# ABC Healthcare Infractions

**SNHU – IT 412**

**By: Scott Allison**

## Information Technology Structure

ABC Healthcare maintains modest organization given its relatively small size. With only 50 employees it's not a surprise that the overall structure and procedures for conduct are how they are. Inexperience isn't a liability in some cases and the weight of responsibility can't all fall to the new networking administrator. Their supervisor the chief information officer should be verifying each step for quality.

The overall structure of the IT systems is satisfactory, at least with regard to physical topology. Computers are linked into a switch that allows them to quickly communicate with one another. However there is an access point is also connected to the switch allowing for usage of wifi for guests, clients, and staff. Then the switch is connected to the router. This is unacceptable.

Additionally, while not extrapolated on in this section there are numerous infractions regarding personal devices in the workplace and their usage on company networks. As well as confidential documents being left unattended in public spaces. Further more there is no segregated network for guests. Everyone uses the same connection which is hazardous.

## Cyberlaws and Ethics Regulations

The most prominent cyber laws and ethics that the company seem to be following are:

- Honesty regarding capability and responsibility about work competence.
- Being inclusive and encouraging coworker dialogue.

However the multitude of laws and ethics being transgressed is much larger.

The Health insurance Portability and Accountability act of 1996 (title II) dictates that efforts must be taken to ensure privacy and security of users information. By having minimal security present this is an infraction.(dhcs.ca.gov, last modified 6/13/19, https://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx)

The Health Information Technology for Economic and Clinical Health Act, or HITECH was passed in 2009 and serves to compliment HIPAA by adding regulations to the minimum security and privacy when handling health care records digitally. One such amendment was the striking the protection from penalties those handling the data had if those they covered didn't reasonably know of any mishandling of their information. Under this amendment each of ABChealthcare's clients are entitled to compensation based on a fine determined with HITECH. Such a fine could be omitted if the errors were fixed within 30 days and not due to willful neglect on ABChealthcare's part. Which, sadly, is not the case here.

Ethical infractions include the inability to design and implement systems that are robust and usably secure. The desire to uphold privacy. Professionalism with regard to confidential data and procedures.

## Ethics Noncompliance

To further elaborate. *Personal* ethical infractions are actions on a personal level that is outside the moral normal or right regarding themselves or their profession. Errs in this category are few, such as eavesdropping on coworkers over potentially confidential matters, intentional or not. Bringing personal machines to work and connecting them to the network. Using work time and network for personal matters such as browsing the internet or checking personal email. These are all not only security risks but huge wastes of company time.

The impact of personal infractions such as these are mostly minimal in the grand scheme. As the average employee has no use of random customer data. The only negative impact to a persons self wasting company time could have is a lack of time to accomplish their real work and potentially being fired.

*Professional* ethical transgressions are many as well. Monitoring employees without consent or notification while not illegal is highly unethical. It's further inappropriate if customer personal data is being captured as well. Further more the printer being at the front desk where anyone including guests can see is unethical and against The Gramm-Leach-Bliley Act. (Mrllp.com, 05/17/2016, https://www.mrllp.com/blog-privacy-law-for-insurance-producers) Another ethical problem is the usage of basic passwords for all machines. Guests being able to use the same connection and network as the staff is a massive security risk as secure data is easily accessible through local networks.

The negative impact of these ethical dilemmas is damaging. The least offensive is the unspoken monitoring of employees. The impact from this would likely result in a small morale drop. The security risk present with printer location could result in guests obtaining information that is not theirs and breaching trust with the client-base after this was acknowledged publicly. Guests using the same network as the staff and the staff being able to connect their personal devices to the work network could result in a data breach of all client information. Thus this is the most damaging infraction there could be to a business that needs its clients to trust it.

## Cyberlaw Noncompliance

HIPAA and HITECH were violated. The blatant and poor location of sensitive documents, open office room where those who don't need to know can overhear with ease, and visual recording devices in sight of sensitive information. Further more outlined above the Gramm-Leach-Bliley Act was in violation due to unsecure information both at the front where the printer is, and by networking security having default passwords and allowing personal and guest computers to share the professional work network.

Breaching any law is very damaging to a company financially and facially. Without trust clients will think twice about enrolling with ABChealthcare and look else-where. They will have to lay off workers due to legal fees and fines accrued from data breaches.

## Acceptable Use-of-Technology Policies

### SANS Institute

Based on the SANS institute computing devices must possess a password protected screensaver with an activation time at =<10 minutes of idleness. They must additionally be strong passwords matching a policy. Such as upper and lower cases, numbers, and special characters. They also state the minimum access policy will be used for all users.

