Assignment 4.1: Cryptographic Controls

Joshua A. Wortz

University of San Diego

CSOL-510

Prof. Hoffman

06/01/2026

Context

National Health Systems (NHS) is a large, US-based healthcare organization that operates a hybrid network of central hospitals and remote outpatient clinics. The operating environment consists of thousands of mobile endpoints, laptops, and desktop computers used by clinicians and administrative staff to access and process patient records daily. Beyond these end-user devices, the infrastructure is comprised of a diverse range of interconnected systems, including specialized medical devices (such as imaging equipment and patient monitoring systems), network devices (like firewalls and secure routers), security cameras for physical access control, and Operational Technology (OT) components for managing facility and supply chain logistics. This vast and complex environment is critical for the continuous delivery of healthcare services. This delivery relies on a robust, data-driven infrastructure that supports Electronic Medical Record (EMR) systems and enables seamless data synchronization across multiple locations. Furthermore, the system must integrate sophisticated lab equipment for diagnostic testing and advanced pharmacy equipment for the management and dispensing of life-saving medications.

NHS's primary security goals center on ensuring the strict confidentiality, integrity, and availability of electronic Protected Health Information (ePHI) while maintaining a seamless, high-performance experience for healthcare providers (Information Technology HIPAA Security Rule, n.d.). The organization must guard against threats and hazards that could deny access to data or render it unavailable when needed, ensuring appropriate disaster recovery and business continuity for all departmental operations (Information Technology HIPAA Security Rule, n.d.). Given the complex landscape of mobile endpoints, EMR databases, and interconnected medical devices, a core objective for the NHS is to implement robust data and network safeguards,

including continuous security monitoring, threat and vulnerability management, intrusion detection, and anti-malware/patch management (Microsoft, 2011). By pursuing these objectives, NHS aims to eliminate unauthorized access, defend against cryptographic attacks, and ensure the continuous availability of critical health services and the synchronization of data.

To execute these objectives, NHS organizational policies mandate the rigorous application of administrative, physical, and technical safeguards across the enterprise. Endpoint and data security policies require that all ePHI at rest, especially on highly vulnerable mobile devices, laptops, and removable media, be secured with approved full-volume encryption solutions, such as BitLocker, before devices can connect to the corporate infrastructure. As demonstrated by the MD Anderson v. OCR case, failure to encrypt mobile devices that store ePHI poses a shockingly high risk to patients and routinely results in multi-million-dollar civil money penalties (Latham & Watkins, 2018). Furthermore, access control policies require dual-factor authorization for network access, along with strict physical access controls supported by biometric scanning and video surveillance (Microsoft, 2011). Finally, hardware lifecycle policies dictate that any devices or copiers with internal storage containing ePHI must be properly handled; disposal must comply with the internal Electronic Data Disposal Policy, and sending any hard drives to outside vendors for data recovery requires a formally executed Business Associate Agreement (Information Technology HIPAA Security Rule, n.d.).

As a large healthcare provider, National Health Systems (NHS) must strictly comply with federal data protection laws, most notably the Health Insurance Portability and Accountability Act (HIPAA) Security Rule and the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HIPAA Security Rule mandates the implementation of comprehensive administrative, physical, and technical safeguards to ensure the confidentiality,

integrity, and availability of all electronic Protected Health Information (ePHI). Furthermore, under the HITECH Breach Notification Rule, NHS is legally obligated to notify affected individuals, the Department of Health and Human Services (HHS), and potentially the media if unsecured ePHI is compromised. To mitigate this severe operational and financial risk, NHS organizational policies mandate alignment with the National Institute of Standards and Technology (NIST) guidelines and the use of Federal Information Processing Standard (FIPS) 140-2-validated cryptographic modules (Microsoft, 2021). By properly encrypting ePHI in accordance with these rigorous standards, NHS achieves a legal "safe harbor," making the data mathematically indecipherable to unauthorized users and exempting the organization from catastrophic breach notification requirements if a device is ever lost or stolen (American Medical Association, n.d.).

Controls

BitLocker Drive Encryption supports several robust encryption algorithms, primarily Advanced Encryption Standard (AES) operating in either Cipher Block Chaining (CBC) or XTS-AES modes, utilizing 128-bit or 256-bit key sizes (Microsoft, 2021). These two encryption modes differ significantly in their cryptographic design and resilience against attacks. In CBC mode, each block of plaintext is mathematically chained to the preceding ciphertext block using an Exclusive-OR (XOR) operation before encryption. Historically, the standard CBC mode presents specific vulnerabilities in full-disk encryption scenarios. Specifically, an attacker with physical access to the drive can flip arbitrary bits in a ciphertext block to manipulate the decrypted plaintext. At the same time, this randomization of the preceding block can still be exploited to alter executable files and introduce malicious code (NIST IR 8459, 2023). To

overcome these limitations, XTS-AES (XEX Tweakable block cipher with ciphertext Stealing) was introduced as the default algorithm for BitLocker (NIST IR 8459, 2023). XTS-AES is purpose-built for storage devices; it independently encrypts each 128-bit data block using a unique "tweak" value based on the sector's logical position, ensuring that identical plaintexts stored in different sectors produce completely different ciphertexts (NIST IR 8459, 2023). Furthermore, XTS-AES utilizes two distinct AES keys simultaneously, essentially requiring twice the key material, and is mathematically proven to be a strong pseudorandom permutation that is secure against chosen-ciphertext attacks (CCA) that can break CBC mode (Mammeri, 2024). Because XTS-AES effectively neutralizes targeted data manipulation on storage media, it remains the highly recommended algorithm for securing operating systems and fixed data drives (Microsoft, 2025).

