Security Controls Assessment: Electronic Health Records

Healthcare Case Study under HIPAA, HITECH and NIST Guidance

Case-study analysis of administrative, physical, and technical safeguards for a U.S.-based electronic health record environment.

HIPAA / HITECH | NIST CSF 2.0 | NIST SP 800-53 | Healthcare Security | IAM | Encryption | Resilience

AT A GLANCE

Scenario	A hospital EHR environment (Wanyonyi et al., 2017) re-analyzed as a U.S.-based organization subject to HIPAA, HITECH and the Breach Notification Rule
Method	Apply U.S. laws, policies, standards and baselines; evaluate the study's proposed controls; judge overall control effectiveness
Finding	Physical security works (97% rated effective) but administrative and technical controls are inconsistent or missing — the program is not effective as a whole
Outcome	Move to a managed security program: RBAC and MFA, encryption at rest and in transit, centralized logging, tested backups, recurring assessment

Sean Richard
sean@autom8ionlab.com · linkedin.com/in/a8l-sean-richard · +1.352.818.9694

Portfolio edition based on original Full Sail University coursework. Substantive project content is preserved; classroom-only submission headers were removed.

ASSUMPTION APPLIED As directed by the original case study, the hospital is treated as a U.S.-based healthcare organization. All other case-study facts remain unchanged, and U.S. laws, policies, standards, and security baselines are applied to the analysis.

01 — REGULATORY BASIS

U.S. laws, policies, standards and baselines applied

Laws

HIPAA Privacy Rule · HIPAA Security Rule · HITECH Act · HIPAA Breach Notification Rule

Policies

Access control · authentication & passwords · workforce security · training · audit logging · incident response · backup & contingency · media disposal · configuration & patching · physical & environmental

Standards & baselines

NIST CSF 2.0 · NIST SP 800-53 Rev. 5 (tailored moderate baseline) · NIST SP 800-66 Rev. 2

The primary U.S. legal and regulatory requirements applied to this case are the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule and Security Rule, together with the Health Information Technology for Economic and Clinical Health (HITECH) Act and the HIPAA Breach Notification Rule. The case study concerns an electronic health record (EHR) system containing patient information, so the hospital would be responsible for protecting protected health information (PHI) and electronic protected health information (ePHI). The HIPAA Security Rule requires reasonable and appropriate administrative, physical, and technical safeguards to preserve the confidentiality, integrity, and availability of ePHI. The HIPAA Privacy Rule also requires controls that limit uses and disclosures of PHI, including application of the minimum-necessary principle. HITECH and the Breach Notification Rule add accountability and notification requirements if unsecured PHI is compromised (U.S. Department of Health and Human Services [HHS], n.d.-a, n.d.-b, n.d.-c).

The policies applied to the case include access control, authentication and password management, workforce security and termination, security awareness and training, audit logging and review, incident response, backup and contingency operations, media protection and disposal, configuration and patch management, and physical and environmental security. These policies directly address the weaknesses reported in the case, including unauthorized access, social engineering, password sharing, failure to remove former users, inadequate backups, lack of encryption, weak multifactor authentication, blackouts, insufficient technical support, and limited training (Wanyonyi et al., 2017).

For standards and baselines, I applied NIST Cybersecurity Framework (CSF) 2.0, NIST Special Publication (SP) 800-53 Revision 5, and NIST SP 800-66 Revision 2 as practical U.S. guidance for implementing and evaluating healthcare security controls. NIST SP 800-53 provides control families covering areas such as access control, audit and accountability, configuration management, contingency planning, identification and authentication, incident

response, media protection, personnel security, physical protection, risk assessment, and system integrity. NIST CSF 2.0 provides a risk-management structure for governing, identifying, protecting, detecting, responding to, and recovering from cybersecurity risk. For this hospital, a tailored moderate-impact baseline is an appropriate starting point because compromise of EHR confidentiality, integrity, or availability could cause serious harm to patients and operations. The NIST baseline is used here as a security benchmark rather than as a claim that every private U.S. hospital is legally required to adopt NIST SP 800-53 (National Institute of Standards and Technology [NIST], 2020, 2024).

