**Executive Summary**

This project paper outlines our research of ZirMed’s policies and procedures regarding information security. To begin our research, we interviewed one of the four information security professionals within ZirMed. We prepared with questions and conducted an interview using the questions to give it structure. Our intent was to gain a unique perspective and a detailed insight into the working of the company’s information security. Our research paper is indicative of our understanding of their information security; limited only by our minimal access to ZirMed information security professionals and software.

In addition to the interview, the information security professional also provided us access to private, internal company documentation containing security policies that we used to gain even further information about their security.

Important points of topic regarding ZirMed’s information security system is their implementation of security controls in response to complying with PCI DSS and HIPAA regulations. Our research paper covers both regulatory organizations, and the information comes from both the interview with the information security professional and ZirMed’s security policy documentation. The importance of HIPAA and PCI DSS compliance, as we concluded, drives many of the information security controls that ZirMed enforces and maintains.

**1.0 Company Overview**

ZirMed is a leading producer of revenue cycle management software for the healthcare industry, and services providers varying from solo doctor practices to enterprise hospital networks. ZirMed’s customer base includes around 8,000 healthcare organizations and about 300,000 providers [(Staff)](https://paperpile.com/c/ovBLTY/CeLV). ZirMed was started in 1999 in Louisville, Kentucky where their headquarters remains today. The company also maintains an office in Chicago, Illinois and just recently sold offices in Texas and in California. ZirMed still retains its private company status in large part thanks to their current high-revenue operations and a financial backing from Sequoia Capital.

The company prides itself on its entirely cloud-based payment solutions. ZirMed is able to supply award-winning management tools for all levels of healthcare. Their high-quality systems improve clients’ revenue cycles while remaining fast and convenient. They continue to work on developing applications that can fill voids, or innovate upon existing and non-existent methods of workflow practices in the healthcare payment industry. This includes the rising field of data analytics whereby ZirMed hopes to provide services to healthcare providers the opportunity to gain valuable insight to the large amount data they possess. The enlargement and increase in quality of the suite of applications that ZirMed already offers its customers are continually in process, and so is the protection of it through information security processes.

With a large and growing client-base information security is a high priority. Any health related-data has potential to violate HIPAA policy, while payment information the potential for theft. Therefore risk management and data confidentiality are critical to ZirMed’s success. Without being HIPAA and PCI DSS compliant, ZirMed’s security practices may not be as stringent as they are today because many of the information security control implementations are required by HIPAA and PCI DSS.

To fail compliance with either HIPAA or PCI DSS would damage ZirMed’s reputation and, as far as HIPAA is concerned, could render a federal criminal investigation. The severity of non-compliance is too great for ZirMed which explains why their information security standards are highly detailed, requires training for every employee and vendor, and contains highly thorough notes of planning, implementing procedures, and maintenance of information security controls.

**2.0 Information Security Management Process**

ZirMed policy recognizes a five-step process for their ongoing risk management. This cyclical procedure allows for evaluation and improvements at any time; it includes the following principles:

Principle 1: Assess risk and determine needs

Principle 2: Establish a clear management approach

Principle 3: Implement appropriate policies and related controls

Principle 4: Promote awareness

Principle 5: Monitor and evaluate policy effectiveness

Each of these principles in conjunction is what guides the business in their upkeep of their information security. There’s a lot that goes into each of these steps that must be further broken down in detail. It’s best practice that this information is then documented and made accessible for employees to implement and follow. ZirMed has done such, and compiled their policies and the tools to maintain them in a single document that is maintenanced and kept by their security team and CTO.

