Using Tracer Methodology to Reduce Breaches

Margret Amatayakul,

MBA, RHIA, CHPS, CPHIT, CPEHR, FHIMSS

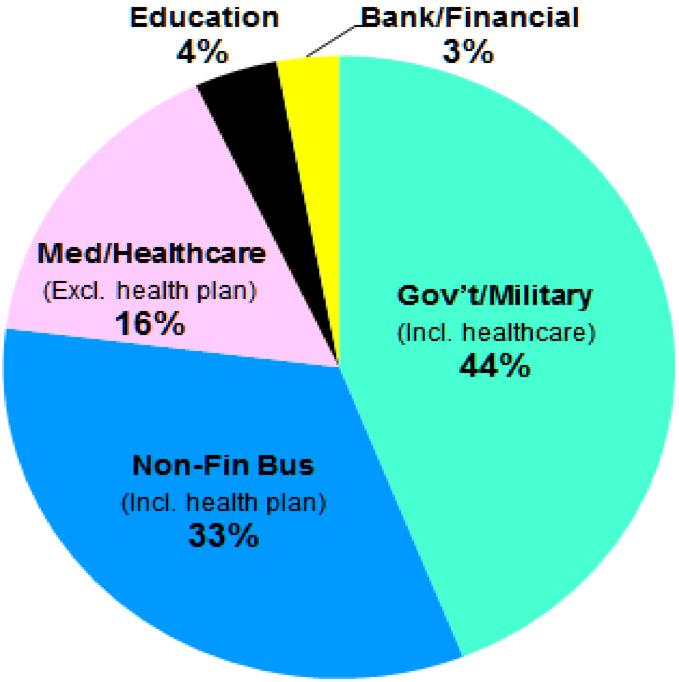
Margret\A Consulting, LLC

Agenda

- Security Trends
- Being Proactive To Reduce Likelihood of Breaches
- Tracer Methodology To Detect and Reduce Risk
- Q and A

All-Industry Breaches

- **Identity Theft Resource Center (2011):** 419 breaches affected 22.9 million reported records (48% of reports did not identify number of records)
  - Hack attacks were leading cause (26%)
  - Lost data storage devices, laptops, or paper records were second largest (18%)
  - Non-financial and healthcare groups saw greatest incidence of insider theft
  - Non-financial businesses (small retail) were target of greatest number of hack attacks, with remote access representing 71% of attack pathways
  - In 81% of records breached, SSNs included



- **Verizon RISK Team 2011 report with U.S. Secret Service found similar results**

