The Healthcare challenge to protect patient information - HIPAA Compliance
Introduction

Every industry presents its own challenges, and the healthcare industry has its own. Healthcare Organisations (HCOs) need to maintain a perfect balance between strict security and privacy regulations with an increasing pressure on enhancing the existing IT infrastructure. Compliance and implementation of new technological updates like including Electronic Health Record (EHR) also remains a concern. Apart from these, increasing pressure to reduce costs, scarcity of IT talent in this industry, is also a cause of concern.

In this whitepaper, we intend to highlight the common healthcare IT challenges, discuss the recent updates in HIPAA compliance and how Cyberoam helps Healthcare organizations to comply to it.
Healthcare IT Challenges

Considering the IT challenges of the healthcare domain in detail, we have the following issues that need attention. These issues include:

**Data breaches**
HCOs today host large data including sensitive patient data, confidential organisational data, intellectual property and also virtual connections to life-critical equipments used for patient care. An attack on any of these can lead to threatening scenarios. Data breaches are common occurrences today in HCOs. A full 94% of healthcare organizations were breached in the last two years, a trend recently highlighted by Backgroundcheck.org. Secure and safe networks are must for HCOs, both to establish credibility and trust. But with such rising cases of breaches, HCOs are finding it difficult to maintain secured networks.

**Mobile health and BYOD**
Mobiles have reached every business today, and healthcare is no exception. Healthcare professionals today use smart phones and tablets to remotely access patient records and for such similar activities. The ease and reach mobile healthcare offers, makes it an ideal choice among healthcare service providers. As a result, the HCO networks also include traffic from personally-held devices such as iPhones, iPads, and Android devices. An article by Tuaw estimates that approximately 22% of physicians in the U.S. now use iPads in their practices. Mobile devices have become an integral part of HCOs, in terms of technological advancements and need of the hour. But are the HCOs prepared with network security to accommodate this change?

**Telemedicine**
Although telemedicine has been around for years, with evolving teleconferencing and web conferencing techniques, it is gaining traction as never before, quotes the New York Times, in their article on telemedicine. "According to Hospitals and Health Networks Most Wired 2011 survey, 27% of physician offices and 42% of hospitals indicated that they provided telemedicine services", quotes Healthcare IT News in its article named ‘Telemedicine is on the rise’. These figures and quotes clearly indicate the rise in telemedicine. The benefits of telemedicine are numerous to both the HCOs and the patients, which include increased reach, better and faster care, increased revenues and so on. Considering the basic necessities needed for telemedicine, HCOs need constant and secure remote network connection; hence demand for solutions that cater to their exclusive needs is also growing.

**Uninterrupted and Secure Wireless Networking**
Wireless networks are a rather recent development in technology being used in healthcare, but they are sure to form a very
Healthcare IT Regulation - HIPAA

What is HIPAA?
Health Insurance Portability and Accountability Act – HIPAA is a Federal law, enacted by the U.S. Congress in 1996, to protect patient’s medical information and records. It seeks to improve the efficiency of healthcare systems by standardizing electronic data exchange and by protecting confidentiality and security of health data. HIPAA is a comprehensive law that affects technical and non-technical aspects of healthcare. Any entity who transmits any health information in electronic form, any provider of medical or health services or any person/organization transmitting health information in the course of normal business, need to comply to HIPAA. Such entities include Hospitals and other Healthcare Providers, Health Insurance Issuers, Healthcare Clearinghouses, Medicare Prescription Drug Card Sponsors, and even vendors who provide outsourced healthcare services (for medical billing, coding etc.). To meet with HIPAA compliance, HCOs and related entities are required to implement complete and efficient security solutions that will protect their valuable and sensitive information and assets.

How does HIPAA ensure security and uniformity in Healthcare domain?
An elementary benefit of HIPAA is that it supports the use of electronic transactions, by greatly simplifying healthcare administration and reducing administrative overhead costs. With growing intervention of technology and computerization of basic healthcare resources like patient medical records, HCOs face amplified security threats from various sources, like unauthorized network access, intrusion attempts, data breaches and other similar security attacks. Therefore HIPAA commands security measures be taken to protect this sensitive data, avoiding breaches and ensuring that only the authorised have access to the information. In order to achieve the same, HCOs need to constantly update their legacy systems, revamp their existing information security capabilities, and define and implement business processes that align with the set security objectives.