**3.0 Location**

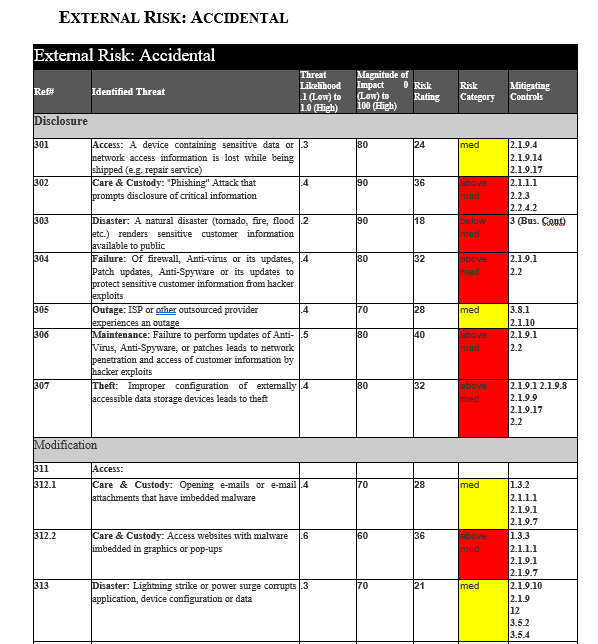
**3.1 Physical Security**

According to ZirMed policy, “Physical security is an essential part of a security plan. It forms the basis for all other security efforts, including data security.” Physical security encompasses any efforts made to guard company buildings, equipment, and their data. Threats can range anywhere from natural disaster to vandalism.

Building access is the first layer of defense against threats. Locked access points, a receptionist, security guard, badge keys, and monitoring cameras are the major components of building security. Within the building, each floor is considered a “suite” and may only be accessed with the appropriate badge key.

The most critical intellectual property is kept inside the company’s network and server rooms. As expected these rooms have the highest level of restriction. This is achieved through hard-walled rooms, locks, CTO-approved access, and high-level monitoring.

**4.0 Risk Assessment**

Risk assessment is the first step in the IS management process identified by the security team. All known company threats have been compiled and organized into four quadrants - first by internal/external, then by deliberate/accidental risk. Each item is documented and given a reference number, title, description, threat likelihood, the magnitude of impact, risk rating, risk category (low to high) and it’s corresponding controls. (See figure below)

**5.0 Classifications**

**5.1 Highest Ranked Threats**

After reviewing each of the most critical risks, the most obvious theme is the protection of client information. This is highly sensitive information that is legally protected by HIPAA and therefore requires the utmost precaution. Some examples of these threats include:

* Risk 102.1: E-mail containing sensitive customer information sent via unsecured/unencrypted means.
* Risk 102.2: Unauthorized accidental disclosure of sensitive customer information either in conversation that is overheard or paperwork in view of an unauthorized person.
* Risk 107.1: Staff falls prey to Social Engineering attack that directly, or as a consequence, gains access to sensitive customer information.
* Risk 122.1: Backup media or mobile computing device containing sensitive customer information is lost, stolen or destroyed.

ZirMed does a commendable job of providing secure services despite these known risks. As mentioned above, each item references the controls put in place to combat them. These will be further discussed throughout the paper, as they are highly important features of information security.

The company must also put effort into complying with HIPAA expectations. In order to do so, they have developed a separate chart that connects company policies that cover those issued by HIPAA. Having this information in one consolidated list is crucial in the event that the company is going through an audit.

**6.0 Corporate Standards/Policies**

**6.1 Privacy**

According to ZirMed policy, the first day of orientation requires PHI privacy training. After the training, IT staff will train new employees on the proper login procedures as well as provide them a thorough guideline of rules and best practice for software and hardware use. This comprehensive training assures that every employee is exposed to proper privacy protection of customer information. This training is imperative to the operations of ZirMed because, without it, it would be illegal to conduct business according to federal law; and it would be unethical to transport, store, and deliver unprotected PHI.

**6.2** **Unacceptable Activities**

The ZirMed policy provides direct responses to certain scenarios that users should absolutely avoid while conducting business in, and out of the workplace. The policy outlines the expectations of employees such as how to maintain their work environment, password, email, usage of the Internet, usage of the intranet, instant messaging, and mobile computing devices. An example of the depth of which the policy goes into, the policy guideline for e-mail exchanges contains a subcategory of six nested guidelines such as using caution when sending e-mails to outside networks. This specific subcategory goes at length to define best practice when dealing with message exchanges outside of the internal network which is very important to the protection of the overall system because, without this training, employees may be unaware of the high risks they take when sending e-mails to external networks.

**6.3 User Responsibility**

As with all policies, users must maintain a large set of responsibilities in order to actually abide by what an organization set out. To remain effective, the information security team must be consistent on pushing user responsibility to ensure that the front-end users are aware of the risks they pose, and to defend against them. User responsibility is also pushed, not just through policy, but through culture. It also gives rules and procedures to handling information, reporting security concerns and responding to security alert issues. Fortunately, the policy is enforced by the culture of the company and is understood by many employees to be of the utmost importance. It is worth noting that user responsibility places trust within end-users to uphold the procedures and guidelines set forth in the policy.

**7.0 Employees**

Employees are considered one of the largest threats to information security because they are most often in contact with sensitive information. It is important that management applies safeguards like training, background checks, and monitoring in order to avoid staff related risk.