Healthcare Breaches Y/E 2011

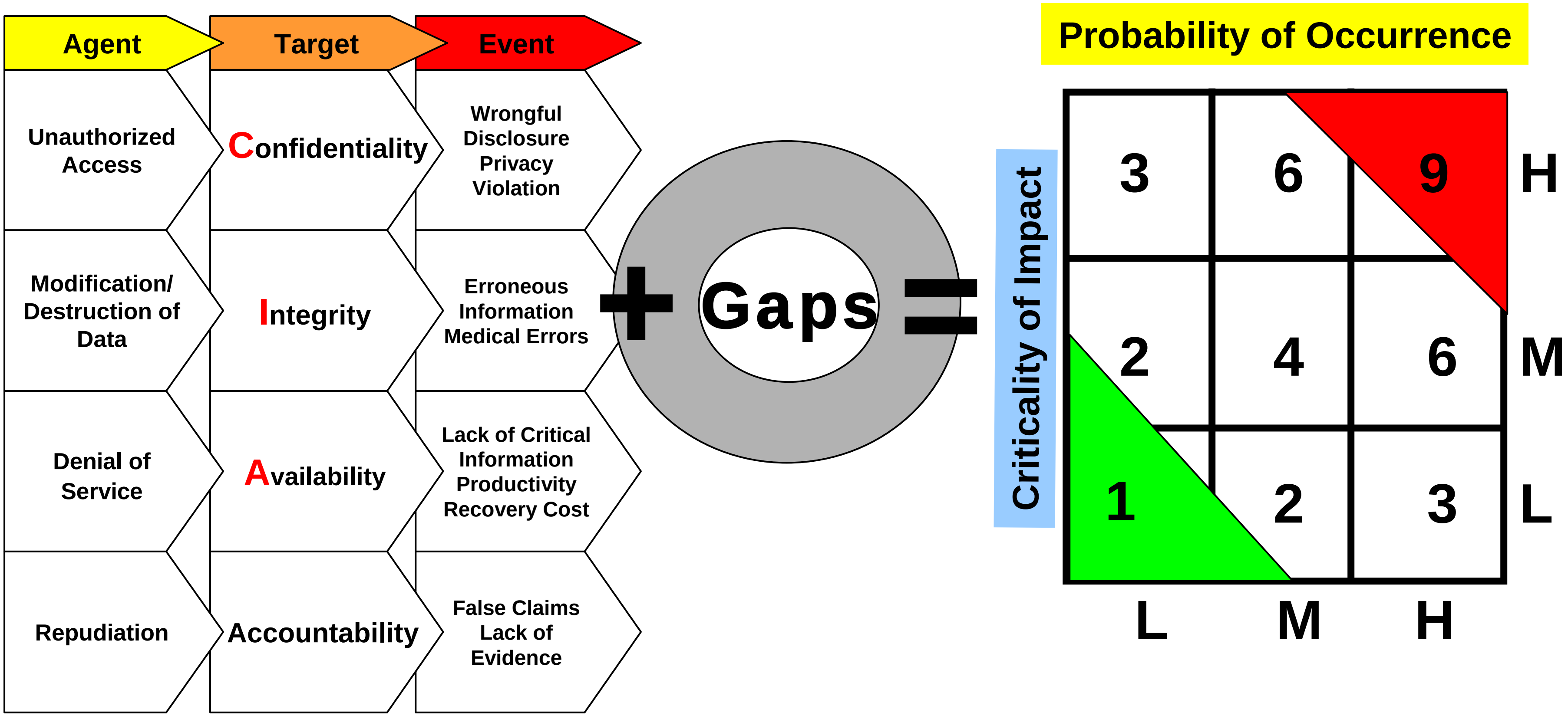
- **2009-2010 OCR Annual Report to Congress** 252 Reports;
  - 7.8 million individuals impacted
  - Theft of paper and electronic media
- **2011 HIMSS Security Survey** (Released Nov. 2, 2011)
  - Co-sponsored with MGMA; incl. 38% medical groups
  - 25% no risk analysis; 49% do annually, 21% do bi-annually
  - 77% reported 1-3 cases of medical identity theft in last year
  - 31% no back up encryption; firewalls, then access controls
  - Security accounts for 1%-3% of most IT budgets
- **Second Annual Benchmark Study on Patient Privacy & Data Security, Ponemon Institute**
  - 32% increase in reports over 2010 sample
  - Discovery of breaches by patients dropped from 41% to 35%
  - Threat of audits affecting changes; encryption most often added, but 29% say stronger access controls not a priority

Security Audit, Assessment, Risk Analysis

- **Audit** = overview of security systems and processes to determine *existence of controls*
- **Assessment** = identification of vulnerabilities in security systems and processes to *assess controls*
- **Risk analysis** = couples identification of vulnerabilities with known or potential threats to describe the probability (or likelihood) that a threat would exploit a vulnerability and to assess the criticality of impact (or level of harm) to *select and implement most effective controls*
- Risk analysis tends to be more proactive; where audit and assessment are more retrospective

