BioHuman Shareholder Report

Daniel C. Pelzl, Elena Sergeeva, & Max Eleff

Department of Cyber Security, University of San Diego

CSOL-510-02-FALL-2023-A – Applied Cryptography

Dr. William Hess

October 9th, 2023

Table of Contents

Table of Figures:

Organizational Needs

Company Overview

BioHuman is a pharmaceutical company that collaborates with research teams worldwide to improve our customers' lives. The BioHuman information systems are used by 500 employees, collaborators, and clients for treatments for life's ailments. The research performed by BioHuman relies on clinical trials, testing, research, and collaboration. The network comprises a range of devices, including Windows Active Directory, Domain Controller, Data, print, 365/Exchange, telecommunications, web servers, and Virtual Machine servers. There are also end-user devices, including workstations, research devices, Biomedical devices, legacy research, imaging, data processing, laptops, cellular, and specialty machines. Most machines run current Windows operating systems, with cellular devices running current Android or Apple software.

Security Goals

The information system's security goal at BioHuman is simply no patient data compromises. A simple goal is required by American law; however, many controls and procedures are required to perform at the highest level at all times. At BioHuman, verifiable guarantees are required to improve the lives of the stakeholders. At the financial level, cyber security protections consume up to 25% of the budget. A compliance violation can result in $50,000 fines and immeasurable damage to public trust (Tampa Bay Compliance, n.d.). BioHuman receives substantial funding from the National Institute of Health, and a NIST violation can result in the loss of future grants (HHS, 2022).

Policies and Controls

The chief information security officer (CISO) will ensure that information systems are appropriately secured and adjust policies as required. A compliance officer will ensure policies and

controls are appropriately implemented to avoid violations and document all findings to allow for corrections and improvements. A risk analysis will be performed using real-time network data to determine the proper controls for each device. Industry best practices will be implemented to ensure HIPAA compliance for all devices handling patient data. Data loss prevention will be implemented to limit the risk of information exfiltration, focusing on insider threats. When possible, data anonymization will be implemented to limit the extent of personally identifiable information stored on BioHuman systems. Monitoring and event logging measures will be implemented to meet compliance and provide a baseline of activity to identify anomalous activity. Physical access will be limited to approved individuals and require proper authorization, including government identification and badging systems. Monitored surveillance systems will be utilized to ensure that physical security is maintained. Information system and network access, including web access or remote connections, will require multi-factor authentication and account approval through a multi-tiered review process. Password security, authentication tokens, and approved device scans will also be required to access the network. Training sessions will be a prerequisite for all individuals to gain authorization to access the network and continue education courses annually for reauthorization. A Just Enough Administration policy will be employed to limit elevated privileges only to individuals who are authorized access and only for the period that is required (Wilson, & Wheeler, 2022). When Patient information is required, a third-party service will be employed to ensure proper standards are utilized and provide uniformity with partner organizations. The Epic EMR system provides instant integration with more than 75% of American medical institutions and can help transfer liability to an industry leader. All communications over the network will utilize encryption, and remote access will require full end-to-end tunneling. Web access will only allow individuals to access their information through the Epic system after authorization has been approved by the individual and BioHuman. In addition to data in transit requiring encryption, resting data will have

encryption to limit the risk of further information exposure. Intrusion prevention systems, firewalls, spam filters, forward link blocking, antivirus, and cyber intelligence tools will be utilized to reduce the risk and increase the mitigation time of an attack. All third-party hardware, software, and partner organizations must meet NIST information security standards to reduce external risk factors. Network segmentation and baseline settings will help ensure proper controls are in place to protect PII. At the same time, low-impact systems are segmented and baselined to industry standards without overburdening these systems. An incident response team will be responsible for preparing a HIPAA-compliant course of action to address events as they occur. Additionally, several exercises will be performed yearly to train individuals and strengthen the response plan (AAPCPS, 2011).

