Preparing for and Responding to OCR HIPAA Audit

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

President, Margret\A Consulting, LLC

An independent consulting firm focusing on optimizing EHR and health IT provisions of HIPAA, HITECH, and ACA

Rebecca L. Williams, **RN, JD**

Chair, Health Information Practice

Davis Wright Tremaine LLP

beckywilliams@dwt.com

206.757.8171

Agenda

- Implementing an internal HIPAA auditing program
- Establishing a baseline for monitoring risk
- Best practices for documenting compliance policies and procedures
- Why organizations should go beyond OCR’s online audit protocol when conducting an internal HIPAA audit
- What to expect in the audit process

Reduce risk; be ready

What is internal compliance auditing?

- Ongoing process for compliance assurance
  - Assists in identifying weaknesses to enable establishment of internal controls
  - Helps demonstrate commitment to responsible corporate conduct
  - Provides accurate view of behavior relative to specific compliance requirements
  - Creates a centralized source for managing compliance
- Most hospitals and large clinics have an internal compliance program to monitor for coding/billing fraud and abuse – but few have such a program for privacy, security, and breach notification

Where does it say to audit for compliance?

- Compliance means ongoing conformance to laws and regulations
- Specifically, HIPAA requires:
  - Uses and disclosures to be consistent with notice of privacy practices [Privacy Rule at 45 CFR 164.502(i)]
  - Security measures to be reviewed and modified as needed to continue provision of reasonable and appropriate protection [Security standards: General rules at 45 CFR 164.306(e)]
  - Periodic technical and nontechnical evaluation in response to environmental changes affecting security of ePHI that establishes the extent to which an entity's security policies and procedures meet the requirements [Security Rule: Evaluation at 45 CFR 164.308(a)(8)]
- EHR Meaningful Use Incentive Program [42 CFR 495.6] measures require:
  - Conduct or review a security risk analysis in accordance with requirements under 45 CFR 164.308(a)(1)
- OCR “encourages consistent attention to compliance activities”

What comprises an internal compliance auditing program?

- Central source for distributing information about compliance
- Process to determine baseline compliance
- Methodology that encourages workforce members to report potential problems
- Procedures that allow for prompt and thorough investigation of a problem
- Initiation of immediate and appropriate corrective action
- Minimizes loss through early detection and reporting
- Reduces exposure to (external audits) and penalties

Business case for internal auditing for HIPAA privacy, security, and breach

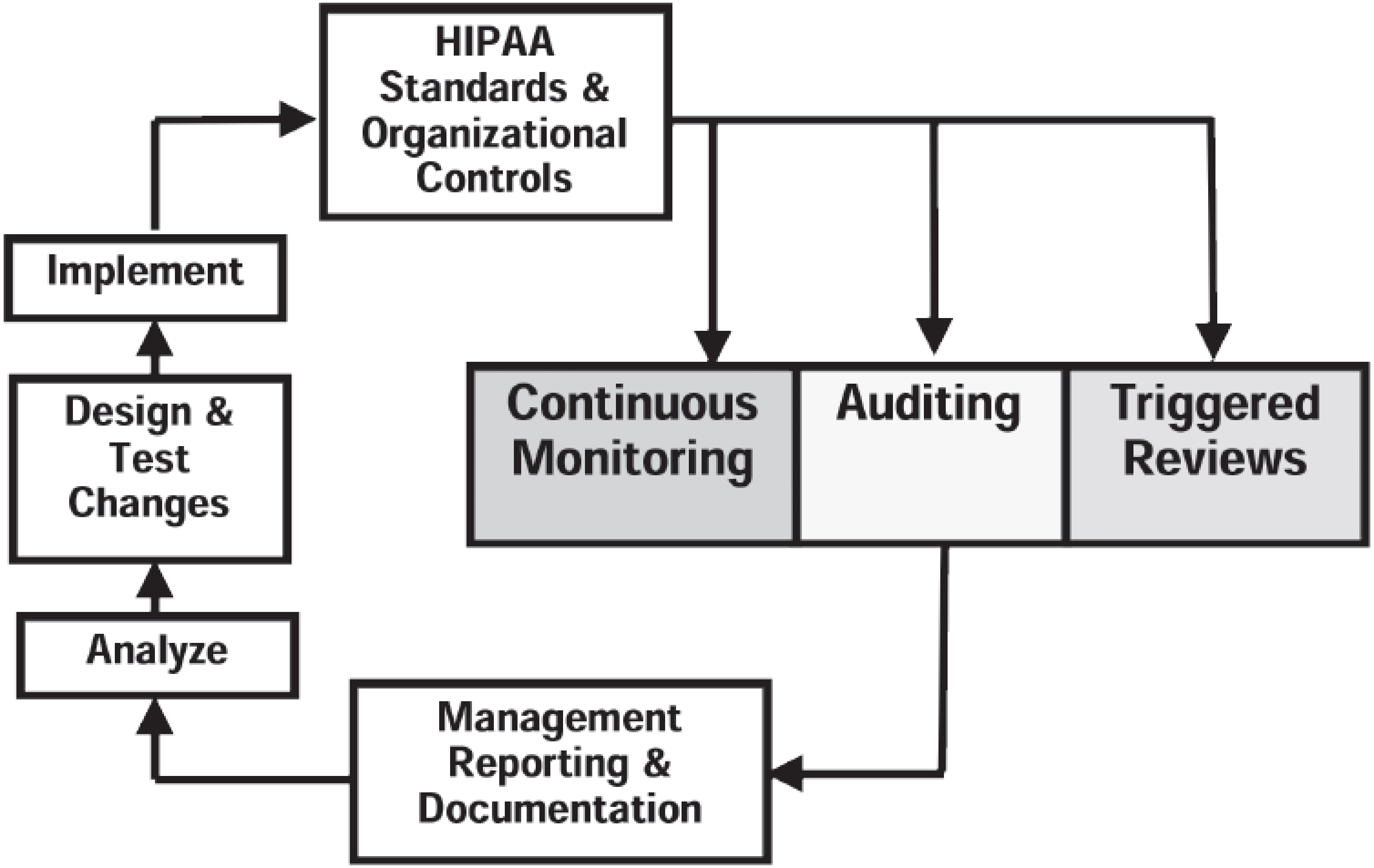
- OCR (HIPAA) and CMS (EHR Meaningful Use) audits reveal serious weaknesses
- Ever-increasing number of privacy complaints to OCR
- Increasing number and amount of settlements for privacy and security issues; expected increase in number of criminal cases
- Major HIPAA breaches have reached 1,000 milestone, with 1 in every 10 people in U.S. impacted
- Cost of a breach estimated at $188 per record. Average # of records in a breach = 23,647; or $4.4M per breach
- Identity theft may be most frequent, costly, and pervasive crime in U.S., with increasing sophistication

