Case Study

Why Do We Need **Proactive Support & Remote Monitoring** For Our DD Organization?

If you use a "set it and forget it" model for your IT system, it's only a matter of time before you'll be in trouble. This is what happened to the Clinton County Board of Developmental Disabilities. We explain more in this case study.

CLINTON COUNTY BOARD OF DEVELOPMENTAL DISABILITIES

What Problems Can We Expect From Unmonitored & Managed IT?

Just like our customer, you can end up with a fragile and vulnerable IT system that could result in:

- Security breaches that jeopardize your HIPAA compliance
- Reduced productivity resulting from IT downtime
- Decreased efficiency and ROI from your IT hardware and software
- Being in the difficult, costly, and time-consuming situation that comes as a result of a breach

How Did Monitored & Managed IT Help Their DD Organization?

Here's what happened to the Clinton County Board of Developmental Disabilities in Wilmington, Ohio and how we helped...

As we see with many organizations, the reality of the risks related to IT and private data are not fully understood. With that, the need for a professional partner experienced and focused on protecting the organization's IT infrastructure, staff, and private data is often improperly seen as just an expense, instead of the indispensable value and benefit it provides across the entire organization. In this specific case, they thought they had taken steps and did not have a company maintaining their IT infrastructure and experienced an intrusion into their server. They store private health information for the developmentally disabled who they serve throughout the county, so this was of great concern, as intrusions like this typically result in a breach of data that violates HIPAA regulations.

Unfortunately, that was the case here, as this did result in a breach and they had to go through the process of breach notification, notifying anyone for which they had information. For HIPAA, a ransomware attack counts as a breach, unless you can prove the perpetrator did not take any data with them.

Like many organizations of this type, they thought they had taken steps toward ensuring their information technology infrastructure was protected. As the saying goes, "they didn't know what they didn't know." They thought everything was secure... what they didn't know, there was a vulnerability left unsecured that allowed for their breach issue. They thought they had reliable back-ups... what they didn't know, the back-up procedure was silently failing so they didn't have data they could rely on. They had strong passwords internally... what they didn't know, a vendor account with remote access did not have the same policy. On the surface, they felt they were fine. However, with their IT not being actively maintained and managed, they were extremely vulnerable.

Then, the intrusion happened. Superintendent J. Kyle Lewis took quick and proper action, handling the situation very well. He knew he needed immediate professional assistance. His actions most likely prevented further potential issues. After being referred to us by another County Board client, as well as by the Ohio Association of County Boards (OACB), we got to work for them right away, quickly mitigating the problem, getting them back in control of their equipment, securing their network, and beginning the painstaking process of researching and helping them respond to what had occurred.

As a result of our quick response and effectiveness, the Clinton County Board of Developmental Disabilities decided to bring us on to handle all their IT management, monitoring and maintenance. We applied our full Managed IT Service and best practices to bring their systems and processes current and provide them with the security and peace of mind they needed. This included:

- **Remote Desktop Services**
- **Email Encryption**
- **Virtual Datacenter Services via The Reliable & Secure GO Concepts Private Cloud**
- **Mobile Device Management**
- **A Complete Data Back-up and Retention Solution with Disaster Recovery**

Today we provide full Managed IT Services with 24x7x365 access, monitoring, maintenance, and emergency response, along with 7-day-a-week Help Desk and Walk-in Support. This includes Remote Management & Monitoring to detect and block IT intrusions, along with vCIO services and assistance with audits and surveys for security and HIPAA compliance, and a Virtual Datacenter that ensures they are always up to date and have a reliable back-up and disaster recovery solution. Now they can focus on their operations and how information technology can drive their organization forward.

GO Concepts
Don't worry about IT.

They now benefit from:

- A secure and reliable IT infrastructure.
- A reliable and secure private cloud with state-of-the-art server hardware and the latest versions of software.
- A complete data back-up and retention solution with disaster recovery.
- Alignment with best practices for their information technology.

- Reliable and secure remote access to their industry-specific software.
- Support they can trust will be there to help them when they need it.
- Better compliance with HIPAA.
- The tools to help increase efficiency and TCM.
- Technology they can rely on.
- And, they "Don't worry about IT."

J. Kyle Lewis, Superintendent of the Clinton County Board of Developmental Disabilities explains:

"In March of 2017, we experienced an intrusion of our server. I was referred to GO Concepts, so I contacted them immediately and they were on site within one hour. The GO Concepts' team members worked closely with me and my staff to resolve the immediate issue very quickly. It was very reassuring to have a team of experts by my side to guide me through a stressful situation.