Before hiring candidates for positions within the company, human resources must put them through extensive screening processes. Often employees undergo a multiple-interview process but are always run through several background checks. SSN verification, multi-state criminal records check, and OIG/GSA exclusion checks must be passed before being considered for hire.

A new employee is able to gain any access privileges or company passwords they must complete company-issued training on HIPAA Privacy and Personal Information privacy. IT staff will guide new associates on proper login procedures and workstation expectations. Therefore employees are not given the opportunity to use any systems/applications without first learning about their potential for information corruption. This allows the company to avoid employee ignorance altogether as a reason for major security compliance issues.

Within the first 30 days of employment, individuals are expected to participate in a Security Awareness Training program. The same training is conducted annually for all other employees. This is ZirMed’s way of keeping users up-to-date with current security issues and expectations. Other methods of providing company-wide security awareness have been implemented as well. These involve annual online refresher courses, screens throughout the building, special training due to company changes, and email alerts/reminders.

**8.0 Security Compliance**

**8.1 HIPAA**

One of the most important security goals for ZirMed is to abide by the standards set forth by HIPAA. There is a detailed, and comprehensive table mapping each requirement from HIPAA to a specific address in the ZirMed policy documentation. For example, a HIPAA standard that requires any area where there is a workstation to have security (that is to only allow authorized users into the space) will have a specific statement written in the policy detailing the resolve to align with the requirement.

With HIPAA compliance at the top tier of ZirMed’s priority, many of the security controls throughout the organization can be traced back to a HIPAA requirement. For instance, the orientation process for new hirees includes training programs on HIPAA compliance and PHI. This is an implementation derived from the standard HIPAA requirement of security and awareness training.

Many physical controls also root themselves to HIPAA requirements. ZirMed maintains access to each floor through the installment of hardware at each entry point which grants access to only authorized users. These physical controls are in direct response to the HIPAA requirement stated above where workstations must have security. This pattern of administrative controls that trickle from the top-down and comes to fruition into physical or software controls seems to be the standard for ZirMed’s compliance with HIPAA.

**8.2 Vendor Compliance**

ZirMed’s HIPAA compliance policy documentation also states the vetting guidelines for the selection of a third party vendor to do such work for ZirMed such as air conditioning maintenance, plumbing, electrical work, paper shredding and hardware disposal, and fire suppression systems. Qualified vendors doing this work, according to ZirMed’s policies, must also be HIPAA client so as to not compromise the security of ZirMed’s already compliant practices. There is an exhaustive list of procedural controls regarding the vendor’s operational standards such stipulating a contractual agreement on the vendor’s proper handling of a security incident with the ZirMed information security team, as well as notice of a staffing changes within 24 hours through a change to a list of all active vendor staff members working on the contract.

ZirMed also documents that the vendor contracts must specify the following:

* The information acquired by the vendor in the course of the contract cannot be used for the vendor’s own purposes or divulged to others.
* The Vendor must only use ZirMed information and Information Resources for the purpose of the business agreement.
* How ZirMed information is to be protected by the vendor.

This, as we understand it, is an attempt at risk transference for ZirMed so as to shift the legal responsibility to the vendor, and to contractually assure that ZirMed is protected if any such event arises. However, if a leak in PHI was severe enough, ZirMed would still be required by HIPAA law to report to the affected victims that their PHI was exposed. The depth to which these contract stipulations are able to protect ZirMed remains to be unclear, however, we believe we can safely assume that including such stipulations is more than the bare minimum protection and can successfully transfer risk in minor to medium breaches.

**8.3** **PCI DSS**

Alongside the compliance with HIPAA regulation, ZirMed’s documentation supports a high level of dedication in complying with PCI DSS requirements. Just as ZirMed addressed HIPAA requirements, they address PCI DSS policy using a large table denoting the requirements with exactly how, and where they implement controls in response.

A large part of becoming compliant with PCI DSS is having system events monitored and logged for PCI DSS auditing. ZirMed implements multiple software to ensure this compliance expectation is met and available. There is a comprehensive list of monitoring tools used and some notable vendors include LogRhythm (SIEM) and Tripwire Enterprise Manager. Both tools offer a detailed logging throughout the system which enables the activity within the system to be, ideally, visible to PCI DSS auditors. Audits with PCI DSS are scheduled annually, and because of this ZirMed retains their logs for a minimum of three months to a maximum of one year.