43% of identity thefts have a medical component, including potential for treatment and payment errors

Level setting on terminology

- **Action:** The performance of a process that is regulated
- **Complaint:** Statement that a situation is unsatisfactory or unacceptable
- **Event:** An action that may contribute to noncompliance
- **Incident:** An event that is noncompliant, or series of events that puts the organization at high risk for noncompliance
- **(HIPAA) breach:** Acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule that compromises the security and privacy of the PHI
- **HIPAA safe harbor**: Guidelines specifying that encryption or destruction render PHI unusable, unreadable, or indecipherable for purposes of breach notification
- **(General) data breach:** An incident in which sensitive, protected, or confidential data have potentially been viewed, stolen, or used by an individual unauthorized to do so

Internal compliance audit cycle

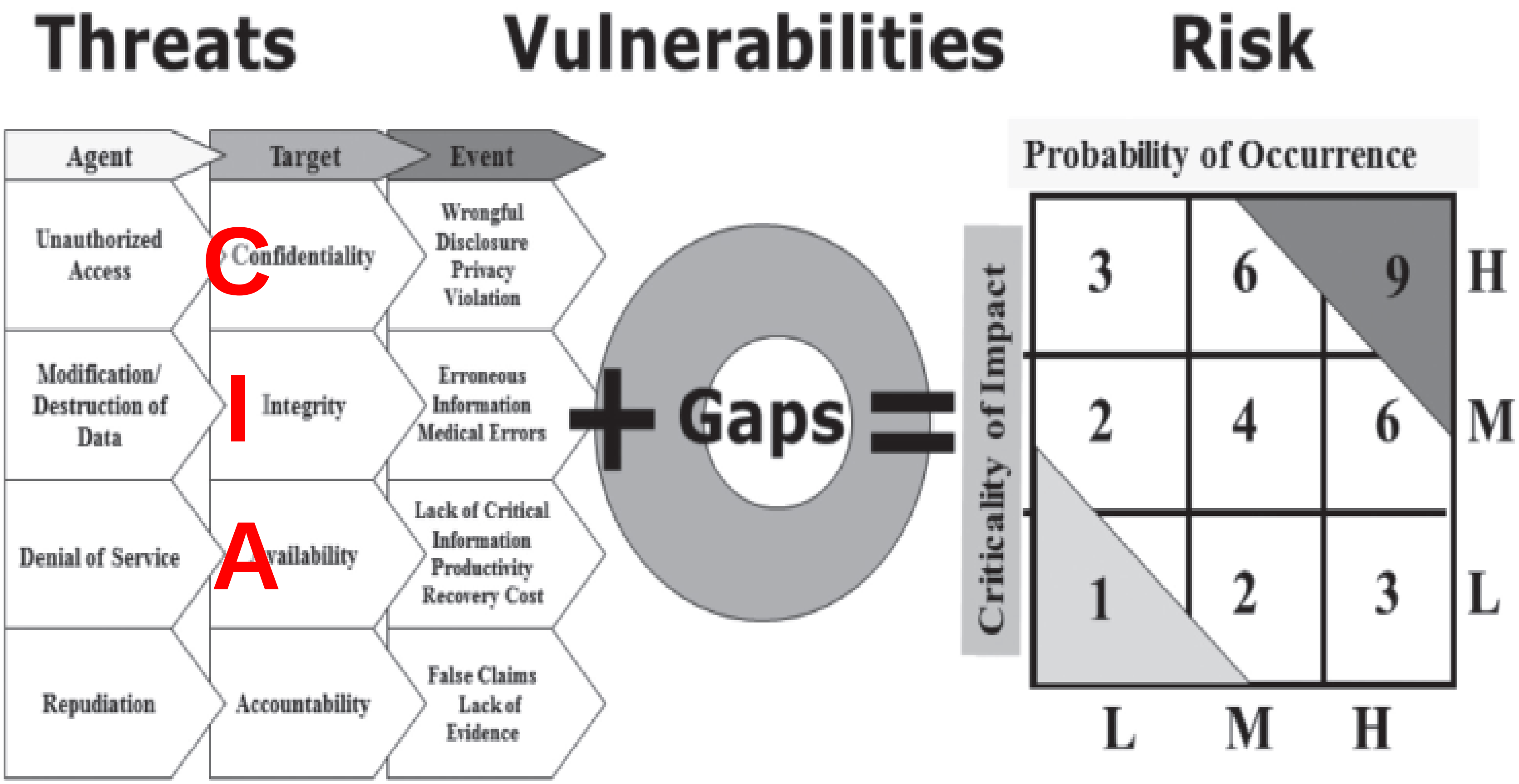


Source: Margret\A Consulting, LLC. Reprinted with permission.

Implementing internal auditing

- IPO, ISO, compliance officer(s), risk manager, legal counsel, develop coordinated program
- Determine focus of auditing; use sources such as:
  - Frequent privacy complaints
  - Known security threats
