BYOD Policy – I330 Midterm Report

Evan Dartt

BYOD Policy

Required uses of Devices:

- Device should only be used for company-related work when working at a job location. Employees must use company-owned applications and software when working on-site. Use of external applications that do not pertain to the company are off-limits. Exceptions include general applications such as:
    - Email
    - Messaging / Calling
    - Calendar
    - Other apps may be approved by IT manager
- Browsing the internet for non-work-related reasons during daily operation hours is prohibited. If caught, the employee's device may be IP banned from accessing certain websites/applications.
- Doing the following on a personal device on-site is prohibited:

    On-site and Off-site:
    - Circulating company data
    - Illegal activity of any kind
    - Harassment
    - Storing proprietary information from other companies

    On-site only:

    - Non-company related business
    - Downloading files or clicking links from external sources

- If misuse of device is persistent, device management technology may be instated and activated.
- Unauthorized access and/or misuse of patient records is prohibited on personal devices. (User must have proper security clearance).
- Smartphones and tablets including iPhone/iPad, Android, and Windows are allowed. Device must be no older than 3 years from release date.
- Laptops including Windows, Mac, and Linux OS are allowed. Device must be no older than 4 years from release date.

- All devices must be approved by IT manager. Proper installation and configuration of company services must be installed before use of device is allowed for company work use.
- Any hardware, software, or network issues must be brought up to IT. Device may be reimbursed if effected by a breach in IT infrastructure.
- Any and all company work outside of work location must be done connected via company VPN.
- Consistent failure to comply with device usage policy may result in additional training, employee probation, no longer being able to use personal devices for work, and possibly termination.

Security and Privacy

- General password security compliance is expected for using personal devices at work location or off-site. This includes but is not limited to:
    - Strong passwords for company services on device (>= 12 alphanumeric characters and symbols)
    - Different passwords among personal and company accounts
    - Company passwords must be reset every 3 months
    - Accessing company data and software will require password and 2-factor-authentication to access.
    - Device must lock itself within 5 minutes of being idle and require a password or pin to log back in. All devices must be locked when away from device for any period.
    - 3 incorrect login attempts will lock you out of company systems. Please contact or bring device into IT to unlock.
- Our company has the right to access and monitor information on any device connected to the network for the safety of our company and its users, clients, and patients.
- System and network traffic will be monitored 24/7 by IT.
- Personal information and data on employee devices will not be accessed unless there is probable cause of suspicious activity.
- A device may be wiped of its company data if subject to potential company threats or digital compromise of device, the device is lost or stolen, or if employee is terminated by company.
- Suspicious activity, malfunction, or theft or loss of device must be reported to IT immediately.
- Backups of work-related data on devices are required.
- Employees will be unable to download unauthorized apps while connected to network.
- Employee location will be tracked while connected to VPN or company network.

- Device applications and OS must be up to date.
- Employees are prohibited from discussing company, user, and patient data with anyone outside the company.
- Any migration of data from personal device must be encrypted and sent via secure company network.
- Our company has the right to deny access to certain services without notification, take disciplinary action against lack of security compliance, and possible termination if security compliance is not followed. Security compliance training and routine security checkups will be issued to employees who fail to comply with basic security rules.

Company Goals and Objectives

Goal	**Objectives**
Improve employee skills and security	• Security compliance training • Proper use of devices when connected to company network
Maintain confidentiality of patient records	• Train employees to be aware of phishing attempts • Maintain effective access control of system and network
Increase efficiency of service	• Regularly update and patch software • Careful management of financial and billing information of users, clients, and patients

Justification of BYOD Policy

Since our company retrieves and stores medical records, personal information, and financial data, the security of our network and data infrastructure is very important to maintain. With that in mind, our "Bring Your Own Device" (BYOD) policy covers many use and security risks a business of our size may have as we strive to provide our users, patients, and clients with upmost confidentiality and privacy. Our company allows the use of personal devices for work whether it is at a job location or off-site. We feel that allowing our employees to feel comfortable using whatever they want is beneficial for our company. In the justification for the different trade-offs of our BYOD policy, we tried to maintain a balance of flexibility, convenience, user privacy and security. Our employees are more likely to do work outside of work hours and may be more efficient in handling work responsibilities with their own devices. However, it is slightly riskier to allow personal devices to interfere with work being done and security of company data, but our policy helps mitigate those risks.

