



HIPAA COMPLIANT HOSTING

SECURE YOUR PATIENT DATA
WITHOUT INVESTING IN SME'S

HIPAA COMPLIANT HOSTING

SECURE YOUR PATIENT DATA WITHOUT INVESTING IN SME'S

LIGHTCREST HIPAA COMPLIANT HOSTING

Lightcrest provides secure, compliant hosting environments to customers around the world. Our clients in the healthcare industry are able to spend more time on brick and mortar HIPAA requirements (like handling physical paper/patient files) by outsourcing the electronic requirements of HIPAA to Lightcrest.

Secure infrastructure tailored specifically to your needs will keep your patient data protected from malicious hackers and unauthorized personnel. From firewalls and dedicated networks to hardened databases and log archives, Lightcrest will ensure you have the physical and logical security necessary to keep your patients' best interests at the forefront of your business.

Let your medical experts do an even better job by off-loading the electronic aspects of HIPAA to Lightcrest. Here are just a few examples of secure HIPAA compliance solutions we provide:

- Virtualized data silos
- Encryption of structured and unstructured data
- ACL-enforced search engines and portals
- Hosting of medical billing systems
- Hosting of patient management systems
- Hosting of electronic medical record (EMR) systems
- Commercial application hosting for healthcare professionals
- Turn-key, secure computing instances for medical SaaS
- HIPAA compliant website hosting in Linux or Windows
- Virtualized private environments for extranet and intranet applications

We work with private medical practices, dental care providers, medical billing firms, vision providers, and insurance companies everyday to maintain their critical applications and HIPAA compliant systems. Even if you're not a healthcare provider, you can benefit from our services if you have customers who are, by passing on our expertise and infrastructure as your own. Have the confidence and the security portfolio you need to win new business with healthcare customers looking for HIPAA compliant partners.

All HIPAA Compliant Web Hosting Solutions Include:

Application Layer Protection for HIPAA Compliance

- Help prevent trojans, worms, and viruses from traversing your infrastructure
- Isolate and contain malicious and spurious traffic before it hits your systems
- Stop Cross-site scripting and SQL injection attacks

HIPAA Compliant Architecture

- Segregated physical infrastructure and DMZ's tailored to specific "zones"
- Even virtualized web servers and databases are maintained on separate infrastructure
- Lightcrest SpeedStacks provide efficient deployment mechanism for quickly duplicating virtual environments without compromising security
- Enterprise grade network infrastructure and scaling hardware
- Enterprise grade servers
- Automated "sleeping" user logout



HIPAA Compliant Customizable Security Rules

- Centralized Cisco firewalls and Linux netfilter hardened relative to your needs
- Application level monitoring and intrusion detection systems
- Custom trip wires to alert all stakeholders of file system modifications
- Detection of brute-force attacks & abuse of remote logons
- Custom backup strategies with retention minimums
- Forced authentication expiration
- Asymmetric encryption algorithms reduce efficacy of man-in-the-middle style attacks
- DSA and RSA key enforced two-factor authentication
- Tunneling to all branch offices via IPSec and encrypted Cisco GRE
- Disaster Recovery, triple redundant backups, black-out-proof DNS

Log Management

- Archived and searchable index for all systems logs relative to customer requirements
- Alerting based on detection of malicious exploit signatures
- Kernel level filesystem alerting

HIPAA Compliant Physical and Logical Security Policies

- All physical, network, and systems changes are documented
- Biometrics, multi-tiered security personnel, cage-level surveillance, and man-traps lock down physical datacenter facilities
- Strict data retention/destroy policies
- Hand scanners on all cage infrastructure

Ongoing Vulnerability Scanning

- Daily scans of all known vulnerabilities and newly released zero-day exploits
- Reports on host and network level vulnerabilities
- Implicit IP ACL's that assume systems are vulnerable until proven otherwise
- Anomaly-based intrusion detection systems
- 10G backbones and 1G distribution-layer links to buffer DDOS attacks
- Null routing capabilities






Lightcrest

11835 WEST OLYMPIC BLVD. SUITE 415E, LOS ANGELES, CA 90064 | 888.320.8495 | www.lightcrest.com