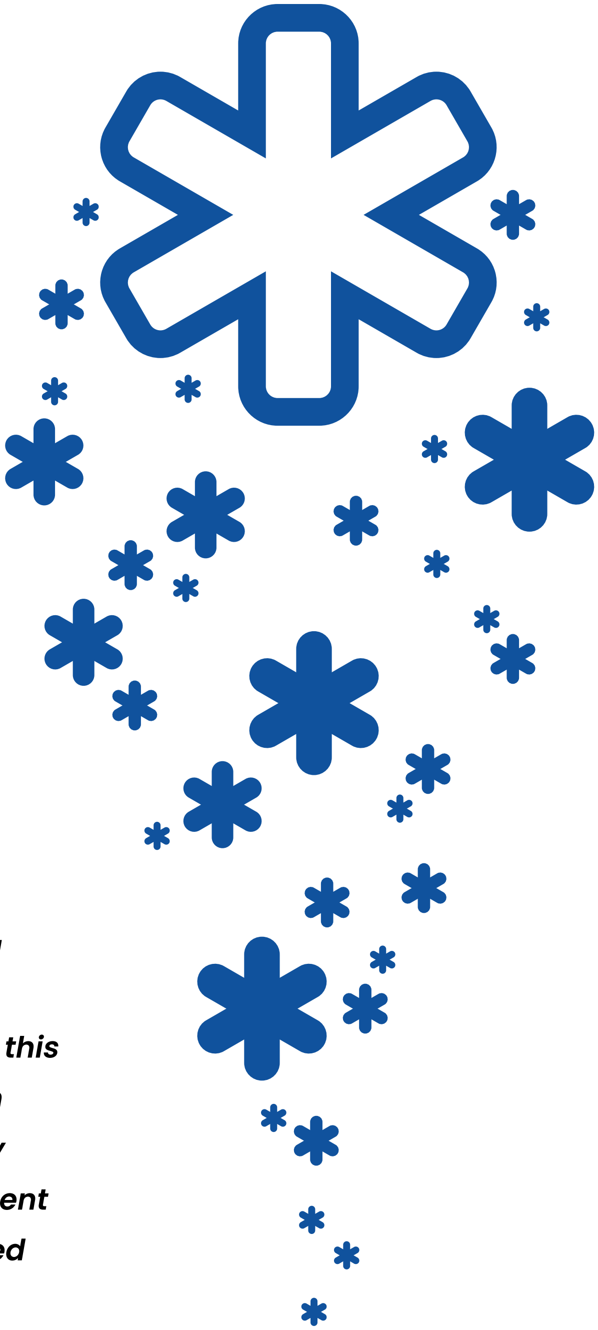
HOW TO BUILD A *HIPAA COMPLIANT* STACK.

Compliancy Group

CONTENTS.

What’s the Big Deal About Healthcare?



It seems like every article you read tells you to find a vertical market to focus on - but with so many options, why is it that healthcare is such a big focus?

The healthcare vertical is full of opportunity. Since HIPAA requires healthcare organizations to protect patient data, they must implement advanced security measures. Most healthcare businesses rely on MSPs and MSSPs to meet their security needs.

Part of a healthcare organization’s HIPAA compliance requires them to undergo a security risk assessment to identify their security deficiencies. These businesses then need to address those deficiencies to meet their HIPAA requirements, providing a huge opportunity to you as their trusted security advisor.

Jesse Perry, Founder, JP Technical - on how the HIPAA audit process opens doors for him when speaking to his clients.

“There’s so much money to be made helping my existing clients become HIPAA compliant because once they go through all this work – when it comes to remediation, it’s this guy who has to help them put these things in place. Then that drives the next six months for the customer. Not only am I doing my customer a solid by helping them implement things they need to do anyway, and I’m well compensated for doing the work. It’s completely win-win.”

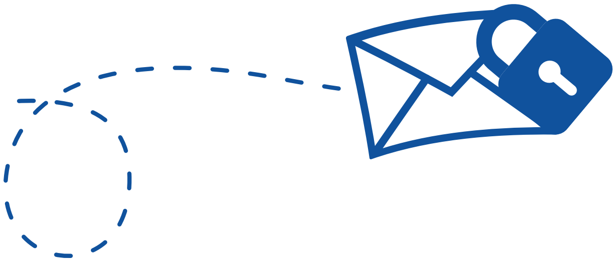
What to Include in Your Healthcare "Stack".

Tools Needed to be HIPAA Compliant

A key aspect of HIPAA compliance requires any business that has the potential to access patient data – known as protected health information (PHI) – to be HIPAA compliant. This not only applies to your healthcare clients but also to you as their service provider. What many organizations miss, however, is the fact that all software tools used in the management of their healthcare data have to be compliant as well. Sure, we all know your backup solution needs to be compliant, but what about your RMM?