Compliance

BioHuman information systems manage patient information and must comply with HIPAA and HITECH regulations. HITECH is an update to HIPAA, requiring controls and policies to prevent private patient information from being released to unauthorized individuals. The regulations include Administrative safeguards detailed in HIPAA 164.308, security management, workforce security, information access, security awareness training, and associate contract assurance. Physical safeguards under HIPAA 164.310, workstation use, workstation security, and device controls. Technical safeguards HIPAA 164.312, access controls, audit controls, integrity, authentication, and transmission security. Notifications of a breach are also required to complete compliance with HIPAA and HITECH (AAPCPS, 2011). All organizations receiving federal funding must comply with NIST standards for information systems (HHS, 2022). The NIST 800-171 standards contain information for controlled unclassified information, which may include research information created by BioHuman. NIST 800-53 and 800-171 detail more than one hundred controls that may be required for a given system to ensure the

information remains secure. The NIST cybersecurity framework provides information for industry best practices to ensure that all systems are configured and operating most securely (Wisdom, 2022).

Cryptographic Controls

Encrypted Hard Drives

At BioHuman, customer data privacy and integrity are held to a high standard. The way that data is stored and accessed is more mobile than ever, so to keep this promise, all computers will be utilizing encrypted hard drives. All Apple computers will use the Apple-developed FileVault encryption, and Windows devices will use a Microsoft-developed encryption standard called BitLocker. These cryptographic operations ensure that the data on all company devices cannot be accessed if the device is lost or stolen. Even if the internal hard drive is removed from the device, the data is useless to any pending threat actors because they cannot read or access any data because of these encryption standards.

Apple's in-house encryption standard, FileVault, is an excellent tool for keeping the data on Apple devices running macOS. "FileVault is a disk encryption feature built into MacOS / Mac OS X, FileVault provides 128bit AES encryption with a 256 bit key to encrypt the disk and all files located on the drive." (OS X Daily, n.d.). In tandem with Apple's T2 Security chip, it gives the device additional security features such as additional drive encryption, secure boot, Mic Drop, and Touch ID. "If you have a Mac with Apple silicon or an Apple T2 Security Chip, your data is encrypted automatically. Turning on FileVault provides an extra layer of security by keeping someone from decrypting or getting access to your data without entering your login password." (Apple, n.d).

BitLocker Drive Encryption

On the Microsoft side, Microsoft uses its form of encryption called BitLocker. BitLocker is included on all Pro and Enterprise versions of Windows. "It uses the Advanced Encryption Standard algorithm with 128- or 256-bit keys. BitLocker combines the on-disk encryption process and special key management techniques. BitLocker uses a specialized chip called a Trusted Platform Module (TPM). The TPM stores Rivest-Shamir-Adleman encryption keys specific to the host system for hardware authentication. The TPM is installed by the original computer manufacturer and works with BitLocker to protect user data." (Gillis, n.d). Since the encryption keys are stored within the device's TPM, if the hard drive were removed and plugged into another device, it would be unreadable without the BitLocker decryption key. BitLocker will only encrypt the data on the drive, making the encryption process much faster than traditional encryption methods.

Personal Data Encryption (PDE)

With Windows 10 coming end-of-life at the end of 2025, moving all new Windows devices to the Windows 11 environment will help the IT team from having a major OS upgrade push at the end of 2025 to stay in compliance. Moving to Windows 11 also has additional security features that benefit the end users. One of those security features is called PDE. "Personal Data Encryption (PDE) is a security feature that provides file-based data encryption capabilities to Windows. PDE utilizes Windows Hello for Business to link data encryption keys with user credentials. When a user signs in to a device using Windows Hello for Business, decryption keys are released, and encrypted data is accessible to the user. When a user logs off, decryption keys are discarded and data is inaccessible, even if another user signs into the device." (Matarazzo, 2023). PDE and BitLocker are two different encryption standards and are different, but PDE should be used in addition to BitLocker, adding an additional layer of security. PDE only encrypts the files on the machine, whereas BitLocker encrypts the entire hard drive. BitLocker starts

