INFO 7374 - Cybersecurity Audit and Compliance
Week 4 Assignment

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

1. Risk Assessment Exercise:

Threat	Likelihood	Impact	Risk Level	Mitigation Strategy
Inadequate access controls for EMRs	High	High	Critical	Implement role-based access control (RBAC) and multi-factor authentication (MFA). Regularly audit user access.
Lack of employee training on data privacy	High	High	Critical	Conduct mandatory HIPAA compliance training and phishing awareness programs. Perform periodic assessments.
Weak password management policies	High	Medium	High	Enforce strong password policies, require MFA, and implement password rotation policies.
Unencrypted data transfers between facilities	Medium	High	High	Enforce end-to-end encryption for data in transit and implement secure VPNs.
Poor incident response plan	Medium	High	High	Develop and test a formal incident response plan, conduct regular breach drills, and establish clear escalation protocols.
Insider threats-inside employees accessing unauthorized data	Medium	High	High	Implement real-time monitoring and access logging. Implement alerts on u nusual patterns of access.
Outdated software and lack of patch management	Medium	High	High	Perform timely updates and patches for all systems. Automation of security updates is a must.
Physical Security Risks: Unauthorized access to the servers	Low	High	Medium	Biometric authentication, surveillance, and restricted access are used to secure data centers.

INFO 7374 - Cybersecurity Audit and Compliance
Week 4 Assignment

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

2. Compliance Gap Analysis Exercise:

HIPAA Requirement	WellCare's Controls/Status	Gap	Action Plan / Remediation
Data Access (164.312(a)(1))	Inadequate access controls for EMRs	Lack of role-based access controls (RBAC), multi-factor authentication (MFA), overprivileged users, and regular access audits	Implement RBAC(with least privileges) & MFA for all EMR systems; Conduct quarterly access audits to detect unauthorized access
Encryption (164.312(a)(2)(iv))	AES-128 for data at rest; Unencrypted data transfers; Some older systems store data in plaintext	Weaker encryption (AES-128); No encryption for data in transit; Older systems store plaintext data	Upgrade to AES-256 for all data; Encrypt data in transit using TLS 1.3 or VPNs; Secure backups with full-disk encryption
Breach Notification (164.404)	Insufficient incident response plan	Lack of formal breach detection, delayed reporting risk, and notification policies; No timeline enforcement	Create 72-hour breach escalation protocol with detection, containment, and 60-day notification compliance; Appoint a Data Protection Officer (DPO)
Employee Training (164.530(b))	Lack of employee training in data privacy practices	Employees unaware of HIPAA requirements and irregular compliance updates	Establish mandatory HIPAA training along with Bi-monthly training + phishing simulations. Conduct annual refresher courses & phishing awareness programs; Track training compliance
Audit Controls (164.312(b))	Logs retained for 30 days	Insufficient monitoring	Extend to 6 months + automated alerts

INFO 7374 - Cybersecurity Audit and Compliance
Week 4 Assignment

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

3. Data Encryption Review Exercise:

Review of Current Encryption Policies & Procedures

Data Type	Current Encryption Method	Issues Identified
Data in Transit	No encryption	Unsecured data transfers between facilities, increasing breach risks.
Data at Rest	AES-128 for newer systems; Plaintext storage for older systems	Older systems store sensitive patient data in plaintext, violating HIPAA security rules.
Backup Data	Limited encryption policies	Backup files may be vulnerable to unauthorized access.

Assessment Against Industry Standards

Standard	WellCare's Compliance
HIPAA Security Rule (Encryption is an addressable safeguard)	**Partially compliant –** Encryption is not uniformly applied.
NIST Guidelines (AES-256 recommended)	**Non-compliant –** AES-128 is used instead of AES-256.
TLS 1.2+ for Data in Transit	**Non-compliant** – Data transfers are unencrypted.

INFO 7374 - Cybersecurity Audit and Compliance
Week 4 Assignment

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

Identified Gaps & Corrective Actions

Gap Identified	Risk Level	Recommended Action
Unencrypted data transfers between facilities	Critical	Implement TLS 1.3 or VPN tunnels to secure data in transit.
Plaintext storage of patient data in older systems	Critical	Upgrade older systems to use AES-256 encryption and migrate plaintext data securely.
AES-128 encryption used instead of AES-256	High	Transition all systems to AES-256, the industry standard for strong encryption.
Lack of encrypted backups	High	Ensure full-disk encryption for backups and use secure cloud storage.
No formal encryption policy	Medium	Develop a comprehensive encryption policy covering data at rest, in transit, and backups.

Conclusion & Next Steps

WellCare's current encryption practices require immediate improvements to align with HIPAA and industry standards. The top priorities should be:

1. Encrypt all data in transit using TLS 1.3 or VPNs.
2. Migrate plaintext-stored patient data to AES-256 encrypted storage.
3. Implement AES-256 encryption across all systems for stronger security.
4. Secure backups with full-disk encryption to prevent unauthorized access.
5. Develop a company-wide encryption policy and train employees on secure data handling.