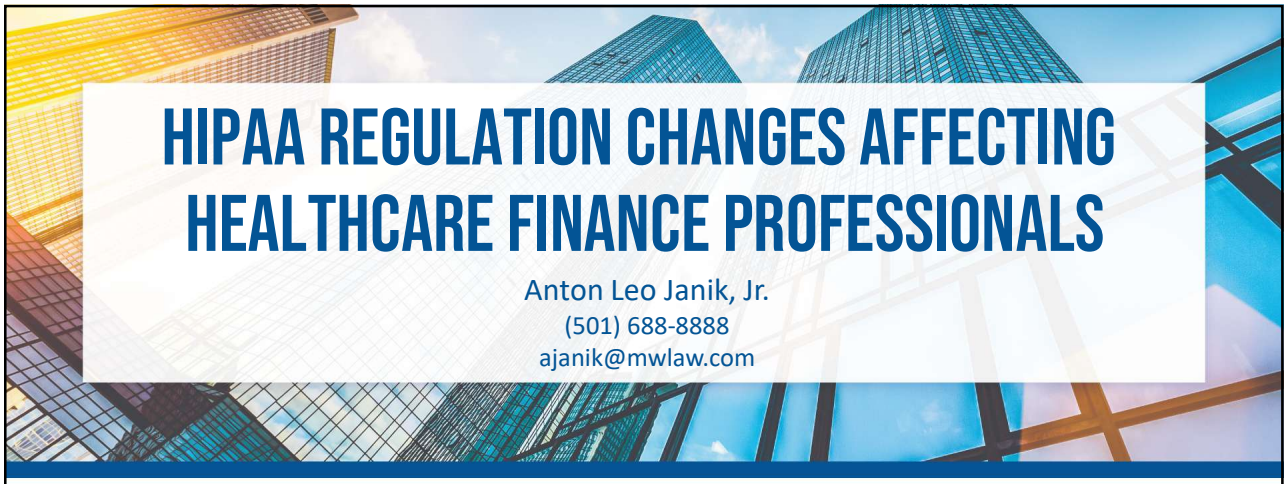

HIPAA REGULATION CHANGES AFFECTING HEALTHCARE FINANCE PROFESSIONALS

Anton Leo Janik, Jr.
(501) 688-8888
ajanik@mwlaw.com

MITCHELL | WILLIAMS
LAW FIRM

Mitchell, Williams, Selig, Gates & Woodyard, P.L.L.C.

1

WHY HIPAA MATTERS TO HEALTHCARE FINANCE PROFESSIONALS

- HIPAA compliance is not solely a clinical or IT responsibility
- Finance teams handle PHI daily — billing, claims, payments, vendor relationships, audits
- Financial consequences of non-compliance are escalating

M | W

2

2025 AT A GLANCE

- The most significant proposed HIPAA Security Rule overhaul since 2013
- OCR launched third round of compliance audits
- 21 enforcement actions — second-highest annual total ever
- 42 CFR Part 2 alignment rule approaching compliance deadline
- Reproductive health privacy rule vacated by federal court

M | W

3

PROPOSED SECURITY RULE OVERHAUL – AN OVERVIEW

- Published January 6, 2025
- First major Security Rule revision in over a decade
- Comment period closed March 7, 2025
- Now in the current administration's hands; final rule projected for May 2026

M | W

4

SECURITY RULE HISTORY

M | W

5

SECURITY RULE REQUIREMENTS – OVERVIEW

The Security Rule requires that regulated entities:

- Ensure the Confidentiality, Integrity and Availability of information
- Protect against anticipated threats to security and integrity of information
- Protect against anticipated uses or disclosures of information
- Ensure workforce compliance

M | W

6

SECURITY RULE - IMPLEMENTATION SPECIFICATIONS

Required and Addressable Implementation Specifications

Regulated entities are required to comply with every Security Rule "standard." However, some of the flexibility and scalability afforded by the Security Rule to regulated entities is achieved by categorizing certain implementation specifications within those standards as "addressable" and others as "required."