**9.0 Risk Mitigation**

Risk mitigation begins first with the identification of security threats. It is only after this, that an information security team, and or policy, can respond to an actual security event. Normally, security alerts will be sent out by management officers, or by the information security team themselves. Some of the areas that should be alerted would be user access and activity audits, and network maintenance and change documentation. Security events resolutions are often a part of policy procedures so it may not be necessary to disperse a security alert if there is no expectation of furthering the threat. However, if the threat is deemed to have a high possibility of affecting the system further, or if the policy explicitly dictates that a security alert is to be sent, then the security team would undoubtedly distribute a security alert to either those affected, or to everyone in the company.

According to company policy, due to the high variety and complexity of threats to ZirMed information and network security, there is a great difficulty in providing specific direction for each issue. Therefore, the security team has placed general guidelines on when it is necessary to alert management of suspicious activity. Some of these instances involve lost/compromised passwords, file/email that causes sudden unexplained activity, unauthorized users attempting to access the network, etc.

When an instance is deemed worthy of an alert an employee is expected to get into direct contact with a member of the security team to describe the problem in detail. Those thought to be less immediate may be issued to appropriate staff via E-mail or other message types. Employees should consider it a high priority to send alerts when needed because they are directly responsible for any insecurities in their passwords and/or workstations.

In the day-to-day practice of the ZirMed organization, there are multiple controls that an employee, vendor, or guest would have to go through in order to gain access to reasonably valuable areas within either the building, hardware, or software. This is apart of ZirMed’s layered security approach. This model mitigates threats to the network and organization by setting multiple controls, one after another, in order to stop a variety of security attacks. An example of this layered security approach would be a firewall, IDS/IPS, anti-virus, and Anti-Spyware technologies. Moreover, while layers of security remain a logical approach, it will always come down to the employee, front-end user, or information security team to follow ZirMed policies and procedures to ensure all layers are implemented properly.

**10.0 Intrusion Prevention & Detection**

**10.1** **Firewalls**

Passwords to firewalls are highly secretive at ZirMed and as it currently stands, only the CTO and one member of the technical team have administrative access to firewalls. This extensive restriction ensures the least amount possibilities of a breach through the exposure of a password to the firewall. All traffic from external networks to the internal network is controlled using the firewall which allows the company to ensure that any detectable unauthorized, or inauthentic connection would not reach its destination. When an unauthorized connection is attempting to make a connection to the internal network, ZirMed Firewall Policies states that the threat agent must be contained in the demilitarized zone.

**10.2 Encryption**

Up until this past January, the information security professional we spoke with informed us that information in storage, we assume PHI and other company data, was not encrypted. However, in January they began using storage encryption. Going through the HIPAA requirements table, as previously mentioned earlier in under the HIPAA section, there is a required field stating that ‘data at rest’ must use file encryption. There is no date on the actual implementation of this control to resolve this requirement. This is important because the HIPAA data-at-rest-encryption requirement has been so even before January -- in fact, there are sources that reference it as a “new” policy in 2013 [(Spiceworks)](https://paperpile.com/c/ovBLTY/bsAu).

Nonetheless, there are technical safeguards in place that is designed to be used whenever appropriate according to policy. ZirMed requires that all electronic transmission of PHI or any other sensitive company information must be encrypted to ensure the protection of data in the case of a breach, either while in transmission or while in storage. This does include internal transmission of PHI and the company policy advocates that this should be done only when necessary and states that the best practice is to delete any such information after consumption.

**11.0 Conclusion**

Information security is fundamental for any company that handles sensitive data. ZirMed is a leading business in healthcare management services, and the information they process must be kept secure in order to protect their client base as well as company reputation. The security team and CTO have put in place policies and controls that allow them to manage their data and the items that contain them.

In order to maintain an effective security system, they follow a process that begins with risk identification, followed by risk assessment, policy and control implementation, user awareness/training, risk mitigation, and finally regular review alongside any needed changes. They must also be aware of their legal obligations to protect their data, in ZirMed’s case the need to comply with HIPAA policy and PCI DSS. These are addressed in the same management process mentioned above.

Without their careful evaluation and maintenance of information security ZirMed would not be the successful company they are today. Data corruption can cause a loss in business value, client trust, and may result in heavy legal fees. This is why copious amounts of time and effort are exhausted in order to avoid sensitive information falling into the wrong hands. While system processes and controls are likely to change over time, and vary from company to company, they will always be needed as a means to run a successful business.