at the machine's boot, where PDE starts when the user logs into the machine. BitLocker stores the encryption keys within the TPM, whereas PDE stores the keys within the user's Microsoft account. PDE uses AES-CBC with a 256-bit key and can be utilized automatically with applications such as Microsoft Outlook when enabled. (Matarazzo, 2023). PDE can also be set up depending on organizational needs. It is important to know that PDE does not protect the machine when accessed via Microsoft's RDP remote desktop, and PDE does not encrypt files stored on a server drive. PDE is also not a backup utility, so utilizing Microsoft OneDrive to back up the machine is still recommended.

Recommendations

BitLocker Use Policy

All devices with PII will use encryption to secure data at rest. BitLocker is not required if a device will not store personal information and is segmented from the rest of the network to limit the ability to access PII. Any regulations, such as HIPAA, that require encryption at rest will be implemented (*AAPCPS, 2011)*. Microsoft's MBAM is utilized to synchronize recovery keys to Active Directory. Only vetted information technology professionals working on authorized service ticket requests are eligible to request JEA access to the key for the specified device. The technician will receive the key when access is granted through an approval process involving a direct manager and department head *(Buck et al., 2023)*. Technicians must log in to an administrative virtual machine after receiving an authorization token to retrieve the key. To log into the virtual machine, the technician must also present a JEA virtual account token and a physical token, verify their password pin, and act as their approved device within a BioHuman facility. The IT department employees undergo background checks and training before joining their team. The process then requires a review of the circumstances surrounding the key request to recover BitLocker. The end user must enter a ticket request to record a BitLocker incident and the failed events. A BitLocker issue can often indicate a security concern, including malware, ransomware, or

unauthorized system tampering. With the required information documented, the review will present the key to the authorized technician, who will then be able to retrieve the key (Matarazzo, 2023b).

BitLocker Authentication

For system protection, BitLocker can be used to encrypt the operating system volume of a drive. This encrypts all system files except for the system partition, which includes the Windows boot manager and core system files required to boot the operating system once the key is available. The TPM 1.2 device is used to ensure boot configurations are secure. The Unified Extensible Firmware Interface (UEFI) authenticates the bootloader with Secure Boot. Secure Boot blocks untrusted firmware and bootloaders from being loaded with the system to ensure no changes have been made since the last system operation. If any failures or changes occur during the secure boot process, the BitLocker key will be required to access the file system and boot the operating environment. Authentication with BitLocker can be configured using a startup key administered with Group Policy. BitLocker keys are accessed and stored in memory only after successfully completing the pre-boot and safe boot process. The startup key can authenticate that the system is uncompromised and that the authorized user is initiating the system boot. BitLocker includes anti-hammering rules that prevent a brute force attack that requires the full BitLocker recovery key after unsuccessful pin attempts. An organization can also use a Network Unlock, which acquires a key from a network authentication server if the device is within a physical network environment (Matarazzo & Pamnani, 2023). At BioHuman, several systems only require a baseline level of BitLocker protection. Some devices are not at risk of being moved offsite and utilize several access controls to prevent tampering. An email server, non-patient data server, and virtual machine servers can be protected with baseline policies. Many of these devices may be prone to configuration changes, including hard drives or memory swaps, to prevent failures that may trigger BitLocker alerts. To prevent extended recovery times, a baseline configuration may be used. Additional systems not accessing

sensitive data may also be configured with a minimum baseline. Janitorial services, for example, are segmented from sensitive information and would not require hardened policies. Some areas need increased BitLocker security over the baseline, such as devices containing patient data, especially mobile devices and laptops with PII. Some devices may require a median security improvement, such as those containing anonymized data that does not contain PII. The data on these devices may still be sensitive and require additional protections from the baseline policies (Matarazzo, 2023b). BioHuman demands multi-factor authentication for access to company hardware and the network. Smartcards are the preferred secondary authentication method as they offer access to secure public keys and shared private keys for each user. Smartcards also integrate across several platforms, including device login, Windows authentication, network access, and Epic systems. Smartcards also serve as physical access badges to simplify the authentication process for employees entering BioHuman locations (IBM, 2013). Some devices, such as mobile phones, may have difficulty utilizing smartcards, and alternative options may be approved, including X.509 certificates and RSA-style authentication code systems (Flores et al., 2023).