The "required" implementation specifications must be implemented. The "addressable" designation does not mean that an implementation specification is optional. Rather, it permits regulated entities to determine whether the addressable implementation specification is reasonable and appropriate for that regulated entity. Where it is reasonable and appropriate, the regulated entity must adopt the addressable implementation specification. Where an addressable implementation specification it is not reasonable and appropriate, the Security Rule allows the regulated entity to adopt an alternative measure that achieves the purpose of the standard, if the alternative measure is reasonable and appropriate.[62] In such cases, the regulated entity must also document why it is not reasonable and appropriate to implement the addressable implementation specification.[63]

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

M | W

7

SECURITY RULE – FLEXIBILITY OF APPROACH

When determining **how** to implement required and addressable specifications, consider:

- The entity's size, complexity, and capabilities.
- The entity's technical infrastructure, hardware, and software security capabilities.
- The costs of security measures.
- The probability and criticality of potential risks to ePHI.

But review when things change

M | W

8

SECURITY RULE – REQUIRED VS. ADDRESSABLE (TODAY)

Safeguard Type	Focus Area	Key Requirements
Administrative	Internal policies and personnel controls	Risk Analysis, Risk Management, Sanction/Disciplinary Policy, Information System Activity Review (logs and events), Assigned Security Responsibility (Security Official), Information Access Management (Clearinghouse), Security Incident Procedures, Contingency Plan (Backup/Recovery/Emergency Mode, Testing and Revision), BAA/Contract Controls (include ePHI Protection, Breach Reporting, Permitted Uses and Disclosures), Evaluate Safeguards as Risks and Systems Change. Authorization and Supervision of Workforce Access to ePHI, Verify role-appropriate Access, Termination Procedures, Security Reminders, Phishing and Malware Training, Log-In Monitoring, Password Management
Physical	Protect physical access to data and equipment	Workstation Use (prevent unauthorized ePHI viewing), Physical Safeguards (locks, secured, rooms, privacy filters), Disposal Controls, Media Re-Use Controls Access Control and Validation Procedures, Contingency and Emergency Access Provisions, Facility Security Plan, Maintenance Records, Asset Tracking, Data Backup and Storage
Technical	IT protocols and technology system controls	Unique User IDs, Emergency Access Procedure, Audit Logs and Alerts (with regular review), Person or Entry Authentication, Automatic Logoff, Encryption and Decryption (at rest), Encryption (in transit), Mechanism to Authenticate ePHI (hash, digital signatures), Data Integrity Controls (checksums)

M | W

9

PROPOSED SECURITY RULE – WHY IS HHS SEEKING A CHANGE?

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

*The proposed modifications would revise existing standards to **better protect the confidentiality, integrity, and availability of electronic protected health information (ePHI)**. The proposals in this NPRM would increase the cybersecurity for ePHI by **revising the Security Rule** to address: **changes in the environment** in which health care is provided; **significant increases in breaches and cyberattacks**; **common deficiencies** the Office for Civil Rights has observed in investigations into Security Rule compliance by covered entities and their business associates (collectively, "regulated entities"); other cybersecurity guidelines, **best practices**, methodologies, procedures, and processes; and **court decisions** that affect enforcement of the Security Rule.*

M | W

10

PROPOSED SECURITY RULE – KEY CHANGES (1 OF 2)

- **No more "addressable" vs. "required"** — all specifications become Required (**but** HHS says the Flexibility of Approach will still apply to Required specifications)
- **Technology asset inventory & network map** — must document all systems handling ePHI, and update it annually
- **Enhanced risk analysis requirements** — written assessments documenting threats, vulnerabilities, and risk levels
- **Mandatory encryption** — ePHI at rest **and** in transit (with limited exceptions: individual right of access, infeasible environments, specific medical devices)

M | W

11

PROPOSED SECURITY RULE – KEY CHANGES (2 OF 2)

- **Multi-Factor Authentication (MFA)** — required for all systems with ePHI access (with limited exceptions: unsupported technology, emergency, legacy FDA-regulated devices)
- **Vulnerability scanning** — at least every six months
- **Patch management timelines** — 15 days for critical patches, 30 days for high-risk patches
- **72-hour system restoration** — critical systems must be recoverable within 72 hours
- **BAs must notify CEs within 24 hours** from activation of BA's contingency plan.
- **Annual internal compliance audits required**