The first section of our BYOD policy covers the usage requirements for using personal devices at work. When an employee is on our network at a job location, there are limits as to what they can access on their device when connected to our network. To make sure that our employees are working efficiently and effectively with minimal distraction, we prohibit the use of most external apps and web browsing. While these applications and use of the internet are not blocked at first, if an employee is found using what they shouldn't be besides basic apps like email or calendar, or using the internet for things like shopping or suspicious searches, we as a company have the right to block websites and apps that can be a distraction or security risk. We as a company want to be transparent with our employees as possible and make them feel comfortable working here, so that is why we do not block websites and apps from being used right away. However, our IT audit team can choose to IP ban or block apps or websites on employee's devices if they're being commonly used for non-work-related instances.

While using company software whether on-site or off-site, there are some restrictions on things our employees can and cannot do. The distribution of our company data is strictly prohibited, and any instances where it is found that an employee shares or stores the data of our company or other companies outside of our network will result in immediate termination. This also includes any unauthorized accessing of patient or client data on our network. This is a direct violation of HIPAA. If it is also found that employees take part in any illegal activity or harassment of employees or users with devices that contain company data, they may be subject to probation and will be put under careful monitorization, with the potential to be terminated and subject to prosecution based on severity of misuse. While on-site, use of device for outside work or business, and accessing external links or downloading files from external sources will not be tolerated. It is very important our employees are focused and knowledgeable of phishing, malware, ransomware, and other malicious attacks that could be catastrophic to our IT infrastructure and daily operations. We allow employees to text, call, check emails, etc., but they are not allowed to open files or click links while connected to our

network for any reason. Keeping a separation of work and home life is a value our company has, but if life outside of work starts interfering with work efficiency, device management may be instated onto employees' devices if IT feels their use of device on our network interferes with the integrity of our company.

Our BYOD policy also lists some basic hardware and software requirements the devices must meet in order to be used with work. We require phones and tablets to be fairly recent models so that they can meet performance standards and be updated to latest versions of OS and software. This is so that the devices connected to our network have a lower chance of being outdated and prone to vulnerabilities, slow performance, and potential data loss. Employees may also purchase devices for work use at a discount, so everyone has fair access to up-to-date technology and devices. In order to use a device for work, they must be sent to IT so that the proper company settings and configurations can be adjusted, and company applications and security can be installed. This also means that the device can be monitored by IT, however employee data protection is ensured. If a device has a hardware malfunction or connectivity issues, the employee should bring it in to be troubleshooted and fixed. If the problem is due to a breach in security that infects a device, the employee may be compensated to purchase a new one. However, if it's found the breach was due to poor security compliance of an employee, they will not be reimbursed. Finally, any work that is done outside of the work location must be done while connected via company VPN. Location of the device will be tracked for security reasons, but only when connected to the network.

The second portion of our BYOD policy covers the security and privacy requirements for personal devices being used for work purposes. Our company requires strong password standards in order to prevent data breaches, insider threats, and outside threats. While it may be tedious, it is necessary for the security of our data that employees follow the appropriate password guidelines. We require passwords of company credentials to be 12 or more letters, numbers, and symbols. We decided 12 to be the lowest amount of characters because the shorter passwords are, the easier it is to brute force them. It is also required that any passwords used for company software credentials are not the same for personal accounts such as social media or payment systems. Passwords must be reset once every 3 months for increased protection of data from brute force attacks. Our company also requires employees to use 2-factor-authentication to login to network or any accounts associated with the company to decrease the chance of an employee's password being compromised and used to leak or steal data from our databases. Also, to limit the threat of data being compromised, our security protocol suggests that more than 3 attempts of incorrect password will lock the device out from any authorization to company systems, and the employee must contact IT to have it unlocked. We do this so that the risk of an inside or outside threat with access to an employee's device cannot easily gain access to data.

Our users and patient's data are important to keep secure for their privacy, but that does not mean we want to sacrifice the privacy of our employees to do so. IT will monitor devices connected to the company network 24/7 and have the right to. However, there must be probable cause of suspicious activity or potentially data compromise for IT to access the personal information and data on an employee's phone. It is a very rare circumstance, and we assure our employees their privacy. In any case of malicious activity, loss or theft of device, or an employee is terminated, company data may be wiped from the phone for security reasons. In this situation, it's important for the employee and company to have backups incase data is deleted for any reason. In case of any malicious attack, its important to have a plan in place.

