


COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

# How Cybersecurity Plays an Integral Role With HIPAA Compliance

11/18/2024



1

---

---

---

---

---

---

---

---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

Chris Stocker

- Director of Client Services at Compass Computer Group, Inc.
- Director of Software Development at Fujifilm Healthcare Americas
- Epicor
- CU Boulder
- Compass handles the Cybersecurity



2

---

---

---

---

---

---


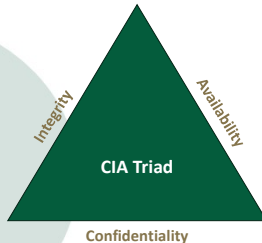
---

---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

### The CIA Triad

- Confidentiality
- Integrity
- Availability



3

---

---

---

---

---

---

---


---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

### Code of Federal Regulations (CFR)

This rule is codified under 45 CFR Part 160 and Part 164, Subparts A and C. The Security Rule mandates these three categories of safeguards:

- **Administrative Safeguards** (45 CFR § 164.308)
- **Physical Safeguards** (45 CFR § 164.310)
- **Technical Safeguards** (45 CFR § 164.312)



4

---

---

---

---

---

---

---

---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

### Developing a Cybersecurity Framework Aligned with HIPAA

How? Conduct a Risk Analysis regularly.

- Implement Administrative Safeguards
- Implement Physical Safeguards
- Implement Technical Safeguards
- Establish Policies and Procedures for Breach Response
- Continuous Monitoring and Improvement



5

---

---

---

---

---

---

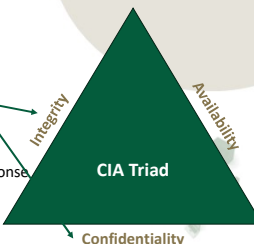
---

---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

### Tools and Technologies for HIPAA Compliance

- Administrative Safeguards – **Compliance Portal** for Policies and Procedures
- Physical Safeguards (Access Controls)
  - Security Cameras
  - Keycard Systems
  - Biometrics
- Technical Safeguards (Data Integrity)
  - BCDR
  - Audit Controls
  - Transmission Security
- Establish Policies and Procedures for Breach Response
- Continuous Monitoring and Improvement



6

---

---

---

---

---

---


---

---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

### Common Cybersecurity Threats in Healthcare

- Phishing
- Data Breach
- Ransomware
- DDoS Attacks
- Insider Threats



7

---

---

---

---

---

---

---

---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024



8

---

---

---

---

---

---


---

---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

### Understanding Risk Management and Vulnerability Assessment

- **Risk Management** is the ongoing process of identifying, assessing, and mitigating risks to an organization's assets, especially its information systems and data. In the context of cybersecurity, risk management involves evaluating potential threats to an organization's digital infrastructure and implementing strategies to reduce or eliminate these risks.
  - **45 CFR § 164.308(a)(1)** – Covered entities and business associates must implement a security management process. This process includes conducting regular risk analysis
- **Vulnerability Assessment** is a crucial part of risk management and focuses on identifying weaknesses in an organization's IT systems, networks, or applications that could be exploited by cyber threats.



9

---

---

---

---

---

---

---

---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

### Technical Safeguards Required by HIPAA

- 1. Access Control** (§ 164.312(a)(1))
  - a) Unique User Identification
  - b) Emergency Access Procedures
  - c) Automatic Logoff: Impl.
  - d) Encryption and Decryption
  - e) Continuous Monitoring
- 2. Audit Controls** (§ 164.312(b))
- 3. Integrity** (§ 164.312(c)(1))
- 4. Person or Entity Authentication** (§ 164.312(d))
- 5. Transmission Security** (§ 164.312(e)(1))
  - a) Integrity Controls
  - b) Encryption

10

---

---

---

---

---

---

---

---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

### Case Study: Cybersecurity Failures/HIPAA Breach

**Anthem, Inc. Data Breach (2015)**  
**Overview:** One of the largest health insurers in the US; massive data breach affecting ~79 million individuals. Hackers gained unauthorized access to the company's network by using stolen employee credentials.  
**Cause:** Several Cybersecurity failures, including:  
 Lack of encryption leaked information, such as names, SSNs, and medical identification numbers.  
 Weak internal access controls and failure to detect the attack in a timely manner.  
**Impact:** Exposure of PI, including names, birthdates, addresses, and SSNs. Anthem agreed to \$16 million settlement with the Department of HHS OCR—the largest HIPAA settlement at that time.  
**Key Lessons:**  
 Encryption both at rest and in transit, is a critical safeguard. Continuous monitoring and rapid response mechanisms are essential for detecting and addressing breaches early.