BitLocker Drive Encryption provides a comprehensive suite of cryptographic components and security assets designed to protect data across an enterprise environment. At its core, the solution delivers full-volume data protection components for operating system (OS) drives, fixed data drives, and removable media via the "BitLocker To Go" feature (Microsoft, 2017). To securely authenticate users and unlock these encrypted volumes, BitLocker relies on various key protector components, which can be configured to require robust multi-factor authentication; these include integration with a hardware Trusted Platform Module (TPM), user-configured startup PINs ranging from 4 to 20 digits, USB startup keys, and Network Key Protectors that automatically unlock OS drives when the device is connected to a trusted wired corporate Local Area Network (LAN) (Microsoft, 2017; Microsoft, 2025). Because unexpected lockouts can occur due to forgotten PINs, hardware changes, or TPM anti-hammering lockouts, BitLocker generates critical recovery assets to ensure data is not permanently lost (Microsoft,

2017). These primary recovery assets include a 256-bit recovery key, certificate-based Data Recovery Agents (DRAs), and a 48-digit recovery password that can be automatically backed up to Active Directory Domain Services (AD DS) during provisioning (Microsoft, 2017; Microsoft, 2025). Furthermore, BitLocker can export a cryptographic key package asset, which is particularly vital for disaster recovery, as it enables the BitLocker Repair tool (repair-bde) to decrypt and salvage block-level data from severely damaged or physically corrupted drives, even when normal passwords fail (Microsoft, 2017). Finally, organizations can leverage management components such as the Microsoft BitLocker Administration and Monitoring (MBAM) tool and the BitLocker Recovery Password Viewer to centrally manage these recovery assets and monitor encryption compliance across all endpoints (Microsoft, 2017).

BitLocker Drive Encryption provides several critical components and assets to secure an environment. These include full-volume data protection for operating systems and fixed drives, as well as "BitLocker To Go" for protecting removable data drives. Authentication components include integration with the Trusted Platform Module (TPM), user-configured PINs, USB startup keys, and Network Key Protectors. Additionally, BitLocker generates vital recovery assets, such as a 48-digit recovery password, Data Recovery Agents (DRAs), and a cryptographic key package for recovering data from physically corrupted drives.

Starting in Windows 11, Personal Data Encryption (PDE) was introduced to work alongside BitLocker. While BitLocker provides full-volume encryption that releases its decryption keys at system boot, PDE focuses on encrypting individual files and protected folders by linking the encryption keys directly to the user's Windows Hello for Business credentials. Consequently, PDE offers an additional layer of security by discarding its decryption keys the

moment the user signs out or the Windows lock screen engages, rendering the files inaccessible even if the device remains powered on.

Implementation

Our strategy for auditing the environment will rely on the Microsoft BitLocker Administration and Monitoring (MBAM) tool and configuration service providers (CSPs) via Microsoft Intune (Microsoft, 2017; Microsoft, 2024). These tools will continually monitor device compliance and automatically test configuration settings before and after network maintenance to ensure all laptops and workstations successfully enforce BitLocker policies (Microsoft, 2011).

For encryption keys and authentication, the strategy will require multi-factor authentication at startup for all operating system drives. Devices will be configured to use the TPM in conjunction with a startup PIN (ranging from 4 to 20 digits) to ensure that possession of the physical device alone is insufficient to boot the operating system and access the decryption keys (Microsoft, 2024).

Our BitLocker provisioning strategy will leverage Microsoft Endpoint Manager and Windows Autopilot (Microsoft, 2021). This allows us to silently trigger encryption on all compliant drives during the initial out-of-the-box setup, ensuring devices are delivered to end-users fully locked down and compliant with NHS security policies without requiring user intervention (Microsoft, 2021).

Integrating BitLocker with Active Directory Domain Services (AD DS) offers the major advantage of automatically backing up both the 48-digit recovery passwords and the key packages to a centralized, secure repository, ensuring IT can recover data if a user forgets a PIN or hardware fails (Microsoft, 2017). However, a key consideration and potential drawback is that

if the policy "Do not enable BitLocker until recovery information is stored in AD DS" is enforced, devices must have active connectivity to the domain controller during initial provisioning, which can complicate deployments for remote users (Microsoft, 2017; Microsoft, 2024).

References

American Medical Association. (2018). HIPAA Security Rule: Frequently asked questions regarding encryption of personal health information.

Information Technology HIPAA Security Rule. (n.d.).

Latham & Watkins. (2018). MD Anderson v. OCR: Key takeaways.

Mammeri, Z. (2024). Cryptography: Algorithms, protocols, and standards for computer security (1st ed.). John Wiley & Sons.

Microsoft. (2011). Addressing HIPAA security and privacy requirements in the Microsoft cloud.

Microsoft. (2017). BitLocker recovery guide. Microsoft Learn.

Microsoft. (2021). Windows 11 security book: Powerful security from chip to cloud.

Microsoft. (2022). Introducing Personal Data Encryption, securing user data before login and under lock. Microsoft Community Hub.

Microsoft. (2024). Configure BitLocker. Microsoft Learn.

Microsoft. (2025). Personal Data Encryption overview. Microsoft Learn.

Mouha, N., & Dworkin, M. (2023). Report on the block cipher modes of operation in the NIST SP 800-38 series (NIST IR 8459 ipd). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8459.ipd