TPM hardware configurations

The Trusted Platform Module (TPM) is a significant component when taking advantage of advanced cryptography security provided by Windows operating systems. It is required for a device running Windows 11 to have a TPM 2.0 chip built into the machine. Without it, the device will not be eligible for Windows 11 upgrade. Since the organization uses Dell computers for Windows devices, Dell made TPM a standard in 2015 on all devices (Dell, 2023). To verify that a system has TPM 2.0 installed, it can be easily checked by running tpm.msc as a Run Command to open the Trusted Platform Module (TPM) Management application within Windows to see if the device has the chip and what version. Figure 1 gives an example of this application.

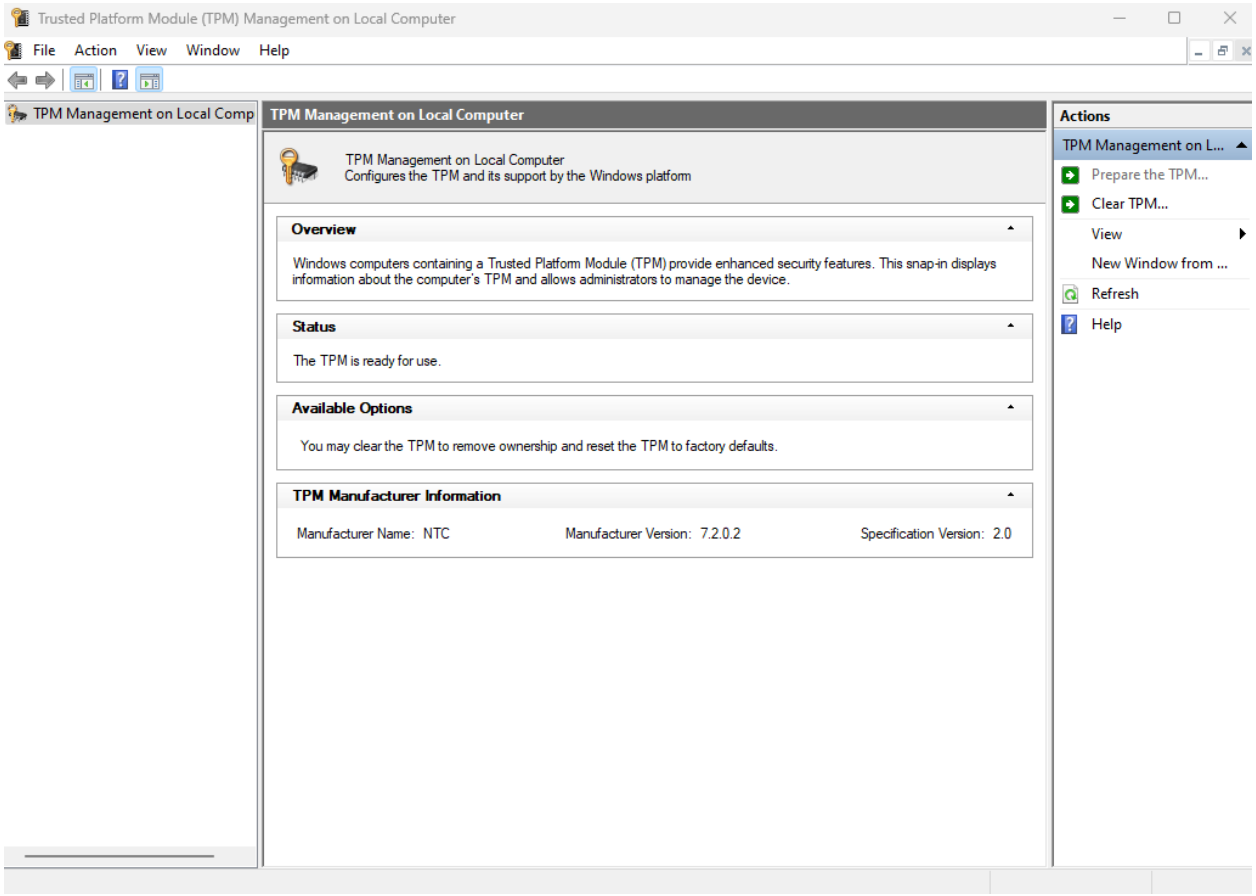

Figure 1: *Example of checking to see if a system has TPM installed.*

(Pelzl, 2023)

Non-TPM hardware configurations

Older devices that do not have TPM chips do not have to be replaced. They still can be used within the organization, but they will not be able to take advantage of the TPM advantages within Windows 11. However, Windows 10 is still a supported and secure platform for another two years before its end-of-life in October 2025. These devices can still enable BitLocker to drive encryption on these older machines by storing the encryption keys on an external flash drive. This alone would not be good security if the USB drive were lost or stolen, but by utilizing Windows To Go Workspace, these older machines can be encrypted, and these USBs are also encrypted, so if they were lost or stolen, the drive

could not be compromised. “When BitLocker is enabled, the user must provide a password to unlock the drive and boot the Windows To Go workspace. This password requirement helps prevent unauthorized users from booting the drive and using it to gain access to your network resources and confidential data. Because Windows To Go drives are meant to be roamed between computers, the Trusted Platform Module (TPM) can't be used by BitLocker to protect the drive. Instead, you'll be specifying a password that BitLocker will use for disk encryption and decryption.” (Microsoft Learn, 2023). The downside of using Windows To Go is that it requires the USB drive to be inserted into the device before each startup, and the speed of the interaction depends on the USB device and port speed. This feature was discontinued in 2019, will no longer be updated after Mac 2020, and will be removed entirely from Windows 10 with version 2004 (Vera, 2023). Windows To Go should be used as a temporary solution, and these older devices should be replaced with newer ones with TPM 2.0 chipsets.

Disk configuration considerations

