Michael Kohronas
Case Study: Company 1 - ISeeU Eyecare

1. **What are all of the specific compliance(s) your company needs to meet?**

ISeeU eyecare must abide by HIPAA and PCI DSS compliances.

   a. **Discuss why your company needs to meet the specific compliances you have identified.**

They must follow HIPAA because they have patient information such as patient records, insurance information, patient qualifications, and images captured during eye exams. They must abide by PCI DSS since they accept credit card payments at checkout. They also log products that are purchased, returned, exchanged, or warranty cases.

   b. **List the compliance organizations you would have to work with for the compliances your company would have to meet.**

Any partnering companies would also have to abide by HIPAA and PCI DSS standards. Depending on the data we are sharing with them. If we are sharing patients' medical documents with CVS or pharmacies we would need to know they are at least meeting HIPAA requirements. If they are meeting PCI DSS that is great but it is more important that we know the data we are sharing with them is safe. Now if we share our logs on products purchased, returned, exchanged, or warrantied it would be important to know that they are meeting PCI DSS standards as well.

2. **Identify the credit card issue(s) that will prevent your company from complying with PCI DSS.**

The largest standing issue that will prevent our company from complying with PCI DSS is the non-compliant credit card systems. We will need to make a plan to fix these systems.

   a. **If there are questionable credit card items, please discuss your thoughts and concerns related to the item in question.**

The logs that they are keeping are valid. They are keeping purchase logs to know when customers bought these products for return, exchange, or warranty purposes. Keeping data on all these helps keep track of the items they sell and what they need to stock more or less of.

3. **Identify three technology issues/gaps you would fix immediately for your company.**

The three technology issues I would fix immediately are their non-compliant credit card machines, ensuring we have met HIPAA Compliance, and ensuring they have a reliable IAM.

a. Propose how you would fix each of the three items.

- How to fix:
  - PCI DSS Compliance & Non-Compliant Credit Card Machines
    - Determine what level of PCI level we are
    - Complete a self-assessment questionnaire (SAQ)
    - Schedule quarterly vulnerability scans by a PCI-approved scanning vendor (ASV)
    - Research-compliant credit card devices
    - Research and ensure all devices, professionals, and manufacturers, are PCI certified
    - Assess finances, project plan, and device security posture.
    - Implementation
  - Update their Active Directory/IAM for Compliance
    - Install Auditing, Logging, Monitoring & Compliance some tools from Splunk, QuestAD, or ManageEngine.
    - Implement an IAM with MFA & SSO so only people who need to access certain information can and easily.
    - Hire someone to manage IAM & Active Directory
    - Implement RBAC to assign people to roles easily.
    - Ensure each user has the role & any additional permissions needed.
    - Monitor the active directory and IAM environment
  - HIPAA Compliance
    - Provide info to patients about their privacy rights
    - Adopt clear privacy procedures
    - Train employees on privacy procedures
    - Hire someone to oversee that privacy procedures are being adopted and followed.

b. What are some of the issues you could face for each non-compliance?

For PCI DSS the responsibilities fall on a merchant processor. If you are not in compliance you could have your merchant account frozen or disabled. Usually, they make you get audited by a third-party QSA to ensure compliance.
For noncompliance with HIPAA, They will issue a fine depending on the severity of the violation. Overall, not complying will cause a lot of financial and customer trust issues for our company.

4. Identify four items you would have ready for a compliance auditor?

The four items I would have prepared for a compliance auditor are documentation of our policy and procedures, Audit trails and logs, Evidence and examples of compliance, and a vendor report of who we are working with.

5. Discuss your thoughts, potential issues, and fixes with potential conflicts between each compliance your company needs to meet?

My company needs to meet compliance with HIPAA and PCI DSS is reasonable and obtainable. The main issues right now are the credit card systems being out of compliance. In addition to

need to ensure our IAM is up to standards to ensure no one is accessing patient records that aren't authorized.

6. **List three reasons/items why it would be a good idea for your company to implement the NIST 800-53 framework in part or in whole.**

I believe we should implement the NIST 800-53 framework. We should be implementing better access control. We also need a plan for incident response. In case something were to happen how would we react? In addition to Information protection processes and procedures.

   a. **Compare some of the issues your company has against the NIST framework and discuss possible solutions based on the NIST framework.**

- Issues based on the NIST Framework
  - Lack of Incident IAM
  - Unprotected patient records
  - Lack of detection
  - Lack of response plan
  - Lack of Recovery
- Solutions
  - Implement a budget-friendly IAM solution
  - Implement IAM to lock down data for only those who need to see it.
  - Implement active directory monitoring tools
  - Create an incident response plan
  - Periodically create backups of the environment.

These are important for us to implement due to us storing sensitive customer information such as patient records and processing credit card information.