**Risk Analysis and Mitigation: ABC Healthcare**

**Michael Johnson**

**IT-412**

**Southern New Hampshire University**

**Introduction**

The purpose of this report is to provide an analysis of ABC Healthcare in regard to its current IT structure and regulations, including any ethics violations that may be occurring. The report will detail any violations of cyberlaw, ethics, and any other relatable violations so that ABC Healthcare can do what is needed to remedy the issues and comply with all cyberlaw and ethics regulations.

**Information Technology Structure**

ABC Healthcare is a small company that is just starting out. As such, the company only employs around 50 people currently. Due to this small size, ABC Healthcare has setup the workspace that is quite small and has little to no barriers between departments or files that should be kept secured. The employees work in a layout hat consists of small cubicles that are all on the same floor and have no other doors or physical barriers between them. This results in a workspace that provides little security for the staff and the clients information. Employees could easily fall victim of eavesdropping, shoulder surfing, and having their files stolen. With all of the files being kept on the same floor in one area, they could easily be read by anyone in the company, resulting in personal information being circulated where access should not be allowed. This is a huge issue as even larger companies with many security checkpoints in place still have their information stolen. According to Experian (2010), A staggering 80% of organization that are in the healthcare field have had at least one instance of health information theft. The current IT structure make ABC Healthcare much more susceptible to theft of PII and PHI.

**Cyberlaw and Ethics Regulations**

ABD Healthcare is a new and growing company. As such, there are many opportunities for the organization to improve their security to ensure they comply with all regulations to protect client’s information from both outside intrusion and from within. The most notable regulation for ABC Healthcare to ensure they are in compliance with is the Health Insurance Portability and Accountability Act (HIPAA). HIPAA helps to protect a client’s PII and PHI by ensuring that the information remains private. This is done by providing standards that must be followed by any health plans, health care clearinghouses, and health care providers to protect PII and PHI (HHS Office of the Secretary, 2017). This means that any use of client information must be approved by the client. This even includes sending that information to another healthcare office or doctor. Clients must be given the option to refuse the use of their information, limit the use of the information, or refuse to let the information be released at all.

**Ethics Violations**

**Personal**

There are numerous personal ethics violations currently identifiable within the organization. One such violation is the allowance of regular clients to utilize the organizations Wi-Fi. This should never be allowed as it creates an entry point for attackers to infiltrate the organizations network and obtain health records and other records that contain PII and PHI. ABC Healthcare should utilize a second wireless access point that is only for guests and clients. This will separate the traffic of the organization from the traffic of the guests to help ensure there cannot be access to confidential information. This goes hand in hand with the next violation, the use of personal electronics in the workplace and access to personal accounts on the network. Allowing employees to use their personal laptops, tablets, or other devices on the organizations network, either for work or personal endeavors, is a large violation that creates many opportunities for theft. Personal laptops could easily be stolen, attackers can access the organizations network through the less secure personal device due to lack of security features or social engineering and put clients PII at risk. I have witnessed such an incident before when the district manager of a company I had worked for left his laptop sitting on the sales for of a sales floor. The laptop was taken by someone and they could not be identified. The laptop had been connected to the stores Wi-Fi and was being used to access company email and other resources. For reasons such as this, there should be policies in place that forbid the use of personal electronics at work unless they are used only on the guest network and never used for work reasons.

**Professional**

It is important to correct violations now while the company is new and can easily correct them. The first and foremost correction needed is that of a company privacy and security policy. This policy should note, foremost, that any use of company property, including the network and workstations, as well as the building itself will be monitored via cameras and other monitoring technology to ensure compliance with workplace policy. The policy should also indicate the proper disposal guidelines for anything containing PII or PHI, which includes excess copies from the copy machine. This could also be a part of the acceptable use policy, which ABC Healthcare does not currently have in place. An acceptable use policy is one that every company implements to help indicate correct use of company property and the steps the company will and can take to ensure the policy is being followed. After that, another thing that should be addressed is the workspace layout. There is next to no privacy in the current operating arrangement. Departments can easily overhear one another, and the files are stored within reach of any person. Each person should have access only to what is needed to do their job and these jobs should be separated to ensure privacy. The files should be moved and secured in separate area to ensure they can be thoroughly monitored and allow access to only those who need it. The organizations hardware setup should also be adjusted and include the use of firewalls to help keep attackers out. The password and information need to be changed immediately to something other than the default information for programs to ensure the protection of PII and PHI. There are lists available that indicate the default information for most hardware and software that is easily accessible to attackers. These should be implemented immediately to help strengthen ABC’s security and the data they store. Failing to protect consumer data and continuing to see these violations could have a huge negative impact on the company including potential closure should they fall victim to a data being stolen.