Security Risk Analysis

Threats + Vulnerabilities = Risk



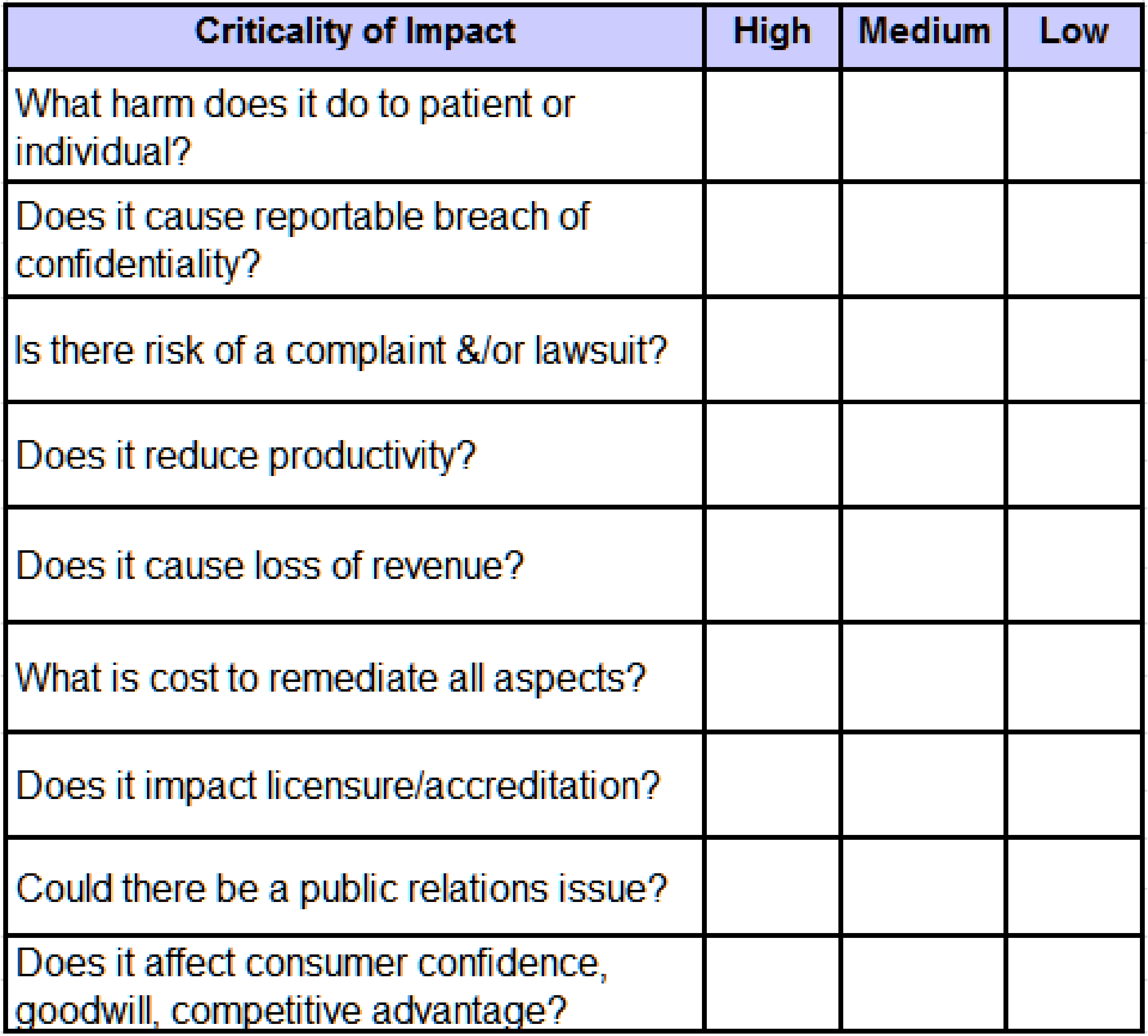
Agent	Target	Event
Unauthorized Access	Confidentiality	Wrongful Disclosure Privacy Violation
Modification/ Destruction of Data	Integrity	Erroneous Information Medical Errors
Denial of Service	Availability	Lack of Critical Information Productivity Recovery Cost
Repudiation	Accountability	False Claims Lack of Evidence

Probability of Occurrence

Criticality of Impact

	L	M	H
H	3	6	9
M	2	4	6
L	1	2	3

Probability of Occurrence	High	Medium	Low
Has it happened before:			
■ Here?			
■ Other health care?			
■ Other industries?			
How frequently does it occur:			
■ Here?			
■ Other health care?			
■ Other industries?			
Does threat source have:			
■ High access, knowledge, motivation?			
■ Predictability, forewarning?			
■ Known speed of onset, spread, duration?			
Are controls available to:			
■ Prevent?			
■ Deter?			
■ Detect?			
■ React?			
■ Recover?			



Criticality of Impact	High	Medium	Low
What harm does it do to patient or individual?			
Does it cause reportable breach of confidentiality?			
Is there risk of a complaint &/or lawsuit?			
Does it reduce productivity?			
Does it cause loss of revenue?			
What is cost to remediate all aspects?			
Does it impact licensure/accreditation?			
Could there be a public relations issue?			
Does it affect consumer confidence, goodwill, competitive advantage?			

Tracer Methodology

- **The Joint Commission** utilizes as an evaluation method in which onsite surveyors select a patient and use the health record as a roadmap to move through an organization assessing and evaluating compliance with standards and systems of providing care
  - *Tracer Methodology for Continuous Systems Improvement* offers insights on how to use this tool proactively
  - Lean, Six Sigma, and other continuous quality improvement (CQI) strategies apply as well

Applying Tracers To Breaches

- Tracing the flow of *known* breaches helps determine the source
- But, is not proactive/preventive; and may not necessarily *predict* future breaches
- Applying tracers periodically to high risk areas will help *pinpoint areas for improvement*

1. Identify High Risk Areas

- Areas of previous breaches for the organization
- Areas of identified vulnerabilities for the organization, even after controls implemented
- Areas of new threats, such as new management, use of new technology
- Any new flow or new uses of PHI or other sensitive information for the organization
- Areas of breaches as identified through trends data in both health care and general

