William Adams

IS-4473-001

11/20/2023

USA Healthcare BYOD Policy

Welcome to USA HealthCare's Bring Your Own Device (BYOD) policy we have constructed. This policy is designed and is set in place to establish guidelines and expectations all employees that are using personal owned IT devices that are on USA Healthcare's network. With this policy being set in place, it is very crucial that employees adhere to the BYOD policy so that we keep the organizations sensitive safe, the integrity of client's information secure, and maintain compliance with regulatory requirements. While our policy sets a standard for BYOD, we do understand and acknowledge that there are some unique situations where employees may go against the policy set in place. An exemption process is in place, allowing employees to request special considerations, they will be carefully considered to make sure they are granted for the right reasons. Employees that are non-compliant are putting the organization at risk of many security vulnerabilities, with that being said, Consequences for non-compliance may include meeting with management, suspension of BYOD privileges, or termination of employment, depending on the severity and frequency of violations. Thank you for complying and reading the BYOD policy, this will help the organization keep and maintain confidentiality, integrity, and availability of our information assets.

There are goals and aspirations that we want this policy to achieve, here are the goals that we want our BYOD to achieve.

- **Security assurance**: We want to ensure that the BYOD policy has no effect on the organizations security and the protection of the organizations information assets.
- **Cost and savings:** This can save USA Healthcare some money by not having to spend money on other IT devices.
- **Can improve employee satisfaction:** Improve employee morale by allowing the use of personally owned devices.
- **Compliance and acknowledge:** All employees sign and agree to comply and follow the BYOD policy.
- **Compliance with the laws and regulations:** The biggest goal for this policy is to make sure it falls within regulations and laws.
- **Training mandate:** Make sure that all employees are trained to follow the guidelines of the policy.

Our organization takes pride in knowing that our policy follows the compliance and laws of security.

- **HIPAA Security Requirements:** Align with the Health Insurance Portability and Accountability Act (HIPAA) security requirements to safeguard patient health information.
- **HITECH Act (Health Information Technology for Economic and Clinical Health):** This act focuses on the promotion and adoption of health information technology and addresses the privacy and security concerns associated with the electronic transmission of health information.
- **Electronic Communications Privacy Act (ECPA**): ECPA governs the interception of electronic communications and may have implications for monitoring employee communications on personal devices.

SCOPE Of Policy

With this new policy, this will be implemented to all employees in the organization, no matter what their role in the company is, anybody that is connected to the network must comply with these guidelines.

The specific appliances that the policy covers are not just laptops, but smartphones, tablets, and other IT devices that employees may use for work related task.

Employees that do choose to use their owned IT devices are only allowed to be using their devices for work activity. Based off of their specific role in the company is how to determine their permissions. Some position within company may be asked to do different task then another position in the organization.

Allowing personal devices does affect the 7 domains of IT Infrastructure in some way. Each of the seven domains does get affected in some sort of way with the allowance of BYOD.

- User Domain: Employees that access the network.
- Workstation Domain: Employees personal IT assets that are being used for work.
- LAN Domain: Interaction with the local area network.
- WAN Domain: Connection to the wide area network for remote access.
- Remote Access Domain: Employees accessing the network remotely.
- System/Application Domain: Interaction with applications and systems.
- Data Domain: Handling and accessing company data remotely.

Standards of Policy

The BYOD policy at USA Healthcare is made up of a bunch of technology standards aimed to ensure the security within the organization. To make sure the security of our data is secure, all personally owned devices must adhere to encryption standards, employing AES-256 for data at rest, and SSL/TLS protocols for encrypted data transmission. This policy will order all employees to use SSL VPN as an approved standard for establishing secure remote connections. It is also paramount that users use approved web browsers that the organization approves to be secure (Google chrome, Microsoft edge) and must updated to the latest versions. Standards for laptop hardware, like dual-core processors, 8GB RAM, and 256GB SSD, guarantee a safe and uniform teleworking environment. Configuration requirements include firewall setups to strengthen the security posture of personally owned devices, automatic upgrades, and password protection. This policy highlights the critical role that the organization's hardware, software, and configuration standards play in preserving the availability, integrity, and confidentiality of data throughout the seven IT infrastructure domains. It also conforms to those standards.

Procedures

Any user that is on their device should be using their device for work functions and data that is essential to do their job and ensuring their secure access. Users in the organization are prohibited from downloading unauthorized software that is not authorized by the organization. The BYOD policy will be spread a utilized all across the nation with other USA healthcare branches. Administrators in the organization duty is to make sure that employees acknowledge and understand the policy. With the addition of the new BYOD policy, there will be training for this new policy for all new employees upon hire. There will be training modules that will cover policy updates, expectations, and security best practices. Employees will be reminded by emails on security awareness, that will reinforce the importance of maintaining security awareness. When it comes to an employee that sees any suspicious activity on their personal device, it is there responsibility to report these incidents to management. We will implement a system where you can email a hotline to get the incident resolved as efficient and fast as possible to maintain the security threat. If a situation presents itself where a device is lost or stolen, the organization has the right to wipe any device that has company information to prevent unauthorized access to it. Users are also responsible for reporting any lost or stolen devices to management to prevent any potential security threats. The organization does employ 24/7/365 monitoring using intrusion detection systems that are set in place. This includes the monitoring of network traffic, device access, and potential security incidents to make sure the response of incidents is efficient as possible. Users must comply with these established standards that are set in place in the IT policy. The policy will be audited frequently to make sure the policy is up to date with the latest concerns.