To wrap up the justification for the security requirements for our BYOD policy, we issued a rule where employees cannot download certain apps or programs while connected to the network. The risk of malware and ransomware attacks are at an all time high, and we do not want to risk some rogue software being loaded onto a device that can spread through our network. It is also important our employees keep the software and operating system on their devices up to date. We also want to make sure to keep patient data confidential and as secure as possible. In order to do that, employees are not allowed to share employee data outside of the company or network. Authorized employees who handle patient data on a personal device must also encrypt any information before migrating it somewhere. This must all be done on the secure network. Secure handling of data is extremely vital, and we don't tolerate any risk of leaking that data. Failure to follow appropriate handling of our client's data resulting in data leaks could result in termination. Other mis compliance of following basic security protocol will subject an employee to further security compliance training, and routine security checks.

Discussion and Connection to Course Material

We have covered many topics in class so far that relate to the benefits, risks, and concerns of the security and privacy of technology. Many of those topics contribute to the risk analysis and different aspects of a BYOD policy, as the policy needs to consider many different risks, concerns, and beneficial trade-offs for allowing employees to use their own device for work. These guidelines that must be followed need to be both legally and socially applicable.

The first connection of my BYOD policy and class material is that the BYOD policy must follow fair information practice principles and comply with legal guidelines. The FIPPs are not a legal framework but are general guidelines of how a company should handle and utilize their IT infrastructure, data, and privacy accordingly. An example from the reading of "Fair Information Practice Principles", which we read for week 3, class 2, states that there should be transparency

of information a company has on an individual. However, that information can only be shared with that individual. In my BYOD policy, I explicitly stated that the distribution or sharing of any data with unauthorized figures inside or outside of the company is prohibited. This topic of privacy of data relates to a core value of my BYOD policy in that any user, client, or patient who utilizes the company in any way is assured confidentiality of their information, and our company holds the integrity of making sure of it.

Every company needs to be ready for the inevitable circumstance that a threat to security emerges. This threat can be either an outside threat or inside threat. In my BYOD policy, I tried to handle the different circumstances an insider or outsider threat could happen in relation with the personal devices being used for work. The password policy guidelines in the policy are very strict and are meant to prevent both insider and outsider threats from being able to get in through an employee account. Specifically, insider threats who have malicious intent to leak company data may have a hard time doing so by framing another employee. Also, I stated in the policy that migrating data with a personal device must be done only on company network and encryption of data is necessary. The reading from week 4, class 1 titled ”Enemies within: Redefining the insider threat in organizational security policy” discusses the increased threat of electronic data exchange, and with that information in mind, I tried to maintain confidentiality of our company data as securely as possible so that privacy would not be expunged.

An important aspect of technology of a company is looking at the trade-off between usability and security for both employees and users. I remember an example from class where the CEO of Yahoo decided not to patch a security threat in account creation the IT team was aware of. Later on, a cyber-attack breached the data of nearly every user on its platform. The patch would have made it a little more inconvenient for users to create accounts. However, the trade-off for usability ultimately failed. Another example from an in-class activity described the situation where a hacker found that he could get the personal information from users through URLs, so he made a script that fetched the account information of thousands of users before telling the company of their vulnerability. Keeping this in mind for the employees of our company specifically, I wanted to have passwords and accounts used by employees whether on personal devices or not to be very secure and uphold security compliance. A reading from week 5, class 1 titled “Where Do Security Policies Come From?” helps extend the point of usability and security trade-off. It proved that many high-value and high-user-volume companies don’t require extensive password security. However, in order to keep data breaches from our own employees to a minimum, I wanted to ensure high security of employee access.

Cybercrime is at an all-time high. Things like spear-phishing, malware, and ransomware attacks are targeting businesses to take advantage of data and try to make money out of it. In my research of ransomware for the topical consultation, I found that the volume of cyber attacks has increased by 97% in the last 2 years alone. Hackers are spamming phishing attempts and searching for vulnerabilities in company systems. With this in mind, the BYOD policy specifically tries to mitigate the risk by disallowing the clicking or downloading of external files and links while connected to the company network. The employees must also go through web safety and security training to be aware of these malicious attempts. From research and knowledge from class information, I know that over 3/4th of businesses are targeted by cybercrimes every year.

The information from the videos, reading reactions, topical consultations, and in-class activities has really informed me on a wide variety of security and privacy topics and risks that are prevalent in today's IT world. A lot of companies don't have the proper security protocols or employees with professional security knowledge to back up or secure their IT infrastructure. It's very important in today's society to be on top of security and have the means to prevent and respond to malicious intent from all angles. The course material so far has given me a general understanding of the threats to security and privacy that I am eager to take with me into the cybersecurity world and may aid me in eventually creating a BYOD policy or security and privacy guideline for a company in the future.