11

---

---

---

---

---

---

---

---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

### Case Study: Cybersecurity Failures/HIPAA Breach

**Premera Blue Cross Data Breach (2014)**  
**Overview:** Based in Washington, they suffered a cyberattack in 2014; breach of sensitive data belonging to 10.4 million people. The attackers had access to Premera's network for nearly nine months before detection.  
**Cause:** Vulnerabilities in IT infrastructure; failing to apply security patches and updates in a timely manner. Weak security measures allowed hackers to infiltrate systems, accessing SSNs, financial information, medical claims data, and PI.  
**Impact:** Faced multiple class-action lawsuits and paid \$74 million to settle claims. In addition, they reached a \$6.85 million settlement with the HHS OCR for failing to meet HIPAA requirements, particularly with regard to patching vulnerabilities and conducting risk analyses.  
**Key Lessons:** Regular and thorough risk assessments are crucial to identifying and mitigating potential vulnerabilities. Timely application of security patches and updates is vital to protecting against known vulnerabilities.

12

---

---

---

---

---

---

---

---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

Case Study: Cybersecurity Failures/HIPAA Breach

**University of Washington Medicine (UWM) (2018)**

**Overview:** In December 2018, the UWM discovered a data breach that exposed the ePHI of nearly 1 million patients. It occurred due to a misconfigured DB that was left exposed on the internet without proper security controls.

**Cause:**

- Technical misconfiguration in a server that allowed public access.
- Failed to conduct adequate risk assessments, which might have identified this vulnerability.

**Impact:** \$750,000 settlement with HHS OCR; violation of HIPAA's Security Rule, specifically not performing thorough risk analyses and failing to apply appropriate technical safeguards.

**Key Lessons:**

- Proper configuration and regular audits of systems and DBs are crucial to preventing unauthorized access to sensitive data.
- Conducting thorough risk assessments regularly can help identify potential security gaps.

13

---

---

---

---

---

---

---

---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

Case Study: Cybersecurity Failures/HIPAA Breach

**Touchstone Medical Imaging (2014-2017)**

**Overview:** A diagnostic medical imaging company; PHI of over 300,000 patients was exposed online. The exposure lasted for over a year, from 2014 to 2017, during which ePHI was accessible through search engines.

**Cause:**

- Misconfigured servers allowed public access to PI, including names, birth dates, SSNs, and imaging data.
- Failed to notify affected patients and did not properly conduct risk analyses.

**Impact:** Fined \$3 million by the HHS OCR, including inadequate risk analysis and lack of timely breach notification. This case highlighted the need for healthcare organizations to manage data stored on public-facing servers and ensure adequate security controls.

**Key Lessons:**

- Secure configuration and frequent audits of web-facing infrastructure are essential.
- Failure to notify patients in a timely manner can exacerbate the penalties and damage associated with a breach.

14

---

---

---

---

---

---

---

---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

Case Study: Cybersecurity Failures/HIPAA Breach

**Avamere Health Services (2022)**

**Overview:** a major operator of assisted living facilities, experienced a data breach that impacted 96 senior living and healthcare facilities. This breach exposed PI, including names, SSNs, and medical records, of around 380,000 individuals.

**Cause:** The vulnerability was caused by a third-party system breach, highlighting the risks associated with vendor and business associate relationships in healthcare organizations

**Impact:** Class Action lawsuits still underway

**Key Lessons:** Underscores the importance of cybersecurity measures like encryption, access control, and risk assessments in compliance with HIPAA regulations.

