management
• Phase VI: Vendor Management Risk Management Program
• Phase VII: Cybersecurity Program Maturity Assessment
• Phase VIII: Why iComply? Video Series
• Phase IX: Threat Intelligence Sharing Initiatives
• Phase X: Multi-Factor Authentication
FDA APPROVED IMAC DEVICE WAS STOLEN FROM A SECURED INFECTIOUS DISEASE RESEARCH LAB AS A RESULT OF A DOOR BEING PROPPED OPEN WHILE THE EMPLOYEE RAN TO THE RESTROOM. THIS DEVICE STORED THE TESTING RESULTS FOR 520 HIV/AIDS PATIENTS.
OUR RESPONSE

• Reported this incident to the CEO, COO & Board
  • Compared the list of affected patients to see if we had any frequent flyers…we didn’t! Thank God!

• Offered an internal reward of $5000 for the return of the device

• Required the Research Administrator to co-sign the notification letter to the affected patients

• Conducted a Root-Cause Analysis again to determine the program gaps

• Reinforced with the Executive Leadership that this is more “cultural” than it is “procedural” and communicated such to the all workforce members
COMMUNICATION & EDUCATION

Our Workforce
• Morning Post Messages & System Emails – Scheduled to deliver key privacy & security messages
• Annual Mandatory Education – iComply & Job Specific
• Privacy & Security refresher trainings conducted by the IPSO team
• Manager’s Update – Monthly email to all leaders detailing key messages

Our Board Members
• Quarterly privacy & security Board updates
• Updates to the Trustee newsletter

Our Patients & Communities
• Intranet Webpage, Internet Webpage & Social Media Sites
BREACH #4 (2013)

A STORAGE FACILITY (BAA) EXPERIENCED A THEFT WHERE RADIOLOGY FILMS SELECTED FOR SMELTING WERE STOLEN FROM THE LOADING DOCK EXPOSING THE PHI OF 15,000+ PATIENTS.
OUR RESPONSE

• Activated the Code B Alert Program to address our largest breach to date

• Worked with the business associate to ensure their practices were on par

• Conducted a Root-Cause Analysis related to the management of our business associates to determine gaps

• Revised existing programs and embedded them into enterprise risk workflows
## REVISED BUSINESS ASSOCIATE PROGRAM

**Inventory**
- Conducted enterprise wide inventory of all business associates
  - Current total approx. 1650+

**Risk Rank**
- Risk ranked each business associate
  - Type of Data
  - Services Performed
  - Disclosures
  - Network Connections

**Manage**
- Implemented management plan to ensure contract & BA compliance
  - BA Education
  - Signature Authority
  - Terminations
Embedded our “Risk Program” into the contract execution and RFP processes

- Identify standards & risks through survey, assessment & Audits
- Analyze & categorize risks to assist with prioritization
- Prioritize & rate risks based on likelihood of occurrence and impact
- Respond, remediate or transfer risks to an acceptable level of risk
- Monitor & continue to identify new risks as they become evident
- Report risks & continually monitor existing risks for potential changes
BREACH #5 (2014)

PHYSICIAN LOST AN UNENCRYPTED FLASH DRIVE EXPOSING THE PHI OF 2,336 PATIENTS. PHYSICIAN VIOLATED ICOMPLY POLICY BY PURCHASING, USING & SHARING AN UNENCRYPTED FLASH DRIVE.
MY RESPONSE...LITERALLY!

• WHAT? WTHeck!!!!!

• HAVEN’T WE BEEN HERE BEFORE?

• YOU GOT TO BE KIDDIN’ ME!

On a serious note, this proved that education...education...education has to be a part of your program and defense strategy.

No amount of technology would solve good people who do the absolute wrong thing!
INCREASED WORKFORCE TRAINING

**Increased** Morning Post Messages & System Emails – Scheduled to deliver key privacy & security messages weekly

**Created** physician specific education to support our provider workforce team members

Continued Privacy & Security refresher training schedule conducted by the IPSO team

**Created** a iComply Corner in every Manager’s Update – Monthly email to all leaders detailing key messages

**Created** “Why iComply” video series featuring hospital CEOs and Executive leadership explaining why “they comply”.
QUESTIONS

Meredith R. Harper, CHC, CHPC, HCISPP, ITIL, CISM
Transformational Leader | Inspiration Broker | Speaker | Advisor

www.linkedin.com/in/deputyciso