Examples of High Risk Areas

- Back up processing area
- Cashier
- Data center
- Dead storage
- Delivery area
- Human resources
- Paper scanning, faxing, duplication, and destruction areas
- Patient accounting
- Patient registration
- Staff lounges
- Trash area

Examples of High Risk Processes

- Billing
- Coding
- Health information exchange
- Privacy rights processing
  - Accounting for disclosures
  - Disclosures to relatives and other caregivers
  - Quality measurement and reporting
  - Requests for restrictions
  - Research
- Release of information
- Remote access
- Transcription
- Unsecured email
- Web portal
- In general,
  - Outsourced functions
  - Use of portable devices
  - Management of portable media
  - Processes were staff have access to all patients

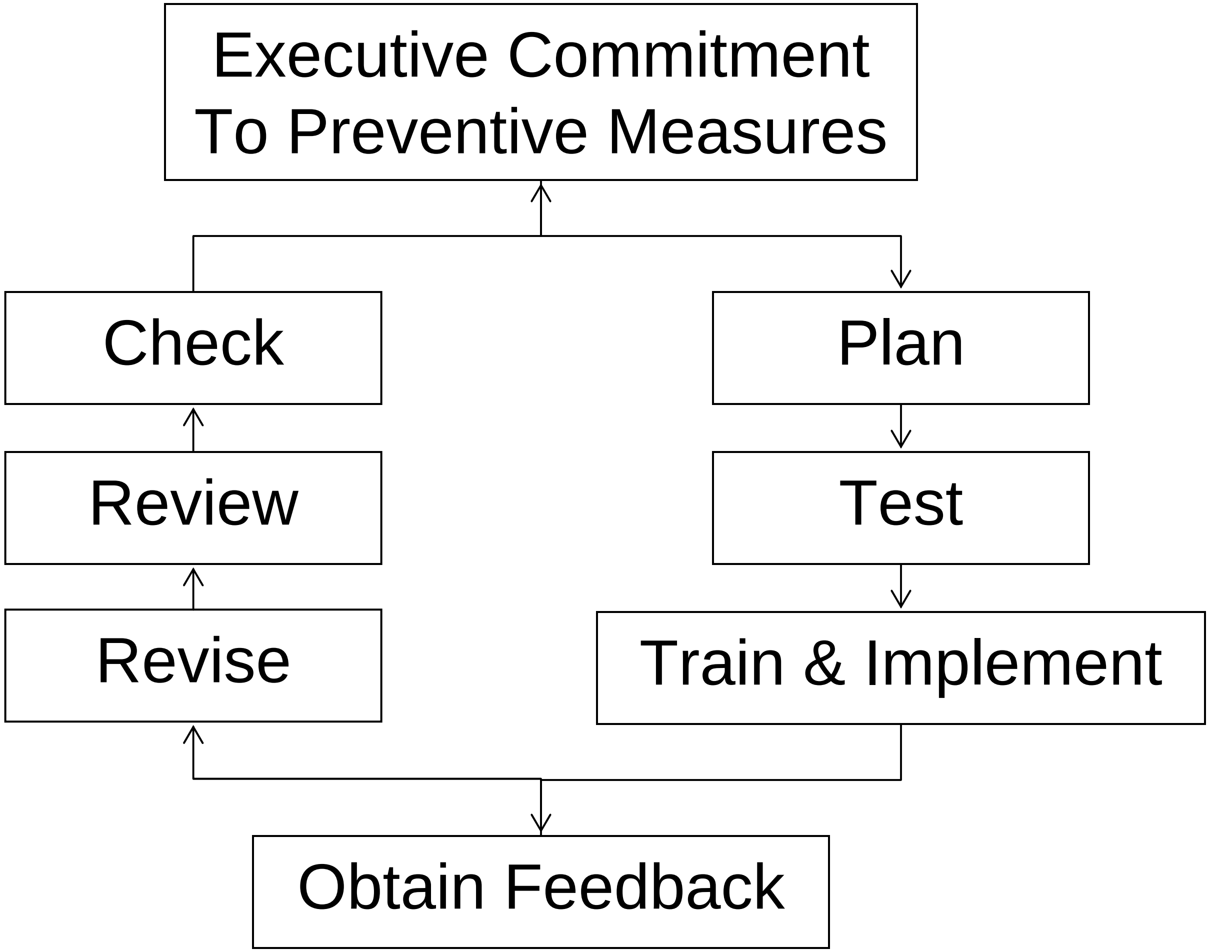
2. Trace Process with Workflow Tools

- The Joint Commission tracer methodology takes a record and traces ***back*** the experience of a patient
  - Use this strategy when attempting to determine the cause of a breach
  - For a risk area that is a new PHI flow or changes an existing flow (e.g., automation), trace ***forward***
- Use **flowcharts** for structured processes to evaluate potential sources of breaches
- Use **mind mapping** tools to evaluate unstructured processes

