lightcrest

HIPAA Compliant Infrastructure Services

Real Security Outcomes. Delivered.

Deploying healthcare and healthcare related services to the cloud can be frightening. The requirements of HIPAA can be difficult to navigate, and while many vendors claim various levels of HIPAA-compliance, most of them treat the requirement as a check-box instead of a **holistic compliance regime**.

The Philosophical Difference

We know many of our competitors offer pre-packaged "compliance as a service" offerings. It is an understandable approach to try to package something complex and make it simple, and while at Lightcrest we agree that packaging of complex services will help you simplify and better structure costs related to HIPAA, we seek to address the deeper causes of risk and cost related to managing electronic Personal Health Information (ePHI) in the cloud.

For Lightcrest, HIPPA and health care compliance are not just a service to be packaged and sold. Understanding and properly implementing HIPPA and protecting ePHI requires skills more fundamental than traditional service delivery. True compliance requires a culture and attitude that seeks to deeply know and understand what needs to be done to protect the interests of your customers, your staff, and your other stakeholders.

Some organizations treat compliance to regulations like HIPAA like a burden. We know you aren't just doing HIPAA because you have to -- we know you want to do the right thing with respect to your users. Your security is your reputation, and **your business success rests with the vigorous defense of your customers' data.**

Most security vendors see HIPAA as a golden goose. They use it as a lever to up-sell customers on more expensive managed security solutions and associated technologies, and the long-term relationship often suffers as a result.

Our philosophy is to protect your customers and your shared interests. We don't measure success in how many packages we can sell, but in **the long term satisfaction and retention of our customer relationships**. That means applying a right-sized risk-based approach which focuses controls where they will be most effective.

Lightcrest is also keenly aware that HIPAA compliance is about demonstrating management control over the risks associated with ePHI. This is not something that can be achieved through deploying a technology package, or achieved by simply signing a Business Associate Agreement. We provide you with the governance required to provide assurance at every layer of your infrastructure. Following cloud provisioning, Lightcrest works closely with your development team to ensure secure and compliant deployment of your application. Our experience is that this phase often involves new risk discovery as we identify use cases and controls that may not have been identified in the initial

assessment. Change is part of the natural progression of business, and Lightcrest works lock-step with your team to ensure your risk assessment and infrastructure controls are updated to accommodate the necessary changes.

Before final deployment, Lightcrest will coordinate a series of validation exercises to prove control-efficacy at every layer, from failover of web services to the data integrity and encryption strength of backups.

Our job does not stop there. As we continue to manage your systems, we will perform periodic validation assessments and update the risk register and architecture with you as your business evolves, as Internet threats evolve, and as regulations are updated.

Reference Architecture

Our reference architecture for HIPAA includes all of the components listed below. Not all components are required for every customer, and additional controls are available for customers with bespoke security requirements

PHYSICAL ARCHITECTURE	
• Dedicated Kahu Hypervisors • High-Octane SSD storage • Dedicated Firewall Pair • 20G Aggregate Ethernet Capacity • Redundant L2/L3 fabric • Dedicated Firewall Pair	Kahu Private Clouds provide customers with rock-solid security and compliance outcomes without sacrificing agility and performance. Single-tenant physical architectures allow for custom HIPAA compliant clouds, while Kahu APIs and Analytics dashboard provides all the agility and elasticity of a cloud environment.
LOGICAL ARCHITECTURE	
• Highly Available Load Balancer Instances • Highly Availability at Every Application Tier • Encrypted Backups • End-to-End Application-Layer Encryption • VPN concentrators • 802.1Q VLAN and optional VXLAN	Lightcrest engineers provide logical architectures to minimize attack surface, maximize application availability, and streamline compliance adherence. Customer applications are highly available at every layer of the stack, with no single points of failure at any physical or logical tier. Customers have complete control over their data in a private cloud, and have a much smaller exposure to threats compared with public cloud environments.

MANAGEMENT AND ADMINISTRATIVE CONTROLS	
• Risk register • Dedicated, Customized Cloud Runbook leveraging Lightcrest best practices	Provide up-to-date state of HIPAA control effectiveness to management.
PHYSICAL CONTROLS	
• State of the art datacenter with redundant power and cooling systems • State of the art datacenter security -- biometric access controls, cameras, locked cages and cabinets • (Optional) Datacenter locations in different geographic regions	Exceeds all HIPAA requirements for physical protection of PHI.
NETWORK CONTROLS	
• Dedicated network address space routed through multiple high-speed carriers • Dedicated, customizable Layer-2 network segmentation -- internal segmentation is available if you choose • Dedicated network firewall • Dedicated network intrusion detection (optional network intrusion prevention) • Dedicated VPN endpoint • Dedicated load balancer with built-in WAF and DDoS-mitigation capabilities • Quarterly network security vulnerability scans, both internal and external • Availability and performance monitoring of your exposed application endpoints	Protects your ePHI from a range of external attacks, and helps prevent intentional or unintentional data leakage.

CLOUD CONTROLS

- Private, Hybrid, and Public Cloud Integration
- Dedicated, security-hardened hypervisors are highly-available, with zero downtime virtual machine migration capabilities
- Your data on your disks -- no commingling of data, and you can choose to encrypt all data at rest

Guarantees the core infrastructure supporting your HIPAA applications are available and secure.

With a private Kahu cloud, the security risks associated with public cloud environments are significantly reduced. The attack surface is significantly smaller and EPHI is never stored on shared infrastructure.

Dedicated resources also eliminate the risk of cotenancy affecting your ability to meet your critical guarantees for availability.

BACKUP, RECOVERY, ARCHIVE

- Dedicated backup server(s) for encrypted backups with your private keys -- your encryption keys never leave your cloud
- (Optional) Off-site data replication
- (Optional) Scale-Out Storage for Archive -- on-premise, off-premise, or both
- Secure data archive and deletion services, or we can ship your physical disks to a data archive or destruction service of your choice

Mitigate loss of privacy data with encrypted backups, and archive critical ePHI to meet long term retention requirements.

OPERATING PLATFORM SERVICES

- Choose from Lightcrest's hardened OS images or supply your own
- Choose from Lightcrest's pre-configured highly available service configurations, or manage your own configuration.
- Regular platform security vulnerability and scanning patching

Guarantee the security of the operating platform for your applications.

Lightcrest best-in-class platform images include mandatory security controls and signed binaries which completely eliminate the possibility of malware running on your hosts.

DATA PLATFORM SERVICES

- Choose from Lightcrest's secure and highly available database server configurations, or manage your own configuration

Database level encryption of EPHI, high availability, and a range of other features designed specifically to address HIPAA handling requirements.

Data masking, fine grained data access controls, and other data security services can help protect the privacy and integrity of data, while extending the usability of the data to your business.

APPLICATION SUPPORT SERVICES

- Dedicated Monitoring, Trending, Alerting
- Dedicated Log and Audit Services
- Dedicated Identity and Access Management Systems
- Regular Application Vulnerability Scanning and remediation support
- Configuration Management and Deployment Services

Additional services, including security consulting to ensure your application and cloud environment are hardened at every layer of the OSI model and at every stage in the application lifecycle.

Fine grained access controls, two factor authentication, increased SDLC automation, and segregation of duties all help increase application security.