BitLocker is designed to protect the user's data on the hard drive. It does this by splitting the drive into two separate partitions. These two partitions consist of the Operating System Partition, which houses the boot files necessary to start the computer, and the System Partition, which houses the operating system and all your data. “Two partitions are required to run BitLocker because pre-startup authentication and system integrity verification must occur on a separate partition from the encrypted operating system drive. This configuration helps protect the operating system and the information in the encrypted drive.” (Matarazzo, n.d.). By separating the System Partition from the Operating System Partition, BitLocker ensures that the computer can start securely, even before the main operating system is loaded. It also prevents attacks that might tamper with the boot process to bypass encryption. In short, BitLocker uses two partitions to ensure a secure boot process and protect the computer from unauthorized access while allowing the operating system and data to remain encrypted and secure.

BitLocker provisioning Strategy

To ensure that all Windows devices are on BitLocker, all tech teams will have to meet to figure out the best way to get BitLocker provisioned within the organization. The first requirement is that when new machines are imaged with the BioHuman Corporate image of Windows 11, the machines will be enabled with BitLocker during this process. If a machine is out of warranty and up for an upgrade, it can be eligible for a replacement with one of these new devices. The current machines in use and under warranty will have to be unencrypted with the current encryption standard and encrypted with BitLocker. This can happen in one of two ways. The first way would be to have the user bring the machine in and have it reimaged with Windows 11, granting them an OS upgrade. The second method might be possible for the desktop engineering team to set up a Windows 11 upgrade, in which a BioHuman company installer will run on the machine, which will decrypt, encrypt with BitLocker, and then upgrade to Windows 11. This can first be tested across all IT teams and must ensure that applications are tested within Windows 11 before upgrading the device. Machines that do not have TPM chipsets should be replaced to ensure they can take advantage of the additional security benefits of Windows 11. User data should be backed up before upgrading if something gets corrupted during decryption; the user does not lose all of their data. Information on this rollout should be sent out to all users so that they are notified of this upcoming rollout, providing them with information on why it is happening and how it will help strengthen the company's security and compliance with Windows 10 coming end-of-life. In case of issues, the BitLocker rollout will have to be set in different rollout schedules so the desktop support team is not overrun with users who cannot work. All desktop support teams should be trained to know where these BitLocker keys will be stored and how to access them if a user gets a BitLocker lockout screen at boot. The situation the company does not want to find itself in is