3. Identify Mitigation Strategies

- Once source of breach or potential breach is identified, determine applicable mitigation strategy or strategies:
  - Training
    - Knowledge
    - Skills
    - Reinforcement
  - Workflow redesign
  - Resources
    - Staff
    - Budget
  - Technology
    - Existence of needed interfaces, security control updates, de-identification tools, etc.
    - Configuration
    - Usability
    - Adoption
    - Monitoring

4. Implement Mitigation Strategies



Executive Commitment To Preventive Measures

Check

Plan

Review

Test

Revise

Train & Implement

Obtain Feedback

Additional Strategies

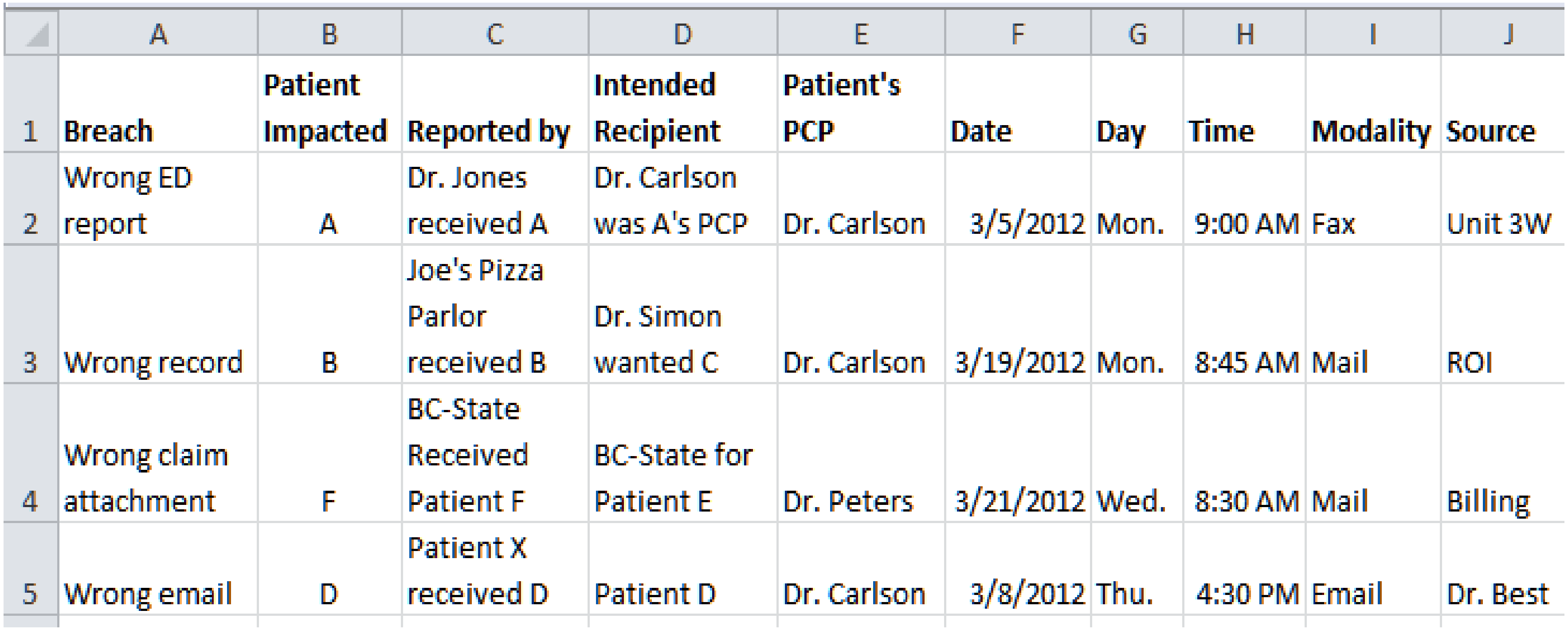
- Teachable moments
  - Talk about any breach from the perspective of lessons learned
  - Solicit input from staff on ways to reduce the risk of breaches
  - Attempt to replace a culture of “blame” with a culture of support
- Explicitly state expectations
  - In contracts require unique access controls for every individual (not role), specific audit logging procedures, that a penetration test is performed annually, use specific level of encryption, etc.
  - Write a sanction policy that can be and is applied fairly and specifies, through example, types of actions not permitted
- Technology
  - Implement technology that aids privacy and security
  - Teach people how to use security controls in an open and reassuring manner