  - Most common causes of breaches
  - Findings from federal audits
  - Results of continuous monitoring and triggered reviews
- Creates culture of:
  - Transparency
  - Hold harmless
  - Data stewardship
  - Commitment to risk mitigation

Conducting a (privacy & security) risk analysis: A special case of internal auditing



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

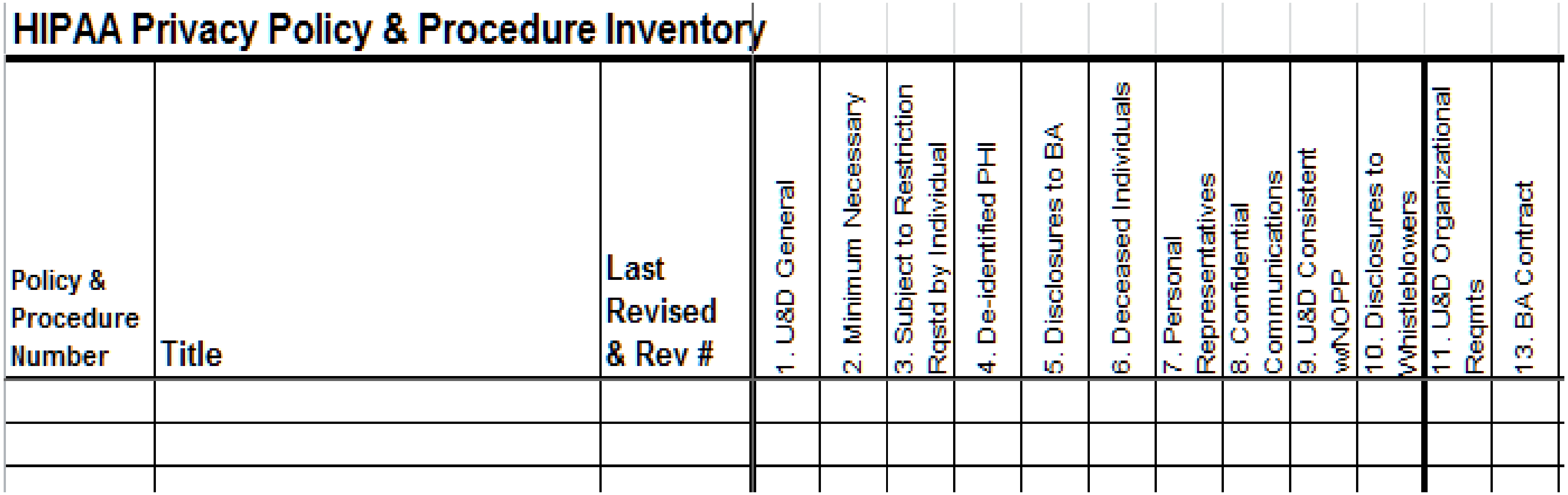
3	6	9	H
2	4	6	M
1	2	3	L
L	M	H	

Breach notification preparation

- Create and regularly drill a SWAT team to address a breach
- Train members of workforce and ensure business associates know how to identify and report a potential breach in a timely manner
- Have prepared decision tree to assess whether potential breach meets:
  - HIPAA definition and/or
  - State data breach definition (Note: not all state breaches are HIPAA breaches)
- Have prepared a checklist of tasks, including:
  - Notification to executive management; legal counsel; board of directors
  - Documentation of all steps taken, by whom, and when
  - Preservation of evidence
  - Management of business associate relationships as applicable
- Have prepared public notification process and materials, including public announcement script
- Conduct required notification, reporting, and mitigation
- Assess and take action on lessons learned