having to hire additional resources to do a massive Windows 11 upgrade at the end of 2025. It is cheaper to get ahead of it and start future-proofing company devices.

Used Disk Space Only Encryption

Encrypting an entire disk space can take a significant amount of time, ranging between hours and days, depending on the amount of data, since it is encrypted every byte on the volume, including areas that do not have data. Used Disk Space Only encryption method encrypts data currently used or written in the future.

The advantage of the Used Disk Only encryption method is the reduced time required to encrypt data; sometimes up to 99% less time taken (Cocosenor, n.d.) The best practice is to implement Used Disk Space Only encryption when the endpoint is new; the main reason is to account for the deleted files. Deleted or moved files on the system that have been used may not be marked and, therefore, can be read by forensic tools as plain text. At BioHuman, the Bitlocker Full Disk Encryption method is selected to secure all data on all devices in use, as this method is considered the most secure way to protect PII and other confidential data.

Active Directory Domain Services Considerations

BioHuman has taken the necessary steps to ensure that BitLocker can be integrated with Active Directory Domain Services to provide centralized key management. This integration allows the recovery key for each device to be kept safe, which is essential for recovering encrypted data in the event of a lost user key. However, there are some considerations to remember, such as the potential for system slowdowns due to Bitlocker's impact on hard drive speed. Group Policy should be fully implemented before enabling BitLocker to guarantee that recovery information is automatically backed up to Active Directory. Additionally, the Active Directory schema should be able to contain the required attributes

and classes to host BitLocker Drive Encryption. At BioHuman, we have taken the appropriate steps to ensure that the Active Directory Domain Service is configured to operate the BitLocker service effectively.

FIPS support for recovery password protector

To comply with NIST 800-171, BioHuman must also comply with FIPS 140-2, which mandates using FIPS mode BitLocker. FIPS 140-2 is a government-approved encryption standard. Products certified to meet the FIPS 140-2 standard remain valid for five years (NIST, 2008).

Any BioHuman system containing patient information or proprietary data, such as staff laptops, servers, databases, and backup utilities, will have FIPS mode Bitlocker installed. FIPS mode does not allow creating or using a recovery password because FIPS 140-2 prohibits password-deriving keys for data encryption/decryption. Therefore, only FIPS-compliant authentication and recovery mechanisms will be used, and only a recovery key can be used for recovery purposes. The benefit of using FIPS-enabled BitLocker is that it provides a more robust way to ensure the confidentiality and integrity of data by limiting how information can be retrieved. BioHuman will follow the security policies for safe storage, backup, and retrieval of the key, as it is essential for the continuous operation of BioHuman systems.

Conclusion

Healthcare organizations like BioHuman must safeguard sensitive patient data through reliable security best practices. This report has examined BioHuman's systems, processes, and operations, recommending implementing security controls and procedures to comply with relevant laws, regulations, and standards. These measures include Administrative, Physical, and Technical controls, all aimed at safeguarding protected health information from unauthorized access. To maintain compliance,

BioHuman must maintain comprehensive documentation of its security efforts and regularly review and update its controls, policies, and procedures to remain agile and proactive in addressing and mitigating potential risks. Securing patients' data in the healthcare industry is a challenging task that requires careful planning, attention, and continuous effort. At BioHuman, the ultimate goal is zero compromises to patient data security.