Scenario

- A hospital was experiencing a significant number of individual breaches, sometimes reported by patients and other times reported by providers, health plans, or others. They suspected the problem stemmed from the release of information area, which was outsourced. They contacted their vendor to step up controls, retrain staff, and institute regular reporting
- The problem of individual breaches, however, continued

Tracer Applied to Scenario

- A catalogue of individual breaches was created



	A	B	C	D	E	F	G	H	I	J
1	Breach	Patient Impacted	Reported by	Intended Recipient	Patient's PCP	Date	Day	Time	Modality	Source
2	Wrong ED report	A	Dr. Jones received A	Dr. Carlson was A's PCP	Dr. Carlson	3/5/2012	Mon.	9:00 AM	Fax	Unit 3W
3	Wrong record	B	Joe's Pizza Parlor received B	Dr. Simon wanted C	Dr. Carlson	3/19/2012	Mon.	8:45 AM	Mail	ROI
4	Wrong claim attachment	F	BC-State Received Patient F	BC-State for Patient E	Dr. Peters	3/21/2012	Wed.	8:30 AM	Mail	Billing
5	Wrong email	D	Patient X received D	Patient D	Dr. Carlson	3/8/2012	Thu.	4:30 PM	Email	Dr. Best

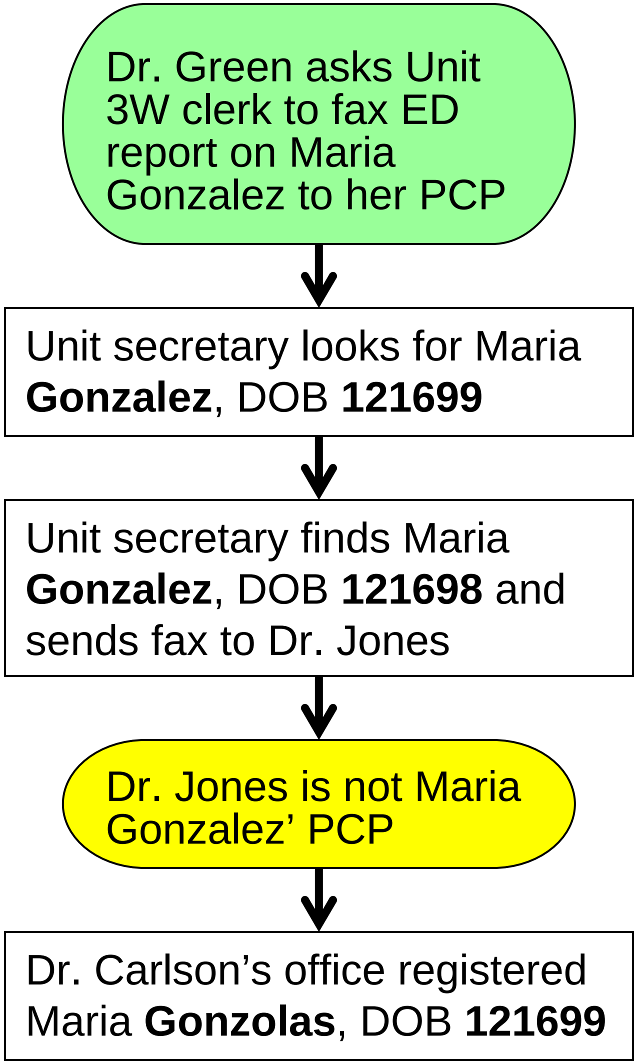
- Patterns were analyzed:
  - Monday mornings were somewhat common
  - Dr. Carlson as Primary Care Provider (PCP) was more common

Tracer Applied

- Each breach associated with each of Dr. Carlson's patients was traced using a **systems flowchart** with actual data
- It was found that Dr. Carlson's office had a large population of patients with many Hispanic surnames that were incorrectly sent to the hospital, impacting master person index
  - Gonzolas – Gonzalez – Gonzales – etc.
- This finding identified the root cause of a number of breaches, but not all

Flowchart Example

1. Original requestor did not know patient's PCP
2. Unit secretary looks up patient with correct information
3. Either doesn't read DOB correctly or assumes error in DOB
4. Breach occurs, but is #3 the root cause?
5. Search* reveals incorrect spelling of name