15

---

---

---

---

---

---

---

---

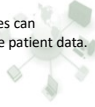
**COMPASS** COMPUTER GROUP, INC. *"Helping Direct Your Future"* 11/18/2024

### Case Study: Cybersecurity Failures/HIPAA Breach

**Conclusion**  
 These case studies illustrate the severe consequences of cybersecurity failures and HIPAA non-compliance, including large financial penalties, legal repercussions, and damage to reputation. The key takeaways emphasize the importance of:

- **Regular risk assessments** to identify vulnerabilities.
- **Encryption and access controls** to protect ePHI.
- **Timely patching and system updates** to mitigate security risks.
- **Monitoring and incident response** to detect and address breaches early.

Following HIPAA's requirements and implementing strong cybersecurity measures can significantly reduce the risk of breaches and ensure better protection of sensitive patient data.



16

---

---

---

---

---

---

---

---

**COMPASS** COMPUTER GROUP, INC. *"Helping Direct Your Future"* 11/18/2024

### HIPAA Compliance Checklist

**1. Administrative Safeguards**

- Risk Assessment
- Security Management Process
- Workforce Training
- Access Controls
- Incident Response Plan
- Business Associate Agreements (BAAs)

A simple HIPAA compliance checklist to help ensure that your organization meets the requirements of the HIPAA Privacy and Security Rules.



17

---

---

---

---

---

---

---

---

**COMPASS** COMPUTER GROUP, INC. *"Helping Direct Your Future"* 11/18/2024

### HIPAA Compliance Checklist

**2. Physical Safeguards**

- Facility Access Controls
- Workstation Security
- Device and Media Controls



18

---

---

---

---

---

---

---

---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024


HIPAA Compliance Checklist

**3. Technical Safeguards**

- Encryption
- Access Controls
- Audit Controls
- Integrity Controls

**4. Privacy Rule Compliance**

- Patient Rights
- Notice of Privacy Practices
- Minimum Necessary Standard



19

---

---

---

---

---

---

---

---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

HIPAA Compliance Checklist

**5. Breach Notification Rule**

- Breach Reporting

**Breach Reporting:** Develop a process for identifying and reporting breaches of unsecured PHI. Notify affected individuals and the HHS OCR within the appropriate time frame.



20

---

---

---

---

---

---

---

---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

HIPAA Compliance Checklist

**6. Ongoing Monitoring & Reviews**

- **Regular Audits:** Perform internal audits of policies and procedures to ensure ongoing compliance with HIPAA regulations.
- **Policy Updates:** Review and update policies to reflect changes in HIPAA laws, regulations, or the organization's operations.



21

---

---

---

---

---

---

---


---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

### HIPAA Compliance Checklist

**7. Documentation**

- **Policy and Procedure Documentation:** Maintain documentation of HIPAA policies, risk assessments, and compliance activities for at least **six years**.
- **Employee Acknowledgment:** Ensure all employees have reviewed and acknowledged understanding of HIPAA policies.
- This checklist is a foundational step for maintaining HIPAA compliance. Regular review and updates to these practices are critical in responding to evolving threats and regulations.



22

---

---

---

---

---


---

---

---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

### Quiz!




23

---

---

---

---

---

---

---

---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

### Preparedness

"Give me six hours to chop down a tree and I will spend the first four sharpening the ax"



"America will never be destroyed from the outside. If we falter and lose our freedoms, it will be because we destroyed ourselves."

— Abraham Lincoln

Failure to Manage Security Risks / Lack of a Risk Management Process

"There's no harm in hoping for the best as long as you're prepared for the worst."

— Stephen King

24

---

---

---

---

---

---

---

---



COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

## Compass Mission

Compass Computer Group's mission is to allow you to focus on your business and not worry about IT. We bring the best in Cyber Security, Operations and Business Continuity, providing you with premier infrastructure and security solutions. Our services and solutions were developed to ensure we are providing the most comprehensive IT support possible. Compass will navigate your company through the complexities of the ever-changing IT world.



25

---

---

---

---

---

---



---

---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

## How Compass Can Help

It's not a matter of IF, but WHEN  
Compass can do a PenTest and give your IT the results  
Compass has tools in our Managed Services that include  
HIPAA, Phishing and Cybersecurity Training  
HIPAA Compliancy

26

---

---

---

---

---



---

---

---

COMPASS COMPUTER GROUP, INC. "Helping Direct Your Future" 11/18/2024

## Thank You!

27

---

---

---

---

---

---

---

---