External audit preparedness

- Documentation is critical
- Have ready all documentation – not only P&P but documentary evidence, ideally with index arranged in order of regulatory standards



HIPAA Privacy Policy & Procedure Inventory

Policy & Procedure Number	Title	Last Revised & Rev #	1. U&D General	2. Minimum Necessary	3. Subject to Restriction Rqstd by Individual	4. De-identified PHI	5. Disclosures to BA	6. Deceased Individuals	7. Personal Representatives	8. Confidential Communications	9. U&D Consistent w/NOPP	10. Disclosures to Whistleblowers	11. U&D Organizational Reqmts	13. BA Contract

- Decide how sensitive documentation will be identified and supplied
- Consider legal counsel review of documentation prior to submission
- Provide copy with any patient or health professional identification masked but which contains name of organization on every page and running page numbers

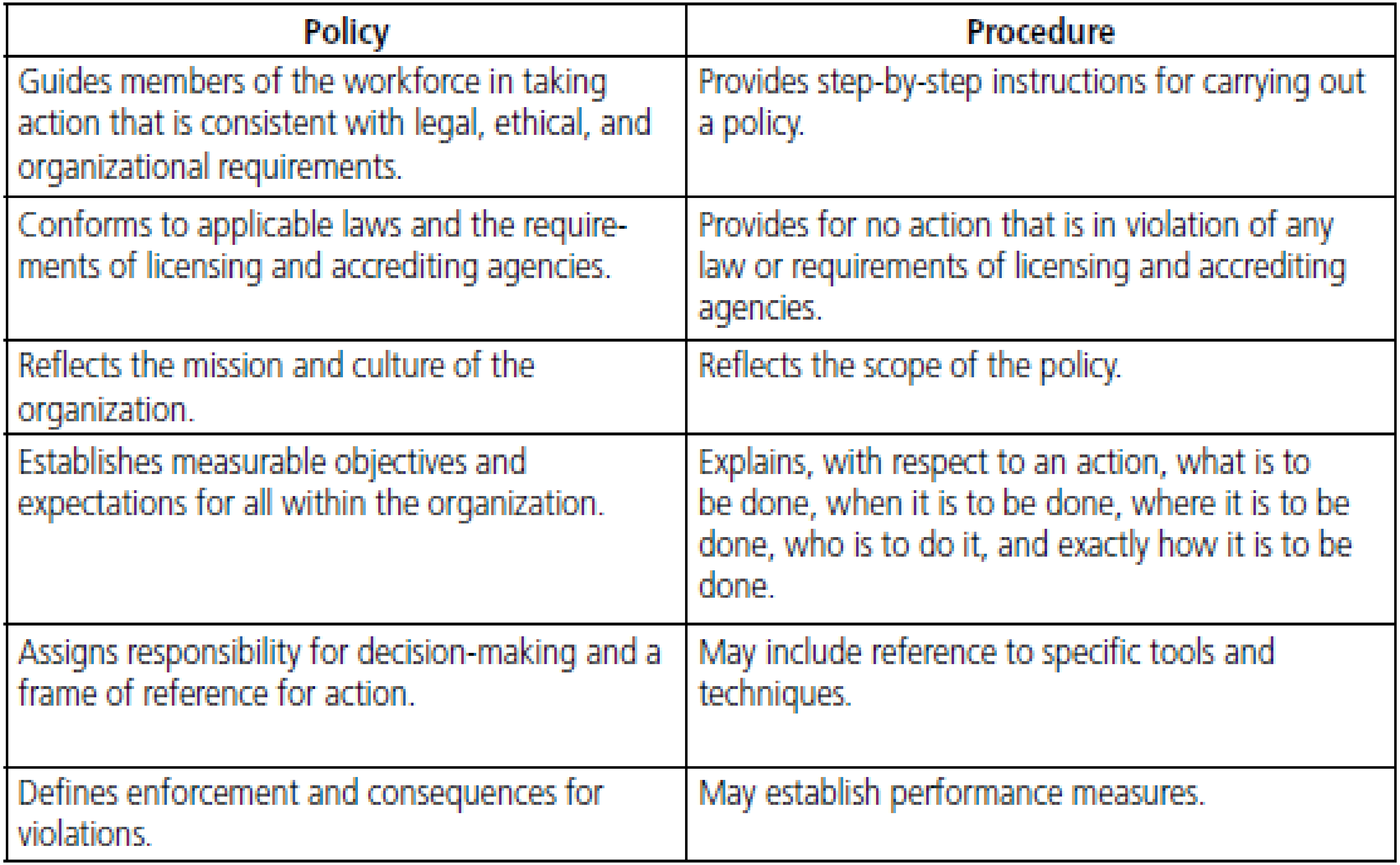
Documentation

Lack of, or poor, documentation is one of major findings in (HIPAA and Meaningful Use) audits and findings in OCR settlement cases