Dr. Green asks Unit 3W clerk to fax ED report on Maria Gonzalez to her PCP

Unit secretary looks for Maria **Gonzalez**, DOB **121699**

Unit secretary finds Maria **Gonzalez**, DOB **121698** and sends fax to Dr. Jones

Dr. Jones is not Maria Gonzalez' PCP

Dr. Carlson's office registered Maria **Gonzolas**, DOB **121699**

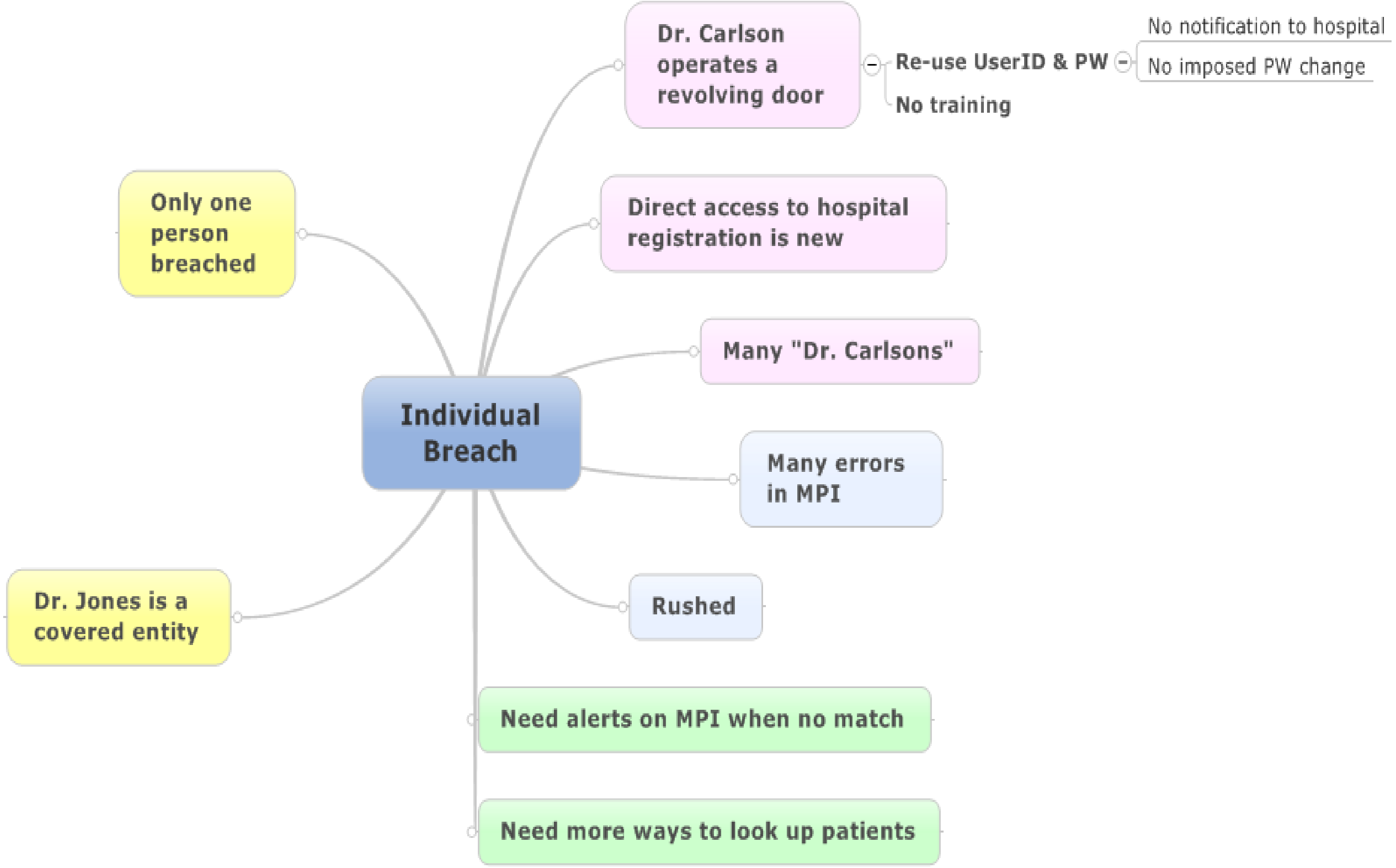
*Search for Root Cause

- Did Dr. Carlson’s staff supply wrong information; or did hospital staff enter wrong information?
  - If source documents or metadata are unavailable to determine source of error
  - Proactive sample must be taken to study primary source of error