**Cyberlaw Noncompliance**

There are several laws in which ABC Healthcare is noncompliant with. This could lead the company down a very dangerous path resulting in heavy fines, litigation, loss of consumer trust, and even the closure of the organization due to the backlash from events that could occur due to their noncompliance with these laws. Currently, the organization is noncompliant with the following laws:

* **Data encryption laws** – Not all states have a specific set of laws that dictate the necessary encryption an entity must use for their data to be secured, however, many states have come up with specific standards that are detailed within the law. One such state is the state of California. California requires that data be encrypted in such a way that it is “rendered unusable, unreadable, or indecipherable to an unauthorized person.” (California Legislative Information, n.d.).
* **Disposal of data** – Most every state has some sort of regulation set around the proper disposal of data containing PII. It is extremely important to ensure that all data is disposed of in a way that makes it unusable by those who are not authorized to view it. According to the New York State Senate (2020), this means shredding, destroying, modifying, or otherwise ensuring that all PII is unreadable by an unauthorized person.
* **Breach Notification Laws** – Currently, ABC Healthcare does not encrypt their consumers information that is held with the organization. This, coupled with the insecure location of most of the data in the organization, can result in some very harsh consequences. Since the organization deals in healthcare, they need to take extra precautions as well. The HIPPA Breach Notification Rule states that HIPPA entities must give notification if a breach occurs where there was unsecured health information (HHS Office of the Secretary, 2013). A key word here being unsecured. By using encryption, in most cases the organization can be covered under safe harbor. If not, the organization needs to ensure it complies with all state policies, not just the state it resides in, for notifying consumers about the breach.

These laws are there not only to protect the consumer, but the organization as well. Failure to comply can impact the organization severely, even causing closure of the organization completely. This can be due to the loss of consumer trust after unauthorized access to data has occurred. This can be magnified when the organization fails to comply with the notification period set forth in the breach notification laws. Alongside the loss of trust, noncompliance with the laws and regulations mentioned can bring serious fines, many of which increase the longer the organization fails to send notification to consumers, and large lawsuits. Many times, noncompliance spells the end for an organization when it faces a security threat.

**Acceptable Use Policy**

One critical component of security that is missing at ABC Healthcare is a AUP (Acceptable Use Policy). This policy is extremely important and should be adopted by all organizations to help keep data secure. The AUP helps tighten security by determining appropriate uses for the organization’s hardware, software, and other components including how to safely operate remotely. The AUP lays ground rules for key aspects of security such as password requirements, email expectations, and the use of VPN’s or other secure avenues of transmission when working outside of the organization. This helps keep data safe from internal threats, some of which happen unintentionally when there are no set expectations on the use of organizational property or data.

There are many AUP’s that can be looked at to help gather insight on creating an AUP for ABC Healthcare. A few of these include the SANS Institute Acceptable Use Policy, the Pennsylvania College of Technology IT Acceptable Use Policy, and the AT&T Acceptable Use Policy. Each of these policies can be learned from in order to create an AUP for ABC Healthcare. However, there are some differences in each of these policies, which include:

* **SANS Institute** - The policy created by SANS Institute provides not only information on acceptable use, but also what is determined as unacceptable use by the company and also includes a section that pertains to blogging and social media activity (SANS, 2014).
* **Pennsylvania College of Technology** – The AUP created by the Pennsylvania College of Technology provides not only information on the use of company property itself but also a section on the use of personal technology that utilizes the college’s network, including what to do if the computer is hacked while on the network. It also includes specific state laws that pertain to the college in conjunction with acceptable use (PCoT, 2013).
* **AT&T** – The AT&T AUP contains a section that is interconnected with the services that AT&T provides. This includes sections on inappropriate interactions with minors, child pornography, and what will happen in those situations (AT&T, 2008).

**Adapting AUP’s**

There are many different components for the various AUP’s researched that could be adapted to fit the needs of ABC Healthcare’s Acceptable Use Policy. One important component should be the appropriate use of email and other communication avenues to ensure security. This can include acceptable attachments to open or send and to never open or forward chain emails or other emails that seem suspicious in nature. The appropriate use of personal technology, such as cell phones, laptops, or tablets on the organizations network should be cited in the policy as well to ensure that the network remains safe and that employees are not using their personal devices to get around other acceptable work behaviors, such as viewing at questionable content. Employee’s should also never download software without the prior approval of the IT department and should never download software that is for personal use. This can cause unwanted and malicious software to be downloaded as well. Finally, the policy should, at its core, explain in detail the consequences that will be incurred from violating the AUP. To ensure that ABC continues to stay compliant with all applicable laws and regulations, audits should be conducted at specific intervals within the company. IT should closely monitor access to all company data to ensure there is no unauthorized access into that data. An IDS (Intrusion Detection System) should also be implemented to help detect such unauthorized access and help record any unusual activity.