- 45 *CFR* 164.530 (j) [Privacy Rule] Documentation
  - o Maintain
    - Policies and procedures
    - Communications required to be in writing
    - Records of actions, activities, or designations required to be writing
    - Documentation sufficient to meet burden of proof
  - o Retain
    - For 6 years from date of creation or date when last in effect, whichever is later

- 45 *CFR* 164.316 [Security Rule]
  - o (a) Policies and procedures, taking into consideration flexibility of approach
  - o (b)(1) Documentation of
    - Policies and procedures
    - Record of action, activity, or assessment as required
  - o (b)(2)
    - Time limit: Retain for 6 years …
    - Availability: Make available to persons responsible for implementing procedures to which documentation pertains
    - Updates: Review documentation periodically and update as needed in response to environmental or operational changes affecting the security of ePHI

Policies and Procedures

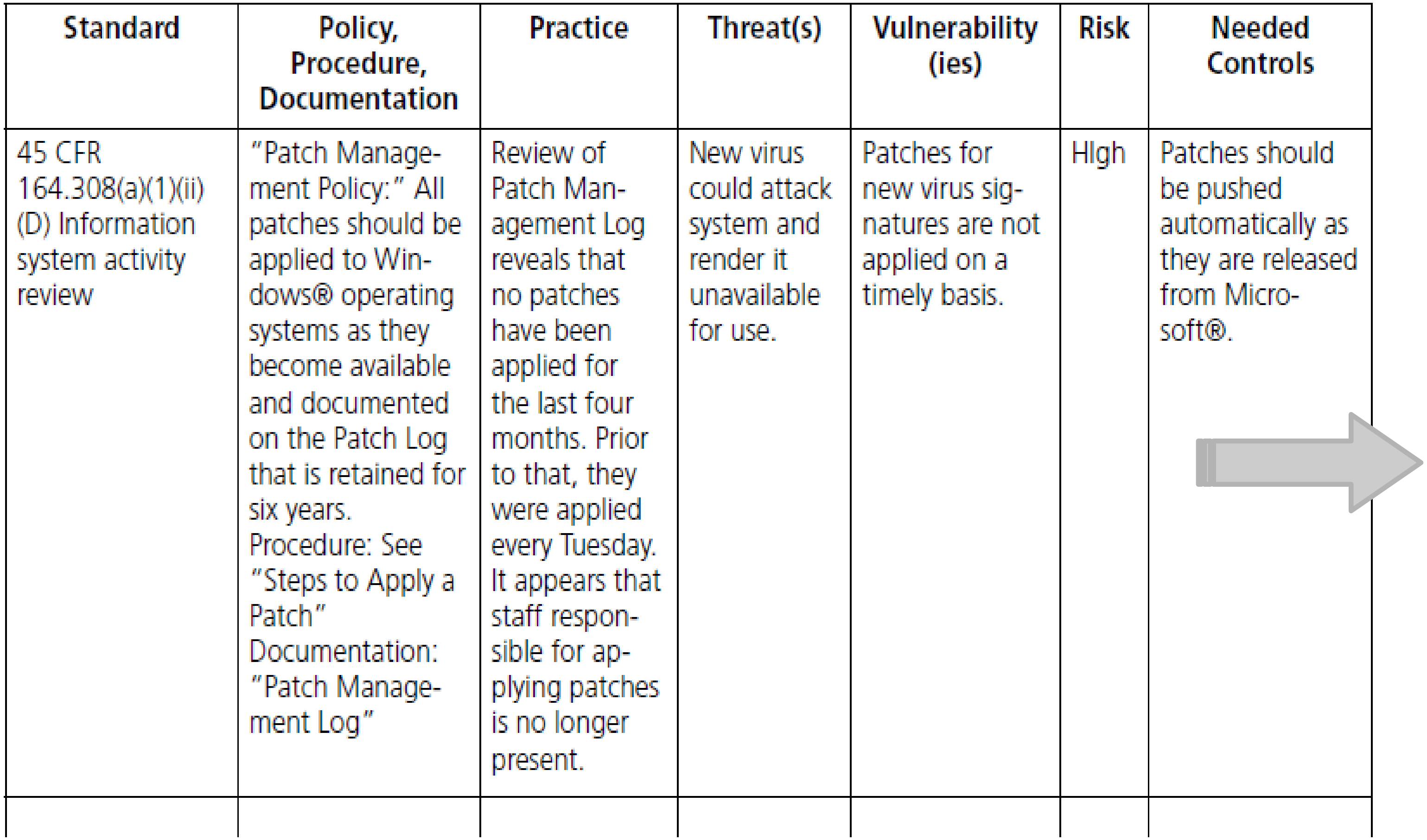


Policy	Procedure
Guides members of the workforce in taking action that is consistent with legal, ethical, and organizational requirements.	Provides step-by-step instructions for carrying out a policy.
Conforms to applicable laws and the requirements of licensing and accrediting agencies.	Provides for no action that is in violation of any law or requirements of licensing and accrediting agencies.
Reflects the mission and culture of the organization.	Reflects the scope of the policy.
Establishes measurable objectives and expectations for all within the organization.	Explains, with respect to an action, what is to be done, when it is to be done, where it is to be done, who is to do it, and exactly how it is to be done.
Assigns responsibility for decision-making and a frame of reference for action.	May include reference to specific tools and techniques.
Defines enforcement and consequences for violations.	May establish performance measures.