Second Tracer Applied

- Not all breaches involved Dr. Carlson’s staff
- So, each person involved in each of the breaches studied was interviewed to determine their thoughts using a **mind map** on why a breach had occurred
  - Some gave rationales for why an individual breach to another provider is not bad
  - Some supplied excuses
  - Some expressed frustrations with processes
  - Some offered suggestions
- Bottom line – source of problems was direct access by PCP staff to hospital registration system causing more errors than normal; and hospital staff not accustomed to many errors and were not careful

Mind Mapping Tool


Individual Breach

Dr. Carlson operates a revolving door

Re-use UserID & PW

No notification to hospital

No imposed PW change

No training

Direct access to hospital registration is new

Many "Dr. Carlsons"

Many errors in MPI

Rushed

Need alerts on MPI when no match

Need more ways to look up patients

Only one person breached

Dr. Jones is a covered entity

Mitigation Strategies

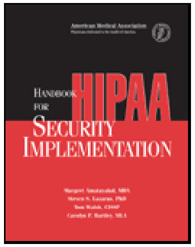
- Results discussed with office managers and hospital’s mitigation strategies shared; request made to change userID and PW for each new employee
- Supply a regular “report card” on individual breaches as a means to raise awareness
- Retrain that one individual breach is just as important as more than 500 individuals
- Add technology to alert to a mismatch in master person index (MPI clean up required)

Margret Amatayakul

Margret\A Consulting, LLC
Schaumburg, IL 60193
Tel. 847-895-3386
margret@margret-a.com
www.margret-a.com

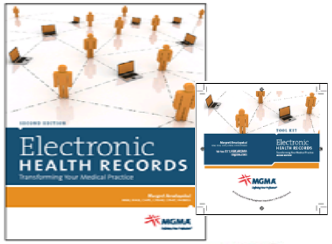
References & Resources

Margret Amatayakul, MBA, RHIA, CHPS, CPHIT, CPEHR, FHIMSS



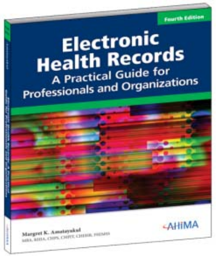
Handbook for HIPAA Security Implementation, Chicago: American Medical Association, Second Edition scheduled for 4Q 2012

- https://catalog.ama-assn.org/Catalog/



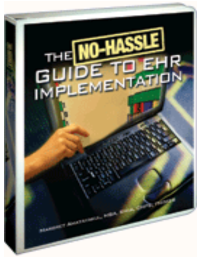
Electronic Health Records: Transforming Your Medical Practice, Second Edition, Denver: Medical Group Management Association, 2010; CD Toolkit available

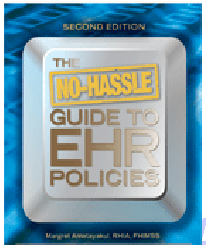
- www.mgma.org

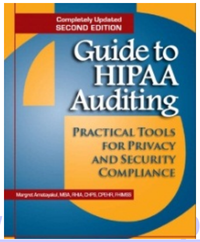

Electronic Health Records
A Practical Guide for Professionals and Organizations
Margret K. Amatayakul
AHIMA

Electronic Health Records: A Practical Guide for Professionals and Organizations, Fifth Edition, Chicago: American Health Information Management Association, 2012

- www.ahima.org




SECOND EDITION
THE NO-HASSLE GUIDE TO EHR POLICIES
Margret Amatayakul, RHIA, FHIMSS


Completely Updated SECOND EDITION
Guide to HIPAA Auditing
PRACTICAL TOOLS FOR PRIVACY AND SECURITY COMPLIANCE

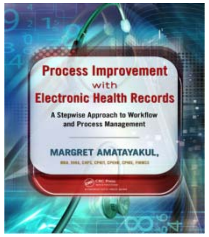
The No-Hassle Guide to EHR Implementation, 2007

The No-Hassle Guide to EHR Policies, 2010

Guide to HIPAA Auditing: Practical Tools for Privacy and Security Compliance, 2nd Ed, 2009

Published by HCPro, Inc. •

w lace.com


Process Improvement with Electronic Health Records
A Stepwise Approach to Workflow and Process Management
MARGRET AMATAYAKUL

Process Improvement with Electronic Health Records: A Stepwise Approach to Workflow and Process Management, Boca Raton, FL: CRC Press, 2012

- www.crcpress.com