HIPAA: Updated and enhanced – More wider and stricter now
In recent times, HIPAA has been updated, and government now insists enforcement of HIPAA regulations. It also imposes financial penalties on violation of HIPAA rules. Besides this, the Health Information Technology for Economic and Clinical Health (HITECH Act) of 2009 has expanded the scope of the privacy and security provisions of the HIPAA and its enabling regulations.

The HITECH Act is designed to promote the widespread adoption and interoperability of health information technology and has brought about various changes in the HIPAA regulations, which includes stronger enforcement and stiffer penalties, increased notification requirements and implications for IT Asset Retirement. As per the official release by the U.S. Department of Health and Human Services recently regarding HIPAA and HITECH, the reasons stated for the modification include strengthening of privacy and security protection for individuals’ health information and protections for genetic information.

HIPAA requirements
As per the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II), definite security issues must be addressed and solutions are required to be implemented. Security of electronic Protected Health Information (ePHI), also known as safeguard initiatives, include the following:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

The HIPAA Security Standards do not specify any particular technological requirements, so every HCO must assess its own threat and develop its own security measures accordingly. Organizations are required to then certify their security measures. Therefore, to comply with the HIPAA Security Rules and ensure that all the various dimensions of HIPAA, including Administrative, Physical, and Technical Safeguards are implemented, a comprehensive and effective information security solution is inevitable.

Source:
Cyberoam enables HCOs to comply with HIPAA

Cyberoam’s integrated security offerings helps HCOs meet HIPAA compliance, along with ensuring security against other threats and challenges. Cyberoam Next Generation Firewall (NGFW) appliances along with Cyberoam Central console and Cyberoam iView, offer comprehensive security and highly reduce the mammoth task of managing security and compliance together. Its seamlessly integrated offerings ensure the availability of holistic and next generation solution for HCOs.

Cyberoam NGFW provides integrated Security over single platform and its features including Stateful Inspection Firewall, Layer 8 Technology (Identity based approach), Next-Gen GUI, On-Appliance Reporting, Real Time Traffic Discovery, Multiple Link Management, High Availability, Bandwidth Management, Web and Application Filtering, Intrusion Prevention System (IPS), Virtual Private Network (VPN) and so on, enable HIPAA Compliance. Cyberoam’s range of security solutions deliver comprehensive protection to healthcare organizations, ensuring centralized network and data security across distributed locations and for telemedicine with secure transmission of medical records anywhere in the world.

With the ever increasing demand for HIPAA compliance among HCOs, Cyberoam’s security controls helps healthcare institutions to meet the requirements of HIPAA compliance with security of patient medical records and employee information over the network. On-appliance reporting over Cyberoam NGFW and Cyberoam iView solutions deliver comprehensive visibility into network and user activity at multiple locations across the globe. Real-time identity-based security reports with Web Usage, Mail Usage, Blocked Web Attempts, Top Applications, and more provide visibility and historic data of user activity, ensuring rapid response, quick audits and forensics. Cyberoam NGFW helps HCOs meet these safeguard initiatives effectively.

Administrative Safeguards:

- Information Access Control
  Access authorization, establishment and modifications are among the parameters identified under this aspect of administrative safeguard. HCO administrator can implement these with Cyberoam’s unique Layer 8 Identity-based security controls available on its NGFW appliance which is integrated with all other security features it offers, allowing user-based network policies and doing away with blanket policies. Administrator can define the policies regarding who (user) can access which (data) using what (device), based on combination of Username, IP Address, Mac Address, eliminating unauthorized access to information. Administrator can also create work profile-based groups for ease of management.

- Security Configuration Management
  Risk analysis and management are integrated part of administrative safeguard and fall under the security configuration management. Cyberoam enables HCO administrators to adhere to these with its NGFW appliances offering Next-Gen User Interface (UI) that enables easy configuration of security policies based on Web 2.0 technology advantages; easy navigation, custom controls, and intuitive interface; and unified security controls that allow all security rules to be created from the firewall page, allowing fewer security errors and increasing security. This enhances administrator productivity and shortens learning curves.

- Security Incident Management
  HIPAA parameters include response and reporting as part of the security incident management. Cyberoam ensures adherence to these parameters with its On-Appliance Logging and Reporting tool ‘iView’ that offers

  - Logs & Reports
  - Identity based reports
  - Pinpoints the exact user for the incident
  - 1200+ drill down reports
  - Security incident management, compliance management, forensic analysis
  - Real time log management for security incidents
  - Alerts on unauthorized attempts

  On-appliance reporting eliminates the need to buy additional hardware/service to access these reports. Cyberoam iView also offers Traffic Discovery feature that offers real-time visibility into network activities.
Here are a few snapshots of reports under the compliance banner using Cyberoam.

