**Risk Analysis**

Brantly R. McKendree

Southern New Hampshire University

IT 412-Cyberlaw and Ethics

Professor Grace

July 19, 2020

**Information Technology Structure**

The information technology structure is set up with a switch linking all the computers within the system together and it also has the Healthcare Data Server, a router, and an access point for wireless access. The access point is setup to allow guests and staff into the network to use the internet. This means that guests have potentially easy access to anything that connects to the switch. The default passwords and usernames make this a serious threat. A way to mitigate this is installing another access point with different passwords to log-in and limiting its connection to staff computers and other things such as the Healthcare Data Server within the network. The Healthcare Data Server houses company records, patient health records with personal identifiable data, patient billing, company financials, and forms. If a client logged into this server and accessed other client’s information this would be a serious data breach. The printer/copier is in the front office and is used by employees. This is a security issue because personal information may be found on printed documents and could be easily stolen and seen by employees who don’t have a need to know. The staff is using wireless for their laptops within this network.

A screenshot of a computer

Description automatically generated

**Cyberlaws and Ethics Regulations**

The cyberlaw that is predominate in this scenario is the HIPAA law or Health Insurance Portability and Accountability Act. This is the law that specifically relates to employees being able to carry over their health care, but most importantly holds medical employees accountable for healthcare information. This law is closely tied to the Hippocratic Oath, which states “Whatever I see of hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private.” This law and oath closely tie together because they mandate information stored in a healthcare technologic device to be protected as such. This ties to the scenario because the staff need to protect the information stored within the Healthcare Data Server. These intimate details could be extremely hurtful to the patient and the hospital if breached. Ethically the employees should uphold the Hippocratic Oath even when it comes to data stored within a computer. Another law that congress passed in February 2009 was the Health Information Technology for Economic and Clinical Health Act (HITECH ACT). This is a stimulus package that promotes the privacy and security within the American Recovery and Reinvestment Act (ARRA). The ARRA contains incentives to help with the change of health care information technologies.

**Ethic Violations**

First, there isn’t a firewall listed within this network and that is a huge issue as well. This is an issue according to the Payment Card Industry Data Security Standard or PCI DSS for short (Official PCI Security Standards Council Site, n.d). Without a firewall this is a professionally unethical behavior because it doesn’t protect the information and violates the HIPPA laws. Next, the printer/copier isn’t located in a secure location and any guest or employee could see information they aren’t supposed to. They also aren’t disposing of misprinted files appropriately to protect information and instead leaving them on the machine and reusing them. This is a professional unethical behavior because it isn’t protecting patient information and personal because it allows for employees to potentially act unethically and view documents they aren’t supposed to. Finally, the network isn’t protected from guests signing into the same network as employees and potentially breaching into secure information. Breaching information would be an unethical behavior on the personal level because it allows for a single party to hack information for personal gain. Open networks like this are a huge security threat as it allows for information to breached. The impact of these things would be devastating to the company as it would potentially lose many patients and it would also lose financial records and money to hackers. The loss of patient trust at ABC Healthcare would cause the startup company to fail and shutdown as it failed to protect its patient’s sensitive information.

**Cyberlaw Noncompliance**

ABC is a Healthcare startup that maintains customer documents and sensitive information. This risk assessment will provide outlook on some of the things out of compliance with cyberlaw and regulations in place. These are just guidelines as there is no specific entity that identifies the laws within information technology. However, HIPAA, ARRA and HITECH must be followed regarding healthcare. SANS institute provides templates for information security and cybersecurity training.

Violations that are notable within ABC Healthcare are substantial, but fixable. The network in which guests and employees sign into share an access point with a shared password. This can turn into a violation of HIPAA as guests can access files the staff can access which would lead to breaches in customer data. This would have an impact on ABC because the company would have to notify all customers of the data breaches and this would cost a large amount of money and company time. A solution to this is to add another access point to split the customer and staff networks into different internet access points. These impacts could shut down a startup company in a single instance if substantial enough a breach with a maximum cap of $1.5 million per year. Another violation regarding HIPAA would be the reuse of failed print jobs. These documents that are printed contain sensitive patient information and would cause a major data breach and data breach report. These reports are costly and require that each patient get notified of the breached information and with this a patient may lose confidence in the protection of their information within ABC Healthcare resulting in the loss of a patient.

Another violation that stems from the prior is the Gramm-Leach-Bliley Act of 1999. GLBA mandates standards for “when and how information is collected, how that information is stored, and what parties have access to it.” This has to do with ABC’s Healthcare Data Server. This server is on a network where all the staff can reach it and even guests on the access point could given that the passwords and users are all default because they were setup by multiple vendors. To correct this a simple change in passwords and users could resolve this issue as well as the access point separation. With given staff member only having access this would limit who can access this information and make it more compliant with GLBA. This type of data breach would also be costly and need to be reported to all patients of the healthcare business because it is a breach of sensitive patient information. The impact would be potential shutdown and cease of existence for ABC Healthcare depending on the severity of the breach and the cost to repair these issues.