M | W

12

PROPOSED SECURITY RULE – VENDOR IMPACT

- **Annual written verification** from all business associates confirming technical safeguard deployment
- Verification must be based on a **subject matter expert's** written analysis
- Applies to billing companies, clearinghouses, RCM vendors, payment processors, coding services, collection agencies
- This is a major escalation from current requirement of simply having a BAA in place (Trust Based >>> Verification Based)

M | W

13

PROPOSED RULE – WHAT FINANCE TEAMS SHOULD DO NOW

- 240-day compliance window expected after finalization
- Do not wait for the final rule — begin gap assessments now
- Priority areas: risk analysis documentation, encryption, MFA, vendor verification processes
- Final rule may be scaled back, but bipartisan support exists for stronger cybersecurity

M | W

14

OCR'S THIRD PHASE OF HIPAA AUDITS

- Launched March 2025 — 50 covered entities and business associates
- Focus: hacking and ransomware prevention
- Prior audit phases found widespread non-compliance; HHS OIG criticized program for lacking teeth
- This round is expected to be more rigorous and consequential

M | W

15

WHAT OCR AUDITORS WANT TO SEE: IDENTIFY, IMPLEMENT

- Documented risk analyses covering all ePHI systems (including billing and claims)
- Evidence that security safeguards are implemented — not just planned
- Current business associate agreements for all vendors
- Workforce training records specific to staff handling ePHI
- **Key principle:** If you cannot document compliance, you are effectively not compliant

M | W

16

RISK ANALYSIS REQUIREMENTS UNDER THE SECURITY RULE

Risk Analysis Requirements under the Security Rule

The Security Management Process standard in the Security Rule requires organizations to *"[i]mplement policies and procedures to prevent, detect, contain, and correct security violations."* (45 C.F.R. § 164.308(a)(1).) Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard. Section 164.308(a)(1)(ii)(A) states:

> RISK ANALYSIS (Required).
> Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization].

The following questions adapted from NIST Special Publication (SP) 800-66[5] are examples organizations could consider as part of a risk analysis. These sample questions are not prescriptive and merely identify issues an organization may wish to consider in implementing the Security Rule:

- Have you identified the e-PHI within your organization? This includes e-PHI that you create, receive, maintain or transmit.
- What are the external sources of e-PHI? For example, do vendors or consultants create, receive, maintain or transmit e-PHI?
- What are the human, natural, and environmental threats to information systems that contain e-PHI?

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

M | W

17

160.414 LIMITATIONS

M | W

18

ENFORCEMENT TRENDS – 2025 HIGHLIGHTS

21 settlements and civil monetary penalties in 2025

Dominant theme: security risk analysis failures, OCR technical review, CE responsibility over BAs increased, Right of Access Initiative increases

Illustrative cases:

- Solara Medical Supplies — $3M (2019/2020 events, 114,000 individuals, failed risk analysis, lack of MFA)
- Warby Parker — $1.5M (2018/2020/2022 events, 200,000 individuals, risk analysis, risk management, monitoring)
- BayCare Health System — $800K (2018 complaint by 1 individual, access management, risk management, system activity review)
- PIH Health — $600K (2019, 190,000 individuals, risk analysis, security controls, late notification to OCR and affected individuals)

M | W

19

ENFORCEMENT TRENDS – WHAT IS CHANGING IN 2026?

- OCR's risk analysis initiative expanding to include **risk management**, evidence that identified risks were actually mitigated
- State attorneys general increasingly pursuing HITECH enforcement under state law, and enforcing state privacy law against entities not excepted therefrom under state law
- NY announced $500,000 settlement with Capital Region Health Care in December 2025

Penalty Tier	Level of Culpability	Min. Fine (Per Violation)	Max. Fine (Per Violation)	Annual Cap (Identical Provision)
Tier 1	**No Knowledge**: Unaware of the violation and could not have known with reasonable diligence.	$145	$73,011	$2,190,294
Tier 2	**Reasonable Cause**: Should have known of the issue, but it wasn't due to willful neglect.	$1,461	$73,011	$2,190,294
Tier 3	**Willful Neglect (Corrected)**: Intentional disregard, but corrected within 30 days of discovery.	$14,602	$73,011	$2,190,294
Tier 4	**Willful Neglect (Not Corrected)**: Intentional disregard with no attempt to fix within 30 days.	$73,011	$2,190,294	$2,190,294