02 — PROPOSED CONTROLS

Evaluating the study's proposed additional controls

I agree with the controls proposed in Section 6.4 of the study because they address weaknesses that the case study actually measured. The proposed controls include proper media disposal, privileged-account ownership, frequent system audits, stronger identification and authentication, proper system configuration, automated off-site backups, improved physical security, environmental controls, power backup, system maintenance, and personnel security. These recommendations are appropriate because the study reported serious exposure to unauthorized access, social engineering, theft of records, lack of encryption, inadequate backups, weak access permissions, system breakdowns, insufficient multifactor authentication, and limited staff training. The study also found that the existing controls were uneven: physical security was viewed as effective by 97% of respondents, while automatic logoff, password controls, and multifactor authentication were rated much lower (Wanyonyi et al., 2017).

I would add several controls to make the security program more complete:

01 Role-based access control and least privilege, with periodic access reviews and immediate deprovisioning when employees leave or change roles.

02 Multifactor authentication required for EHR access, especially for privileged and remote accounts.

03 ePHI encrypted both at rest and in transit.

04 Centralized audit logging and security monitoring to detect abnormal access to patient records and privileged accounts.

05 A formal vulnerability and patch-management process, tested incident-response procedures, and regularly tested encrypted backups.

06 Recurring security-awareness training and phishing/social-engineering exercises.

These additions strengthen the administrative, physical, and technical safeguards expected by the HIPAA Security Rule and align the hospital's controls with NIST risk-management practices (HHS, n.d.-a; NIST, 2020).

03 — EFFECTIVENESS

Are the existing controls effective?

No. The existing controls are not effective as an overall security program. The case study shows that some individual controls work, particularly physical security, but the EHR environment remains exposed because the administrative and technical controls are inconsistent or missing.

REPORTED THREATS AND GAPS — SHARE OF RESPONDENTS (WANYONYI ET AL., 2017)

The study also states that basic safeguards such as a security professional, proper access-right allocation, removal of former users, power backup, and protections against unauthorized access had not been fully implemented. Effectiveness ratings were also weak for automatic logoff, password implementation, and multifactor authentication (Wanyonyi et al., 2017).

To increase effectiveness, the hospital must move from isolated controls to a managed security program with documented requirements, assigned control owners, measurable baselines, and recurring assessments. Identity and access management should enforce least privilege, role-based access, multifactor authentication, strong password rules, periodic access recertification, and immediate account removal upon termination or transfer. Technical controls should include encryption, secure configuration, endpoint protection, patching, vulnerability management, centralized logging, alerting, and routine audit review. Operational resilience should include automated off-site backups, restoration testing, UPS and generator capacity, environmental monitoring, and a tested contingency plan. Administrative controls should include recurring risk analysis, workforce training, incident-response exercises, personnel screening, and sanctions for policy violations. The hospital should then reassess the controls on a scheduled basis using defined performance measures. This approach is consistent with HIPAA's requirement to protect the confidentiality, integrity, and availability of ePHI and with NIST guidance for ongoing control assessment and cybersecurity risk management (HHS, n.d.-a; NIST, 2020, 2024).

References

Marron, J. (2024). *Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A cybersecurity resource guide* (NIST Special Publication 800-66, Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-66r2

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53, Rev. 5). https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

U.S. Department of Health and Human Services. (n.d.-a). *The Security Rule.* https://www.hhs.gov/hipaa/for-professionals/security/index.html

U.S. Department of Health and Human Services. (n.d.-b). *The HIPAA Privacy Rule.* https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

U.S. Department of Health and Human Services. (n.d.-c). *Breach Notification Rule.* https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Wanyonyi, E., Rodrigues, A., Abeka, S., & Ogara, S. (2017). Effectiveness of security controls on electronic health records. *International Journal of Scientific & Technology Research, 6*(12), 47-54.