**Acceptable use-of-technology policies**

There are many acceptable use policies in place that produce a baseline for how an organization uses its technology. A few of these are SANS Institute of Acceptable Use Policy, ISSA Acceptable Use Policy, Pennsylvania College of Technology IT Acceptable Use Policy, and AT&T Acceptable Use Policy. These policies are baselines that can be used within any organization to help prevent Cyberlaw noncompliance. Here are a few examples of what each are capable of.

SANS offers two pages of expandable policies that produce documents to help the organization establish their own acceptable use-of-technology policies. Each of the tabs offer PDF and word documents that can be used within the organization for training. ISSA or Information Systems Security Association International provides membership to sign up and speak with local security professionals and discuss their policies and uses of these policies. Of these policy rules many of them apply to ABC Healthcare.

Pennsylvania College of Technology IT acceptable use policy states several rules for acceptable use. They are as follows from their webpage <https://www.pct.edu/campus-life/student-policy/it-resources-acceptable-use-policy> (Student Rights & Responsibilities IT Resources Acceptable Use Policy, 2020).

1. Intentionally and without authorization, access, modify, damage, destroy, copy, disclose, print, take possession of, or disrupt in any way all or part of any computer, computer system, network, software, data file, program, database, or any other College IT resource. This includes:
   1. Gaining access by willfully exceeding the limits of authorization
   2. Attempting (even if unsuccessful) to gain unauthorized access through fraudulent means
   3. Gaining access by using another person’s name, password, access codes, or personal identification
   4. Attempting (even if unsuccessful) to gain unauthorized access by circumventing system security, uncovering security loopholes, or guessing passwords/access codes
   5. Attempting to disrupt any resource from being available to other users
2. Give or publish a password, identifying code, personal identification number or other confidential information about a computer, computer system, network or email account, database, or any other College IT resource.
3. Load any third-party software on computer systems in the computer labs, unless authorized by a member of the lab staff, a faculty member, or an Information Technology Services (ITS) representative.
4. Transfer copyrighted materials to or from any system, or via the College network, without the express consent of the owner of the copyrighted material. (See section entitled “File Sharing and Copyright Infringement.”)
5. Provide unauthorized external access to College-developed or commercially obtained IT resources.
6. Use any College IT resource for commercial, political, or illegal purposes; personal financial gain; or harassment of any kind.
7. Display obscene, lewd, or otherwise offensive images or text.
8. Intentionally or negligently use computing resources in such a manner as to cause network congestion and performance degradation.

These policies are extensive and cover every instance that an employee may miss use a computer to gain access or information not provided to them. This is a responsibility of all IT professionals that deal with information security. Many of these rules apply to ABC Healthcare as well.

**ABC Healthcare Acceptable Use Policy Adaptations**

SANS and Pennsylvania College of Technology provide detail rules that would meet the organizational needs of ABC Healthcare. SANS rules are as follows. The clean desk policy, which requires employees to safeguard patient data to comply with HIPAA. This policy would require the employees to secure any confidential information at the end of the day. The workstations are to be locked at the end of the day and between each use. Any time an employee leaves their workstation they must lock the workspace. Any sensitive information must be locked up when the employee leaves it unattended. Keys for the locked storage should not be left unattended for any reasons. This would be simple to implement as the employees would receive training and then be expected to uphold these standards or risk losing their jobs or be written up. This is a serious matter that requires serious response.

SANS lays out a password policy that should be upheld within ABC Healthcare. The passwords should be conformed to a specific requirement of capital letters, numbers, and special characters. Users should use a unique password for work related passwords. Passwords should be changed every year. This could be implemented by requiring a password change once the requirements are in place within the systems. Some coding and setup may be required but this will allow for safe passwords to be created and protect the patient’s information as well as the employees.

**References**

Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards. (n.d.). Retrieved July 21, 2020, from https://www.pcisecuritystandards.org/

Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act), Pub. L. No. 111-5, 123 Stat. 226, codified at U.S. Code Vol. 42, sec 300jj et seq., and sec. 17901 et seq. (2012).

Student Rights & Responsibilities IT Resources Acceptable Use Policy. (n.d.). Retrieved August 03, 2020, from https://www.pct.edu/campus-life/student-policy/it-resources-acceptable-use-policy

Security Policy Templates. (n.d.). Retrieved August 03, 2020, from https://www.sans.org/information-security-policy/?category=general