Their ethics statement states employees will respect the privacy of their colleagues and clients, nor will they harm the property, reputation, or their colleagues by false of malicious action. A final highlight for their policy is state pushing their opinion as fact.

However there are detrimental policies at play in this document. One bullet point notes that employees will document their setup procedures and/or any modifications made to equipment. While noble in ideal, this costs hours of company time each time the employee uses a piece of machinery(digital or physical). There is another ethics statement that decrees the agreeie will not pursue private interests at the expense of colleagues, end users, or employer. Again, while noble in concept. If one reads between the lines “private interests” could be anything personal such as taking time off, refusing to offer exclusive rights to new ideas, or even looking for other work. Vague statements like these allow businesses to overreach their control.

### Valley Medical

Valley Medical's acceptable use policy indicates that all employees should report weak-points in computer security or any incidents of misuse or other violations. They also state that users should keep personal browsing or usage of the internet minimal or on personaal time. Employees must not install, run, or use unknown, unsupported, or unapproved softwares.

This includes wallpapers, screensavers, other typically harmless applications. This is a smart policy to have, despite its negative impact on morale. Malicious code piggybacks in the least suspecting ways and this is no different. Employee VMC accounts must not share their information with any other person, including other employees. The old standard “no soliciting” is also present.

A few poor policies include: “Electronic communication facilities (such as Email or news and Internet Browsing) are in no way to be used in a manner inconsistent with this policy or the mission or values of VMC or for personal, business or entertainment during scheduled work time. Fraudulent, harassing or obscene messages and/or materials shall not be sent to or from, viewed or stored on VMC systems.”(valleymed.org, https://www.valleymed.org/vt/valley-medical-center-computing-resources-acceptable-use-policy/) Two aspects of this statement are acceptable, however forbidding using their working accounts work email from being used for work during working time is strange.

The demand of that employees must not share VMC account information with anyone is acceptable, yet further down they demand passwords be given to supervisors upon request. This is not only unprofessional but a gross breach of overreach and a massive security risk.

The lack of password protocols is disturbing, as is the shallow depth of their privacy statements.

## ABChealthcare

ABChealthcare can learn from these two businesses. Employees reporting weak-points in security is a valuable tool to not only better the company but also give the employees a vested interest in the success of the business and a sense of value.  Restricting personal tasks during working hours is another policy that could be lifted from Valley medical.

The secure password protocols that the Sans Institute calls for is a valuable policy to lift. Their usage of privacy statements and restriction of information is a useful tool for a healthcare organization.

While it's important to lift and replicate, its important to dissuade and avoid as well. Ignoring the negative policies detailed above will lead to a more successful business. By not incorporating their mistakes ABChealthcare stands to propel itself further in the industry as a trusted insurer.

## A New Policy

Detailed below is an adapted policy statement, in addition to what already exists.

- Employees at ABC healthcare must not use their position to exploitative ends over other employees or clients.
- Employees will refrain from damaging company property.
- Employees will not download or install unsupported, unapproved, or unknown softwares. Including but not limited to: wallpapers, pictures, songs, or other media.
- Employees will uphold the integrity of ABChealthcare by not using personal devices on company the company network, not will they give out information about the company network to guests.
- Employees will limit personal matters to personal, non-working time. Such as breaks, lunch, or other non-working hours.
- Employees will uphold IT industry standards by possessing passwords a minimum of 10 characters in length, using suitable protective assortments of characters.
- Employees will uphold privacy standards, handling sensitive information carefully and attentively.

## Codes of Ethics Research

SANS outlines an IT ethical code for seeking permission before seeking vulnerabilities in network and computer security. They also state to encourage sharing of IT industry best practices. Harvard notes several IT ethics such as not using private data the employee has access to for nefarious purposes, not exploring their personal data out of boredom, and subjection to annual training regarding ethics policies.

These policies are a useful tool to ensure that an employee understands the severity and importance of the access and trust they've been granted. As well as yearly reminders of that fact along with an official briefing of any changes that had been made in recent time. Adapting these policies would similar to the prior section. Where-in a briefing pamphlet would be constructed and delivered to each employee, with either a signature of acquisition or a test regarding knowledge of the material. Once signed binds the employee to that they understood whats expected and that any breach will be subject to action.

- dhcs.ca.gov, last modified 6/13/19, https://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx
- https://www.fcc.gov/general/cybersecurity-small-business
- Mrllp.com, 05/17/2016, https://www.mrllp.com/blog-privacy-law-for-insurance-producers
- https://www.valleymed.org/vt/valley-medical-center-computing-resources-acceptable-use-policy/
- https://www.sans.org/security-resources/ethics
- https://huit.harvard.edu/it-professional-code-conduct-protect-electronic-information
- HHS.gov, last amended june 16th 2017, https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html