M | W

20

42 CFR PART 2 – SUD COMPLIANCE DEADLINE: FEBRUARY 16, 2026

- Governs confidentiality of substance use disorder (SUD) patient records
- Final rule aligns Part 2 more closely with HIPAA
- OCR now enforces Part 2 regulations (as of February 16, 2026)

M | W

21

42 CFR PART 2 – (SUD) WHAT CHANGED FOR FINANCE TEAMS

- **Single consent** now covers all future uses for treatment, payment, and healthcare operations
- Segregation of Part 2 records no longer required
- Redisclosure of SUD records now permitted under HIPAA Privacy Rule
- **But:** SUD records still restricted in civil, criminal, administrative, and legislative proceedings — important for billing disputes and litigation holds

M | W

22

42 CFR PART 2 – HIPAA PHI DISCLOSURES IN PROCEEDINGS

164.512(e): A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:

(i) in response to a **court order**, or

(ii) in response to a **subpoena** … without a court order, **if**:

(A) the covered entity receives **satisfactory assurance** that reasonable efforts have been made by such party to ensure that the individual who is the subject of the PHI that has been requested **has been given notice** of the request and the time to respond has elapsed (or subject did object and objection now resolved), **or**

(B) The covered entity receives documentation of an **agreed protective order** has been submitted or requested from the tribunal.

M | W

23

42 CFR PART 2 – PART 2 (SUD) PHI DISCLOSURES IN PROCEEDINGS

If you haven't received a separate patient consent for this legal disclosure:

A specific Part 2 Order is Required, plus a subpoena.

(e) *Content of order.* An order authorizing a use or disclosure must:

(1) Limit use or disclosure to only those parts of the patient's record, or testimony relaying those parts of the patient's record, which are essential to fulfill the objective of the order;

(2) Limit use or disclosure to those persons whose need for information is the basis for the order; and

(3) Include such other measures as are necessary to limit use or disclosure for the protection of the patient, the physician-patient relationship and the treatment services; for example, sealing from public scrutiny the record of any proceeding for which use or disclosure of a patient's record, or testimony relaying the contents of the record, has been ordered.

M | W

24

42 CFR PART 2 – (SUD) ACTION ITEMS

- Update Notice of Privacy Practices to address SUD record handling (deadline: Feb. 16, 2026). Include the following:
  - (1) Records, or testimony relaying the content of such records, shall not be used or disclosed in any civil, administrative, criminal, or legislative proceedings against the patient unless based on specific written consent or a court order;
  - (2) Records shall only be used or disclosed based on a court order after notice and an opportunity to be heard is provided to the patient or the holder of the record, where required by 42 U.S.C. 290dd-2 and this part; and
  - (3) A court order authorizing use or disclosure must be accompanied by a subpoena or other similar legal mandate compelling disclosure before the record is used or disclosed.
- Obligation extends to any entity through which Part 2 records flow
- Review BAAs with vendors that process SUD records

M | W

25

OF NOTE: PENDING HIPAA PRIVACY RULE UPDATE?

- Strengthen individuals' rights to access their own protected health information, including electronic information.
- Improve information sharing for care coordination and case management for individuals.
- Facilitate greater family and caregiver involvement in the care of individuals experiencing emergencies or health crises.
- Enhance flexibilities for disclosures in emergency or threatening circumstances.
- Support the use of telecommunications relay services by individuals and workforce members of HIPAA covered entities and business associates who are deaf, hard of hearing, deaf-blind, or who have a speech disability.
- Expand the Privacy Rule permission to use and disclose protected health information of Armed Forces personnel for national readiness purposes so that it applies to all uniformed services personnel.

Potential impacts for finance teams:

- Patients directing records to personal health apps of their choosing
- Shorter maximum response time for patient access requests
- New workflows and privacy risk considerations

M | W

26

OF NOTE: REPRODUCTIVE HEALTH PRIVACY RULE – VACATED

- Finalized April 2024; vacated nationally by Texas federal court in June 2025, HHS did not appeal
- Attestation requirements for reproductive health information disclosures are no longer in effect

Action item: Remove attestation workflows from billing processes and forms, ensure staff are not still collecting unnecessary attestations