I was so impressed with GO Concepts that, ultimately, I decided to partner with them for our IT needs. They worked closely with us to bring us into full HIPAA compliance. That was not something that happened overnight. It was a process. HIPAA compliance can be very daunting. GO Concepts made it very manageable for us.

J. Kyle Lewis

Approximately one year after contracting with GO Concepts, I brought in an outside company to conduct a thorough risk assessment. Not only did I have the company review this board's policies and practices, but I also had them review GO Concepts. The results of the review demonstrated substantial compliance.

Partnering with GO Concepts has been a great business decision. I am now confident in our IT processes, systems, and practices. Their motto is "Don't worry about IT!" I can honestly say that I no longer worry."

How Will Proactive IT Service With Remote Monitoring & Maintenance Benefit Our DD Organization?

Proactive IT Service and Remote Monitoring & Management (RMM) will ensure that your systems are protected and reliable. An RMM tool allows your Managed IT service provider to assess the health and security of your system on a 24x7x365 basis.

Proactive IT Service and RMM tools not only gather information regarding how your hardware and software are operating, but they insure operating system and application software, along with anti-virus/anti-malware programs are always up to date, in order to help identify and block potential security threats and possible breaches, ensuring your confidential data remains secure.

Proactive IT Services include taking steps to prevent malicious processes and protect the security of your employees and your confidential data. It also means providing ongoing security training for employees, testing their recognition of dangerous phishing attempts, and ongoing monitoring of the dark web for data related to your organization and employees that would leave you vulnerable to a breach. This especially true when it comes to HIPAA compliance.

GO Concepts
Don't worry about IT.

The RMM tool also supplies your Managed IT company with activity reports that allow them to remotely get to the root of IT issues and resolve them, many times before users are even impacted. It provides tracking for trouble tickets, remote desktop monitoring, and an interface for user support.

With Remote Monitoring & Management, we can fix issues without signing directly into an infected machine even if you're still using a server or computer. All of this enhances the overall performance of your IT infrastructure because issues can be identified and resolved before they create problems.

Will Proactive IT Service & Support Include A HIPAA Compliance Plan?

The right Managed IT service company will always help you implement a HIPAA Compliance Plan for your DD Organization in Ohio. It should include the following:

1. **Designate a Privacy and Security Officer** – This needs to be an employee. Your IT Managed Services Provider (MSP) can provide guidance, help with policy, and support for this person in order to ensure your company remains compliant. This is a foundational building block for your compliance success. Hiring an individual or MSP who has a track record of success is critical for HIPAA compliance.

2. **Perform Risk Assessments** – This is an overall review of both macro and micro levels to ensure your electronic protected health information (ePHI) is secure. This is a mandatory aspect of any DD organization's compliance endeavors. Not only is it mandatory, but it's the foundation for implementing safeguards to better protect your confidential data.

3. **Implement Policies and Procedures** – You must provide your employees, and anyone who handles your sensitive information, a blueprint explaining the do's and don'ts when it comes to HIPAA compliance. Your blueprint must continuously be updated and adjusted as you implement your compliance planning. For example, encryption is necessary to protect electronic protected health information (ePHI). This is an extra layer of security, comparable to an unbreakable password. Other standard procedures like locking a laptop when it's not in use should be included in your policies and procedures. There are other examples where policies and procedures will help ensure your DD Organization's HIPAA compliance.

4. **Train Your Employees** – Ongoing Security Awareness Training for your employees should be implemented to ensure everyone in the organization understands your policies and procedures. Training only once a year is not enough. The best plan in the world can be ruined by an employee who doesn't understand what they can or cannot, should or should not do, and is not aware of the latest sophisticated attempts at fooling them. Take the time to regularly train them on best practices for handling sensitive information and what constitutes a HIPAA violation. This is also a mandatory aspect of HIPAA compliance.

5. **Develop and Implement an Incident Response Plan** – What if you've done everything that you should? And you've "checked all the boxes" but you still experience a breach? Report it! — Have a plan in place to identify and respond to a threat. Once the source is identified, stopped, and documented, it must be reported. From this point on, you should have a prevention plan in place to ensure a breach doesn't occur again.

What Can We Take From This?

DD Organizations in Ohio are exposed to daily dangers and threats to their HIPAA compliance status. With proactive Managed IT Service & Support, Remote Monitoring & Management and a HIPAA Compliance Plan you can feel assured you'll be protected from security threats, data intrusions and HIPAA violations.