Some indications of a HIPAA compliant tool include encryption, access controls, user authentication, audit logging, and the ability to sign a business associate agreement (BAA).

Email Protection



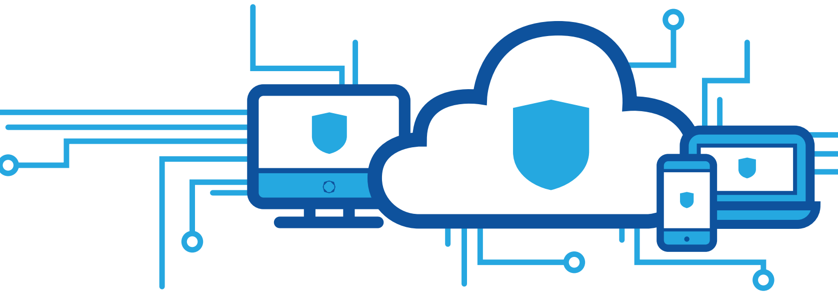
- Threat Detection
- Email Backup
- Encryption

Email is the number one source of all breaches. Email security starts before the message gets delivered. All emails containing patient information must be encrypted and backed up.

mailprotector

Dropsuite

Endpoint Protection



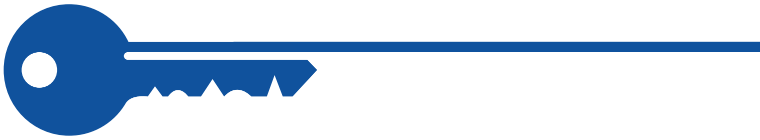
- EDR
- Ring Fencing
- Antivirus

todyl SOPHOS Cybersecurity delivered.

THREATLOCKER

Endpoint protection should be a part of any HIPAA stack.

We have moved beyond antivirus - preventing zero-day attacks a better toolset.



Access Management

- Password Management
- MFA
- Directory Services
- Identity Managers

HIPAA mandates access management for all accounts with access to ePHI. You must assign individual accounts with unique credentials.

HIPAA requires access to patient data to be restricted and tracked to ensure minimum access is maintained.

Microsoft Azure JumpCloud

Data Loss Prevention

- Offsite Data Backup
- Disaster Recovery

Microsoft Azure actifile

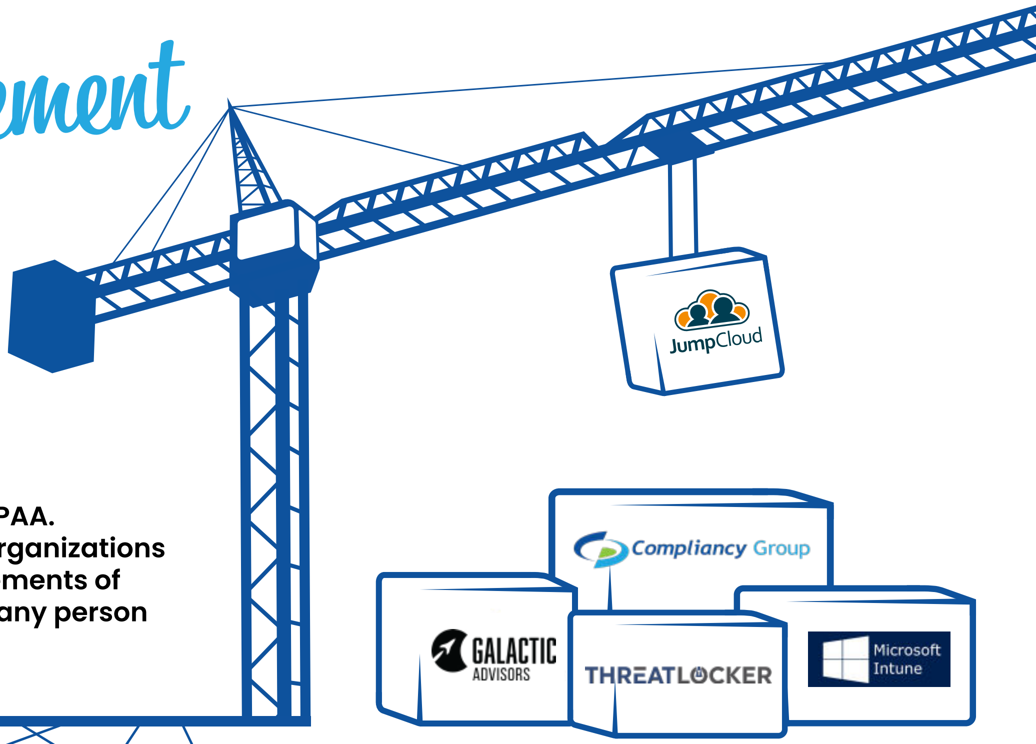
Data loss prevention is essential in healthcare, you must know what you have, where it is stored, who can access it, and where they send it.