Many sources of policies and procedures

- Many policies exist already
  - Management
  - Human resources
  - Public relations
  - Procurement
  - Institutional review board
  - Medical staff bylaws, rules, and regulations
  - Others
- Ensure HIPAA is explicitly identified, or catalogue generic policies and procedures (e.g., sanction policy) under a HIPAA umbrella
- Ensure HIPAA procedures are not copies of the regulation, but specific step-by-step descriptions written in plain language that guide work
- Recognize the sensitivity of certain procedures and documentation; handle appropriately (e.g., penetration test procedure including identification of all IP addresses)

Documenting (privacy and security) risk analysis and remediation priorities/plan



Standard	Policy, Procedure, Documentation	Practice	Threat(s)	Vulnerability (ies)	Risk	Needed Controls
45 CFR 164.308(a)(1)(ii)(D) Information system activity review	"Patch Management Policy:" All patches should be applied to Windows® operating systems as they become available and documented on the Patch Log that is retained for six years. Procedure: See "Steps to Apply a Patch" Documentation: "Patch Management Log"	Review of Patch Management Log reveals that no patches have been applied for the last four months. Prior to that, they were applied every Tuesday. It appears that staff responsible for applying patches is no longer present.	New virus could attack system and render it unavailable for use.	Patches for new virus signatures are not applied on a timely basis.	HIgh	Patches should be pushed automatically as they are released from Microsoft®.

Extend spreadsheet for project plan

Documentation pitfalls

- Maintaining action logs in help desk ticketing system or IT staff member's email is generally not conducive to:
  - Producing documentary evidence for an audit
  - Conducting pattern analysis to identify issues
  - Retention assurance
  - Accessibility to authorized individuals
- Buying policies and procedures and not changing them to fit your environment All policies and procedures carrying the same effective date, and with no version history Logs maintained without case files
- Documentation without analysis (e.g., records of breaches without risk assessment documented)
- Risk analysis without remediation plan/evidence of completion
- Integrating federal and state breach files; all forms of compliance (e.g., coding compliance with privacy compliance)

Training

- Most providers include HIPAA privacy and security training during orientation; thereafter in an annual compliance training requirement
  - Ensure content is updated annually
  - Ensure content reflects current trends in industry; issues in environment
- Annual training is not enough. Privacy, security, and breach awareness need to be part of organizational culture
  - Managerial staff need to walk the talk and be held accountable
  - Use “teachable moments”
  - Discuss noteworthy complaints/incidents in newsletters, meetings, etc.
  - Patients also need “training;” waiting room CCTV, newsletters; website information; “non-negative” clinician reinforcement
- Don’t put fear into HIPAA
  - Many organizations have paralyzed staff into inaction that potentially is harmful to the organization and the clinical care delivered to its patients
  - Find ways to protect privacy and address the **CIA** of security in positive ways; ensure transparency and stewardship

They’re Baaack: HIPAA Audits

- Phase 2 audit process has formally started … yesterday
- Audits of
  - Covered entities
  - Business associates
- Findings from audit:
  - Primarily compliance improvement
  - Possible enforcement action

History of Audits: Phase 1: Pilot 2011 – 2012

- Required by the HITECH Act
- Phase 1: Conducted 115 audits (through 2012)
- Two parts:
  - Initial 20 audits to test original audit protocol
  - Final 95 audits using modified audit protocol
- Covered very broad range of topics regarding HIPAA compliance

Overall Findings & Observations of Pilot

Only 11% of the entities had **no findings**

Security accounted for 60% of findings and observations – although only 28% of potential total

Providers had a greater proportion of findings and observations (65%) than reflected by their proportion of the total set (53%)

Overall Cause Analysis

- For every finding and observation cited, a "Cause" was identified
- Most common: **entity unaware of the requirement**
  - 30% of all findings and observations
  - 39% of privacy findings
- Other causes noted included:
  - Lack of application of sufficient resources
  - Incomplete implementation
  - Complete disregard

Cause Analysis – Top Elements
Unaware of the Requirement

Privacy

- Notice of Privacy Practices
- Access of Individuals
- Minimum Necessary
- Authorizations