**Code of Ethics**

While there are many laws that govern an organization, personal behavior within an organization is managed differently. Laws typically depict how an organization should act and behave on an organizational level, however, the employees that work within the organization are just as important when it comes to acting responsibly and ethically. A good example of this are superiors who play favorites within a company based on personal factors. This could be anything from sharing the same interests in sports to the persons gender (which then borders on discrimination). Creating a code of ethics for ABC will help provide clear and concise direction on how employees, including upper management, staff, and even vendors when visiting should conduct themselves when at work. This could even extend beyond that, as many do now days, to include organizational outings or any other scenario where employee behavior could cause negative views to the organization.

Being born from the organization itself allows the organization to tailor the code of ethics to best fit their goals and future. This allows for a great deal of personalization, the result of which can be very differing expectations from one organization to the next. While many organizations share some basic ethical expectations, most every code of ethics will have a little something that is unique to that organization’s goals. For example, a section on conflict of interest, where one’s personal interests get in the way of the companies’ interests, can be found in the code of ethics for both AT&T and Microsoft (AT&T n.d., Microsoft n.d.). This is an important aspect that should be included in any code of ethics. There are typically some differences in each code of ethics that can pertain to the organization itself. This can be seen in Microsoft’s code of ethics, where a section on ensuring they design their products and services to ensure that they are accessible to everyone.

**Code of Ethics Adaptation**

ABC’s code of ethics should be just like any other organizations. It should include sections on critical components that are seen in the code of ethics in most every business. It should, however, include sections that are unique to ABC and the field the organization represents. Some of the biggest pieces for the code of ethics should include:

* The organizations employee’s and management should follow all applicable state and federal laws. This is especially important for ABC as they are a healthcare entity and are affected by HIPAA.
* Employee’s and management should always operate in a manner that is ethical and fair. This includes having good judgement and applying policies fairly among employees.
* Employees and management should avoid all conflicts of interest. Such conflicts can put a person in a tough spot where they can jeopardize their job or the company.
* Employees and management should be prompted to report any wrongdoing that is seen in the organization or from any of its vendors. Employees should know that they are safe doing so and cannot be retaliated against for bringing issues forward.

While this list only provides insight into a few of the items that should be included into the organizations code of ethics, it provides a good starting point of some of the critical components. The code of ethics is something that should be easy to read and understand and should be given promptly upon the hiring of a new employee. The organization could also benefit from having an annual review of the code of ethics.

**References**

AT&T. (2008, October 15). Acceptable Use Policy. Retrieved October 02, 2020, from <https://web.archive.org/web/20160617030541/https:/www.att.com/legal/terms.aup.html>

AT&T. (n.d.). Code of Ethics. Retrieved October 16, 2020, from <https://investors.att.com/~/media/Files/A/ATT-IR/governance-documents/att-code-of-ethics-2012.pdf>

California Legislative Information. (n.d.). Code Section. Retrieved October 01, 2020, from <https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV>

Experian. (2010, March). *About Medical Identity Theft and Healthcare Data Breaches –An Overview*. Retrieved from <https://www.experian.com/assets/data-breach/white-papers/about-med-id-theft-healthcare-data-breaches.pdf>

Microsoft. (n.d.). Standard of Business Conduct. Retrieved October 16, 2020, from <https://www.microsoft.com/en-us/legal/compliance/sbc/default.aspx>

New York State Senate. (2020, July 04). Disposal of records containing personal identifying information. Retrieved October 01, 2020, from <https://www.nysenate.gov/legislation/laws/GBS/399-H>

Pennsylvania College of Technology. (2013, February). Student Rights & Responsibilities IT Resources Acceptable Use Policy. Retrieved October 02, 2020, from <https://www.pct.edu/campus-life/student-policy/it-resources-acceptable-use-policy>

SANS Institute. (2014, June). Acceptable Use Policy. Retrieved October 02, 2020, from <https://www.sans.org/information-security-policy/?category=general>

Secretary, H. (2013, July 26). Breach Notification Rule. Retrieved October 01, 2020, from <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

Secretary, H. (2017, June 16). HIPAA for Professionals. Retrieved September 16, 2020, from <https://www.hhs.gov/hipaa/for-professionals/index.html>