HIPAA requires healthcare organizations to maintain exact copies of records stored at an offsite facility.

Asset Management

- Inventory Tracking
- RMM Tools
- Vulnerability Scanners
- SCM

Asset management is required by HIPAA.
The HIPAA Security Rule states that organizations must “maintain a record of the movements of hardware and electronic media and any person responsible thereof.”



Network Management

- Firewall Controls
- WiFi Controls
- DNS Filtering
- Network Scanners

todyl LUMU

SOPHOS
Cybersecurity delivered.

Network management - HIPAA requires effective network security. How effective is a firewall by itself when half of your employees work remotely?

Network based attacks against healthecare organizations (and supporting vendors) are on the rise. Protect the edge in order to protect the endpoint.

BACK TO CONTENTS

Vulnerability Management

- SRA
- Vulnerability Scanning
- RMM
- SCM

Vulnerability management is arguably one of the most important parts of HIPAA.

Healthcare organizations that fail to identify weaknesses and vulnerabilities to their data, and implement measures to mitigate them, are often breached and subject to fines.

Incident Response

LUMU

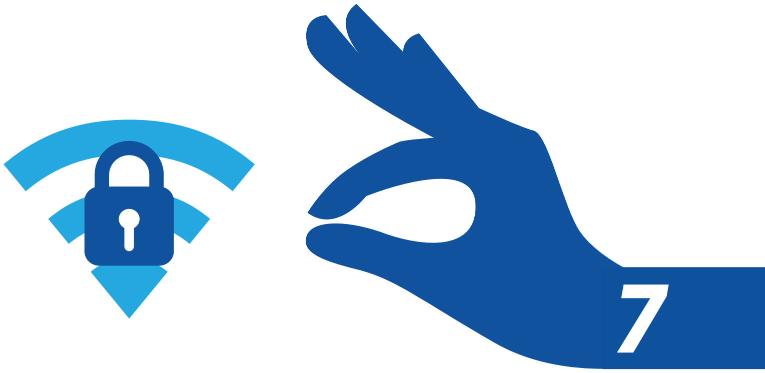
blackpoint

HUNTRESS

- Policies, Procedures, and Training
- SOC
- SIEM
- MDR
- Logging, Monitoring, and Auditing

HIPAA requires organizations to have a system in place to detect, mitigate, and respond to breaches.

To meet incident response requirements it is not only important to have tools in place to detect incidents, but also to have policies and procedures for breach response.



Medical Device Safety

- Firewall/Network Security
- Policies

Medical devices are increasingly connecting to healthcare networks.

Since many medical devices are operating on outdated operating systems, they can pose a huge risk to an organization's security.

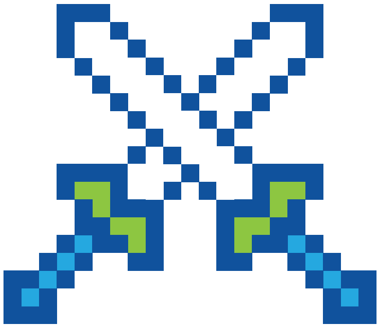
SOPHOS
Cybersecurity delivered.

THREATLOCKER

Compliancy Group

Cybersecurity Policies

Compliancy Group



- Roles and Responsibilities, Education, Acceptable Use, Data Classification, BYOD, Mobile, Incident Reporting.

Cybersecurity policies are written policies dictating an organization's security controls and procedures.

Cybersecurity policies must be aligned with HIPAA standards, including what administrative, technical, and physical safeguards are in place protecting PHI.

HIPAA Compliance as a Service.

A total HIPAA security stack wouldn't be complete without adding HIPAA Compliance as a Service to your offerings.

You can benefit from your current client relationships while building new ones by simply providing Compliance as a Service alongside your other offerings.

In addition to the potential for new revenue streams, having a strong HIPAA Compliance as a Service offering can improve your relationship with professionals in the healthcare field.

> Jesse Perry, Founder, JP Technical - commented, *"So I'm not just a customer. I can help my customers do this too, and it was a very low barrier to entry. I didn't want to just turn my clients over to some company that I didn't know without knowing how they would take care of them. By going through Compliancy Group's process myself first, I got to see how everything works."*

Conversations with Compliancy Group's staff were pivotal to the growth of his business. Perry saw the potential that HIPAA created for him in becoming his client's trusted advisor.

He was also able to determine which other tools were essential for creating a complete stack that would provide his clients with the security tools they needed to meet HIPAA requirements.