M | W

27

IMPACT ON REV. CYCLE/AUDIT RESPONSE – CHANGE HEALTHCARE

- February 2024: largest healthcare data breach ever — **192.7 million** individuals affected
- Claims processing halted for weeks; massive revenue cycle disruption nationwide
- Root cause: remote access servers **lacked multi-factor authentication** (but was it Required? If Addressable, should it have been employed)
- Attackers spent 9 days inside the network before deploying ransomware
- Change still has not notified all affected individuals

M | W

28

IMPACT ON REV. CYCLE/AUDIT RESPONSE – CHANGE HEALTHCARE

- When a clearinghouse goes down, revenue stops — no claims submission, no payments, no eligibility verification
- Covered entities remain responsible for breach notifications even when the breach occurs at a business associate
- This underscores need for:
- Mandatory MFA on all ePHI systems
- Network segmentation
- 72-hour restoration capability
- Vendor diversification and contingency planning

M | W

29

IMPACT ON REV. CYCLE/AUDIT RESPONSE – CHANGE HEALTHCARE

In the Iowa District Court for Polk County

STATE OF IOWA, *ex rel.* BRENNA BIRD, ATTORNEY GENERAL

Plaintiff,

v.

CHANGE HEALTHCARE INC., UNITEDHEALTH GROUP INCORPORATED, and OPTUM, INC.,

Defendants.

Case No. _____

PETITION

WHEREFORE, the State of Iowa, ex rel. Attorney General Brenna Bird respectfully requests that this Court enter judgment against Defendants and:

A. Declare that Defendants violated the **Iowa Consumer Fraud Act**, Iowa Code § 714.16 et seq. and the **Personal Information Security Breach Protection Act**, Iowa Code § 715C et seq., by engaging in the unlawful acts and practices alleged herein;

B. Award the State civil penalties of **$40,000 per violation** pursuant to Iowa Code § 714.16(7);

C. Award the State civil penalties of **$5,000 for each violation** of the CFA committed against an older individual pursuant to Iowa Code § 714.16A(1).

D. Require Defendants to **disgorge** to the Attorney General all moneys or property acquired in violation of the Iowa Consumer Fraud Act pursuant to Iowa Code § 714.16(7); 27

E. Award the State **damages** on behalf of persons **injured** because of Defendants' violation of the Personal Information Security Breach Protection Act pursuant to Iowa Code § 715C.2(9);

F. **Enjoin** Defendants from committing or continuing to commit further unlawful practices pursuant to Iowa Code § 714.16(7);

G. Require Defendants to **pay all costs and fees for the prosecution and investigation** of this action pursuant to Iowa Code § 714.16(11); and

H. Grant **any such further relief** as the Court may deem appropriate

M | W

30

HEALTH CARE CLAIMS ATTACHMENTS RULE – BY MAY 26, 2028

- The Rule replaces fragmented, manual processes—such as faxing, mailing, and proprietary portal uploads—with a standardized electronic framework. It adopts the following specific standards:
- **Administrative Transactions:** Uses **ASC X12 Version 6020** for the 275 (Additional Information Submission) and 277 (Request for Additional Information) transactions.
- **Clinical Data Integration:** Adopts **HL7 Consolidated Clinical Document Architecture (C-CDA)** templates and the HL7 Attachments Implementation Guide (March 2022 version) to package clinical data like medical records, X-rays, and lab results.
- **Electronic Signatures:** Establishes a standard for secure, authenticated electronic signatures to be used specifically within these transactions.
- **Wins**: cost savings by eliminating manual workflows, faster reimbursements, reduced administrative burdens

M | W

31

SECURITY RULE - VENDOR AND BUSINESS ASSOCIATE MANAGEMENT

- The Proposed Security Rule requires annual written verification by BA that it has employed technical safeguards, **via SME analysis**
- Affects all vendors touching ePHI — billing companies, clearinghouses, RCM vendors, payment processors, coders, collection agencies

Best practices now:

- Request security posture documentation annually from key vendors
- Update BAA language to anticipate evolving requirements
- Assess BAAs for Part 2 compliance where SUD records are involved

M | W

32

NO SURPRISES ACT – ONGOING IMPLEMENTATION

- Effective January 1, 2022; several provisions still not fully implemented
- IDR operations rule expected to be finalized soon
- QPA calculation enforcement discretion extended until August 1, 2026 (TMA III litigation)
- Good faith estimate requirements for uninsured/self-pay patients already in effect
- Gag clause prohibition: annual attestation required