Security

- Risk Analysis
- Media Movement and Disposal
- Audit Controls and Monitoring

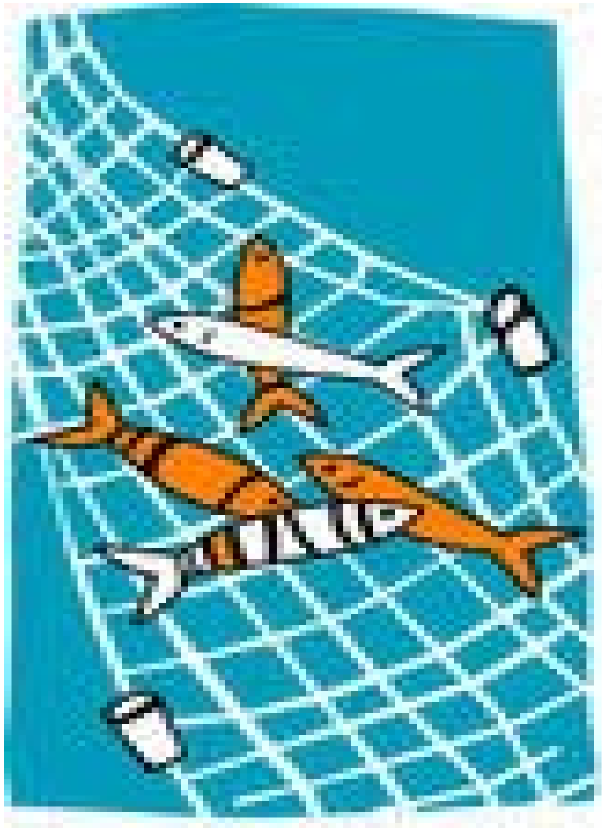
What to Expect for Phase 2 OCR Audits: 3 Rounds

- Round 1: Desk audits of Covered Entities
  - Remotely performed
  - More targeted
  - To be completed by 12/16
- Focus
  - Privacy: Notice of privacy practices and access
  - Security: Risk analysis and risk management
  - Breach: Content and timing

What to Expect for OCR Audits: Phase 2

- Round 2: Desk audits of Business Associates
  - Same form and format as for Covered Entities
- Round 3: Full audits of Covered Entities and Business Associates
  - On-site visits of 3 – 5 days
  - More comprehensive
  - Could include an entity audited during Round 1 or 2

Phase 2 Audits: Audit Candidates



- Currently developing pool of candidates
- Confirming contact information
  - o Check spam filters
- Pre-Audit Screening Questionnaire
  - o Size, type, location, services
  - o Identification of business associates
- Goal: Diverse pool of covered entities and business associates

Audit Phase 2

- How to avoid being audited: OCR will NOT include entities with an open complaint investigation or compliance review
- OCR: We expect covered entities and business associates to provide the auditors their full cooperation and support

Timing and Other Requirements

- Response due within 10 business days
- Opportunity to review draft report
- 10 business days to submit comments to draft report – written responses to be included in final audit report
- Final draft issued 30 days after comments submitted
- Auditee to receive final report

The Data Request Letter. . .

- **You are the Lucky Winner of an OCR Audit!!!!!**
  - Subject of the audit (e.g., privacy, security, breach notification)
  - Initial request for documents
  - Audit team introduction
  - Information about audit process
  - OCR expectations

Notification/Data Request

- Make sure notification is routed correctly
- Have audit response team ready to go, both internal and external support (including legal counsel)
- Read request carefully
  - o Timing
  - o Desk audit v. on-site audit
  - o Full or limited review

- Have and implement audit response plan: Ready, set, go!

Audit Response

- Timely:
  - o May not assess data that is not submitted on time
  - o Short time to respond
- Current:
  - o Documentation should be current as of the date of the request
  - o Documentation developed after data request likely will be given lesser weight or not be considered

Audit Response

- Self Explanatory: Uncertain about level of clarification permitted
- On Target: Don’t submit extraneous information
- Digital: Submission through a secure portal

Audit Response

- Demonstrate Compliance:
  - Show effective HIPAA compliance program

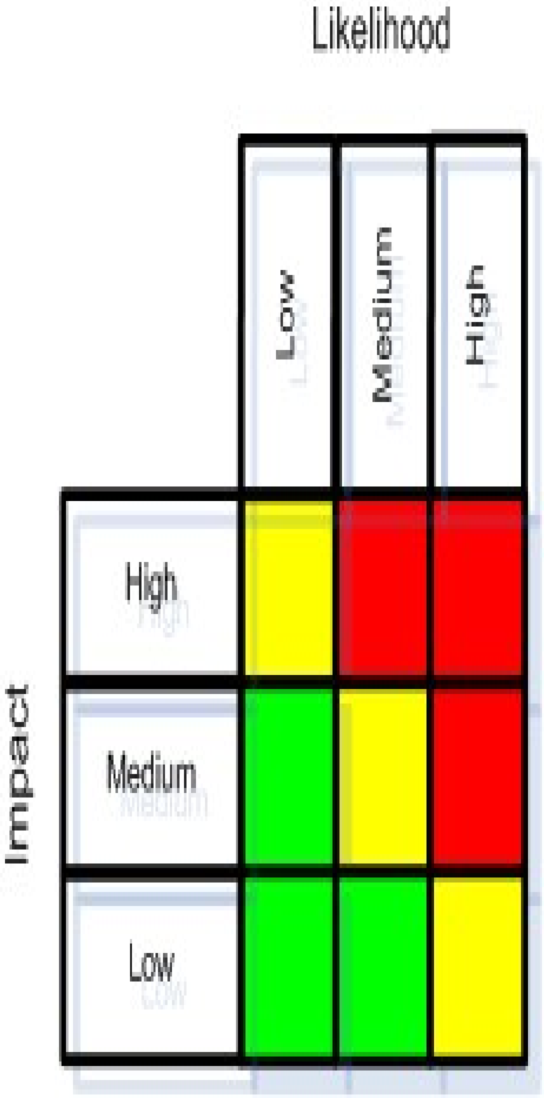
- Respond!
  - Still may be selected for audit even if you don’t respond to pre-survey requests:
    OCR will use publicly available information
  - No response may result in compliance review