References

AAPCPS. (2011). *HIPAA Security and HITECH Compliance Checklist*. http://aapcperfect.s3.amazonaws.com/3f227f64-019f-488a-b5a2-e864a522ee71/93474f1d-58b3-4364-b060-790f48531f8a/71e98110-fafe-4880-8449-bddfbef5efa6.pdf

Apple. (n.d.). *How does filevault work on a Mac?*. Apple Support. https://support.apple.com/guide/mac-help/how-does-filevault-work-on-a-mac-flvlt001/mac

Buck, A., Czechowski, A., Mardahl, M., Paniagua, S., Paunovic, D., Rojas, F. (2023). *Microsoft BitLocker Administration and Monitoring 2.5.* https://learn.microsoft.com/en-us/microsoft-desktop-optimization-pack/mbam-v25/

Cocosenor. (n.d.). BitLocker Full Disk Encryption vs Used Disk Space Only. https://www.cocosenor.com/articles/computer/bitlocker-full-disk-encryption-vs-used-space-only.html

Dell. (2023, August 8). *Trusted platform module (TPM) frequently asked questions for windows 11*. Trusted Platform Module (TPM) Frequently Asked Questions for Windows 11 . https://www.dell.com/support/kbdoc/en-us/000190999/trusted-platform-module-frequently-asked-questions-for-windows-11

Flores, J., Gill, C., Hall, J., Ommi, N., Rang, V. (2023). Overview of Microsoft Entra certificate-based authentication.https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-certificate-based-authentication

Gillis, A. S. (n.d.). *What is bitlocker? definition from searchenterprisedesktop*. Enterprise Desktop. https://www.techtarget.com/searchenterprisedesktop/definition/BitLocker

HHS. (2022). National Institutes of Health grant program cybersecurity requirements need improvements. https://oig.hhs.gov/oas/reports/region18/182006300.pdf

IBM. (2013). Epic Integration Guide. https://www.ibm.com/docs/en/SS9JLE_8.2.1/com.ibm.itamesso.doc_8.2.1/IBM_SAM_ESSO_EPIC_pdf.pdf

Matarazzo, P. (2023, August 25). *Personal Data Encryption (PDE) - windows security. Windows Security | Microsoft Learn.* https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/personal-data-encryption/

Matarazzo, P. (2023b). Prepare an organization for BitLocker: Planning and policies. https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/prepare-your-organization-for-bitlocker-planning-and-policies

Matarazzo, P., Pamnani, V. (2023). BitLocker Countermeasures. https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/bitlocker-countermeasures

Matarazzo, P. (n.d.). *Bitlocker FAQ - Windows Security*. Windows Security | Microsoft Learn. https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/faq

Microsoft Learn. (2023, February 27). *Security and data protection considerations for windows to go (windows 10) - windows deployment*. https://learn.microsoft.com/en-us/windows/deployment/planning/security-and-data-protection-considerations-for-windows-to-go

NIST. (2008, July 07). BitLocker Drive Encryption Security Policy. For FIPS 140-2 Validation. https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp1053.pdf

OS X Daily. (n.d.). What is filevault? filevault for Mac explained.

https://osxdaily.com/what-is-filevault/#:~:text=FileVault%20is%20a%20disk%20encryption,files%20located%20on%20the%20drive.

Pelzl, C. (2023) Student's computer screen

Tampa Bay Compliance (n.d.). HIPAA–HITECH Non-Compliance. https://tampabaycompliance.com/resources/hipaa-hitech-non-compliance/

Vera. (2023, June 21). *The end of windows to go is announced by Microsoft now*. MiniTool.

https://www.minitool.com/news/end-of-windows-to-go.html

Wilson, C. & Wheeler, S. (2022). Just Enough Administration.

https://learn.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview?view=powershell-7.3

Wisdom, A. (2022). A Complete NIST Compliance Checklist. https://www.datalinknetworks.net/dln_blog/a-complete-nist-compliance-checklist-1