M W

33

NO SURPRISES ACT – ADVANCED EOB (COMING SOON)

- AEOB proposed rule targeted for March 2026, ***and …?***
- Would require health plans to send enrollees cost estimates incorporating provider good faith estimates
- Will create new data-sharing workflows between providers and plans
- PHI handling and HIPAA compliance implications
- Finance teams: begin preparing for provider-plan data exchange requirements

M W

34

FY 2026 IPPS/LTCH PPS FINAL RULE – SECURITY REQUIREMENTS

- Focuses on increasing security requirements for hospitals participating in the Medicare Promoting Interoperability Program.
- Hospitals and Critical Access Hospitals must attest Yes to completing full annual self-assessment using all 8 Guides, not just the High Priority Practices Guide.
- Begins with the EHR reporting period in Calendar Year 2026 (minimum 180-day period).
- Failure to do so will result in a **downward payment adjustment** for the applicable fiscal year.

M | W

35

RECOMMENDATION #1 – PERFORM/UPDATE YOUR RISK ANALYSIS

- This is the #1 current enforcement priority — Risk Analysis failures dominate OCR penalty assessments
- In 2026, OCR expands focus to include risk management (**mitigation** of identified risks)
- Include all finance systems: EHR billing modules, claims platforms, clearinghouse connections, payment processing, cloud-based RCM tools
- Document, document, document

M | W

36

RECOMMENDATION #2 – MAP YOUR ePHI DATA FLOWS

- Develop a technology asset inventory and network map for finance systems
- Document where ePHI enters, flows internally, and exits to vendors and payers
- Common blind spots: spreadsheets with patient data, email attachments, legacy systems
- This is a best practice now — but will be mandatory if proposed Security Rule is finalized

M | W

37

RECOMMENDATION #3 – STRENGTHEN VENDOR MANAGEMENT

- Begin requesting security documentation from key BAs
- Update BAAs for evolving HIPAA requirements and Part 2 obligations
- Avoid vendor concentration risk — Change Healthcare showed the consequences
- Proposed rule will formalize annual written verification requirement

M | W

38

RECOMMENDATION #4 – UPDATE NOTICE OF PRIVACY PRACTICES

- February 16, 2026 deadline for Part 2-related NPP updates
- NPP must explain how SUD records are handled
  - Pull the language from the Regulations at **42 CFR 2.22(b)(1)(ii)(H)** … or search 2.22 for "Notice of Privacy Practices" and scroll to (H)
- Applies to any entity through which Part 2 records flow
- Verify your compliance again, even if you think you have it right, today

M | W

39

RECOMMENDATION #5 – PREPARE FOR OCR AUDITS

Ensure documentation is audit-ready:

- Risk analyses and remediation plans, showing risk management
- Training records
- BAAs
- Policies and procedures
- Evidence of safeguard implementation
- Priority controls: MFA, encryption, access management, incident response

M | W

40

RECOMMENDATION #6 – TRAIN FINANCE STAFF ON HIPAA REQ'TS

- If they interact with ePHI, they need role-specific HIPAA training, more than generic annual awareness
- Key topics:
  - Minimum necessary standards in claims and billing
  - Proper handling of SUD records under Part 2
  - Breach identification and reporting obligations
  - Secure use of finance technology platforms

M | W

41

RECOMMENDATION #7 –STATE LAW PRIVACY COMPLIANCE

- Know the states of your insureds.
- Not all states exempt HIPAA regulated entities from state privacy law requirements (notice to AGs or DOIs, specific notification language or notification deadlines, relief afforded, applicability of consumer protection laws, etc.)
- **Ask your lawyers** to keep you apprised, build in that state law risk into to your incident response planning

M | W

42

RECOMMENDATION #8 –BCDR/REVENUE CYCLE DISRUPTIONS

- Study the Change Healthcare breach
- If it's on a network, hackers can get to it. So, have offsite, non-networked backups. Practice network segregation.
- Determine what you have that is a critical system. Build in alternative plans and options to get you back in operations within 72 hours if your primary option fails.
- Tabletop and plan, run it until it is smooth, document it for OCR.

M | W

43

44