Audit Considerations: Know your Business Associates

- Will be asked to identify your business associates
- Have lists and contact information
- Remember: Definition of “business associate” has changed
- Verify business associate contracts have been updated and signed

Audit Considerations: Risk Analysis

- Make sure it is a HIPAA risk analysis
- Identify locations of PHI
- Identify reasonably anticipated threats (e.g., human, natural, environmental) and vulnerabilities
- Assign risk levels based on likelihood and impact
- Update the risk analysis based on:
  - Organizational experience
  - Changes in operations and facilities
  - Industry experience (e.g., ransomware)



Impact \ Likelihood	Low	Medium	High
High	🟨	🟥	🟥
Medium	🟩	🟨	🟥
Low	🟩	🟩	🟨

Audit Considerations: Documentation

- Document, Document, Document
- Verify policies and notice of privacy practices are updated
  - o Reflect HIPAA changes
  - o Include high profile areas (e.g., portable media, taking PHI off-site)
  - o Accurately reflect the HIPAA compliance program and practices

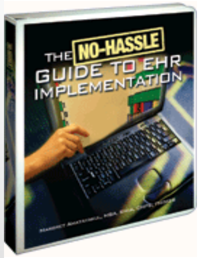
Prepare!

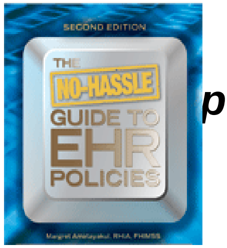
- Likened to an “open book test”
- Review audit protocols
- Phase 2 protocols
  - Promised before audits begin
  - To be updated from Phase 1 to reflect HIPAA Omnibus Rule
- Perform own assessment/audit
  - Internal or external
  - Use audit protocol
  - Identify other toolkits
  - Consider use of attorney-directed review
- Corrective action for gaps

Q & A

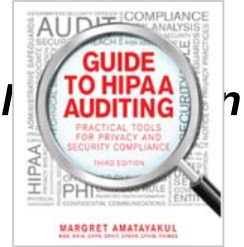
References & Resources

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





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



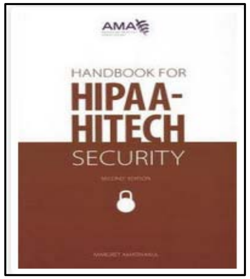
***The No-Hassle Guide to EHR pl n*, 2007**

***The No-Hassle Guide to EHR Policies*, 2010**

***Guide to HIPAA Auditing: Practical Tools for Privacy and Security Compliance*, 3rd Ed, 2014**

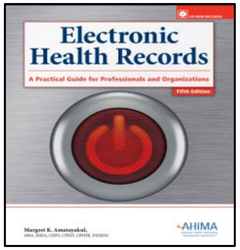
Published by HCPro, Inc.

- www.hcmarketplace.com



Handbook for HIPAA-HITECH Security, Second Edition, Chicago: American Medical Association, 2013.

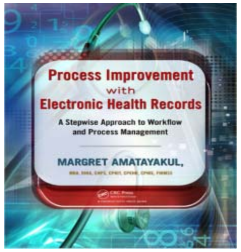
- https://commerce.ama-assn.org/store/



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

Electronic Health Records: A Practical Guide for Professionals and Organizations, Fifth Edition, Chicago: American Health Information Management Association, 2013. Sixth Edition available Fall 2016

- www.ahima.org



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

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

References & Resources

Becky Williams, RN, JD, Partner and Co-Chair Health Information Practice (DWT)

The DWT HIPAA Audit Toolkits – A Cost-Effective Answer to Meeting the Challenges of HIPAA

Maintaining the privacy and security of patient information is part of the foundation of providing good health care and protecting the safety of patients, participants, and consumers. But complying with regulations under the Health Insurance Portability and Accountability Act (HIPAA) presents daunting challenges. The stakes for compliance are higher than ever, with the next wave of random government audits, investigations, compliance reviews, breach notification obligations, and threat of hefty financial penalties.

Davis Wright Tremaine offers audit toolkits to assist your organization prepare for HIPAA audits and investigations and to further your HIPAA compliance efforts..

24/7
BREACH
RESPONSE TEAM
844-GoToDWT
(844-468-6398)

Incident Response & Breach Coaching

Davis Wright's information privacy and security team regularly assists companies in preparing for, responding to, and recovering from information security incidents. We have six regional teams of specially trained incident responders who are prepared to help your organization respond to a potential breach at a moment's notice. We provide a full-service offering that can work seamlessly with your internal compliance teams and coordinate with other external professionals, as needed.

- http://www.dwt.com/practices/incidentresponsebreachcoaching/