7 Domains that are addressed in this section.

1. **User Permission and restrictions (User Domain):** Employees are responsible of adhering to user permissions that are brought up in the policy.
2. **Nationwide Policy implementation (LAN, WAN, Remote Access Domains):** Users in the organization will make sure of BYOD nationwide, ensuring the consistently of the policy worldwide.
3. **Standard Compliance (Workstation domains):** Administers across the organization will conduct frequent audits of the policy to make sure users are complying with the policy.

Guidelines

There may be some roadblocks or hurdles that a user may face in the policy, in the event of any technical issues, users are recommended to contact the IT support team for assistance. Users are required to give the IT support team a description of the issue at hand, and they will collaborate with the user to solve the issue. Email etiquette is also very important to make sure we have a professional environment with the way we email each other, this is mandatory, but this is advised of users. With how often accounts get breached, it Is advised for users to have strong passwords that can’t be easily guessed. It is recommended for users to have a password between 10 characters and a special character in it as well. Also, when checking emails or on the web, be cautious with what you are clicking on. If you see a suspicious link, do not bother, and click on it because it can be malicious.

Policy Exceptions

In the event that a user in the organization needs an exception from our BYOD policy, a request must be submitted through our system. We do understand that there may be some unique circumstances where a request in required, the user will fill out the request and it will be reviewed. These requests will typically be submitted through a dedicated email that is for these requests to be made. The IT security team, in collaboration with relevant stakeholders, will be responsible for evaluating each exception request.

Administrative Notations:
Author: William Adams
Department: IT security management

Considerations for this policy were focused on to algin with industry best practices and to comply with the states laws. Any changes to this policy were driven based off of the idea to have the most secure organization and for this policy to enforce that idea. We intend for this new policy to have no effect on our security as an organization even with the addition of employees' personal devices.

This policy will go under review at least 2 times a year to make sure all procedures are up to date and are working to the best of its ability.

The latest version of the BYOD Policy can be found on the USA HealthCare intranet. The hyperlink is [BYOD Policy - Hyperlink].
Developed By: USA healthcare IT team.
Reviewed By: William Adams
Approved By: William Adams (security director)
Department Represented: IT Security Management

Policy Definitions:

BYOD (Bring Your Own Device): A policy allowing employees to use their personally owned devices, such as smartphones, laptops, or tablets, for work-related activities and network access.

IT Assets: Physical or virtual components used in information technology, including devices, software, and data, which are subject to management and security measures.

Audit: defines account limits for a set of users of one or more resources. It comprises rules that define the limits of a policy and workflows to process violations after they occur.

Encryption: The process of converting information or data into a code, especially to prevent unauthorized access.

SSL VPN: A technology that establishes a secure and encrypted connection over the internet, allowing remote users to access the organization's network securely.

Version Control

Revision	Originator	Change Date	Change Description	Approver	Approval
1.0	**William Adams**	**10.21.2023**	**Device change**	**USA Healthcare Management**	**8.22.2023**

Policy Enforcement Clause: Violations our policy will be taken very seriously to ensure that integrity of our organization. Employees that fall under these violations will be subject to the following consequences.

First violation: The employee will be given a verbal or written warning, to clearly let them know what they violated under the company policy.

Second violation: Suspension of BYOD privileges, the second time you break the policy you will instantly lose your privileges.

Third violation: A 3rd break in the policy may result in possible termination of employment, you are putting our organizations security at risk and haven't changed behavior after the first two warnings.

Acknowledgement:

I ______ have read USA HealthCare's BYOD policy and have agreed to all terms and conditions. By signing below, I commit to the following guidelines, standards, and procedures that are set in place. I understand the consequences that will be in place if I fail to meet company standards.

Employee name _____

Employee Signature ____

Date _____

Refences

Chapple, M. (2023, May 22). *5 strategies for implementing a BYOD policy in healthcare*. Technology Solutions That Drive Healthcare. https://healthtechmagazine.net/article/2019/09/5-strategies-implementing-byod-policy-healthcare

ConductScience. (2022, May 19). *BYOD in Healthcare*. Conduct Science. https://conductscience.com/byod-in-healthcare/

Peremore, K. (2023, July 27). *Bring your own device (BYOD) policies in Healthcare*. Paubox. https://www.paubox.com/blog/bring-your-own-device-byod-policies-in-healthcare#:~:text=July%2027%2C%202023-,The%20Bring%20Your%20Own%20Device%20(BYOD)%20approach%20provides%20the%20freedom,health%20information%20protection%20remains%20uncompromised.

Snell, E. (2016, December 14). *BYOD security in the healthcare setting*. HealthITSecurity. https://healthitsecurity.com/features/what-is-healthcare-mobile-security-secure-messaging

Wani, T. A., Mendoza, A., & Gray, K. (2020, June 18). *Hospital bring-your-own-device security challenges and solutions: Systematic review of Gray Literature*. JMIR mHealth and uHealth. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7333072/