Top Attackers Report:

Top Attacks Report:
Top Viruses Report:

• Internal Audit
  Internal audit is a very integral part of HIPAA compliance. HCO administrators can ensure seamless internal audits with Cyberoam’s On-appliance Reporting that offers complete Compliance Management Reports including Inbuilt Reports for HIPAA compliance and other compliances like SOX, PCI DSS, GLBA, and more. It offers 1200+ Drill-down Reports that facilitates Forensic Analysis to identify trail of activities and suspects in case of mishap. Its Identity-based reports pinpoint the exact user for the incident.

• Education and Training
  To facilitate user awareness and training, Cyberoam supports custom messages on various security events for educating the user about Security Policies. Network administrators can identify users who need education and training based on their individual identity based activity reports that include reports like ‘Top Denied Web Users’, ‘Top Attackers’, ‘Top Spam Senders’ and more.

• Information Availability
  Continuous network connectivity and business continuity are critical for timely access to information, especially in the Healthcare domain. Cyberoam ensures this by its features like Multiple ISP Link Management that offers Automated Link Load balancing for assured ROI/investment, Link Failover, and Policy-based routing by Source ID/Users/Protocols. Cyberoam also ensures Remote Access Connectivity with its features like VPN (IPSec, SSL VPN) over Cyberoam NGFW and VPN Failover for continuous remote access connectivity. Cyberoam’s High Availability feature is ICSA Labs Certified that reduces single-point-of-failure and ensures business continuity. It is IPv6 Ready and identifies and processes both IPv4 and IPv6 traffic.
Technical Safeguards:

- **Secure Communication**
  For requirements like these, HCOs can rely on Cyberoam as it offers encrypted tunnels for secure access to organizations’ network anytime, anywhere for virtually any endpoint. It offers secure VPN connection by scanning every packet for various types of threats like malware, spam, inappropriate content, and intrusion attempts. All VPNs, including IPSec, SSL, PPTP and L2TP, are supported from a single platform, allowing client-based and clientless VPN access. Network administrators also get secure remote Management of local networks or data centers.

- **Identity-based Authentication, Authorization, Audit Controls**
  Access control is one of the primary implementation specification requirements for HIPAA compliance. HCO administrators can adhere to this using Cyberoam that offers User / Device Authentication, Service Authorization, and Audit (Logs & Reports) over a single security device. Cyberoam’s Layer 8 Technology (Identity-based controls) applies at all stages.

Apart from the HIPAA compliance, HCOs that have multiple centers or remote infrastructures all connecting to the main HCO, centralized management over various appliance s is also a challenge. For such HCOs where there is a requirement for centralized management of security, Cyberoam offers centralized security control and visibility through Cyberoam Central Console and Cyberoam iView logging and reporting solutions. Cyberoam NGFW appliances deliver easy-to-manage, yet highly effective security in a single appliance at central and remote healthcare locations. Healthcare institutions gain secure remote access for telemedicine between remote centers and the central healthcare locations with the presence of specialists.

Cyberoam VPN ensures identification and access control of doctors logging in from home or other remote locations in addition to preventing malware entry from these remote endpoints into the central location. With the increasing ratio of Advanced Persistent threats and Insider threats, Identity-based Secure Authentication becomes a necessity to track attack attempts and take faster corrective actions. Cyberoam’s Layer 8 Identity-based security offers identification and access controls by the username, ensuring high levels of data and network security, despite the dynamic Wi-Fi and shared endpoint environment with shared nursing stations and common endpoints for doctors or other medical staff.

Cyberoam is a complete solution for HCOs with Integrated Security over single platform offering Identity-based approach with its patent pending Layer 8 Technology across all features. It offers a unified interface for achieving Unified Security Controls with reduced TCO (Total Cost of Operations) including best quality of security features, lower expenditure, ease of management, reduced cost of training and support. It offers future-ready security with IPv6 support and its ability to upgrade to future threats as security needs to grow.

Cyberoam is ICSA, Checkmark Level 5 and VPNC certified. HCOs must always remember that using Cyberoam effectively can assist them in meeting compliance, but just using Cyberoam or any other device alone, will not meet all the compliance needs. In addition to this while conducting the annual security and compliance reviews, examine where and how Cyberoam has helped increase the compliance posture of the organization, which will help you choose the right kind of solution needed for your unique requirements.

Conclusion

Cyberoam identity-enabled Next Generation NGFW appliances offer comprehensive network security, enabling healthcare institutions to protect patient records from both internal and external network attacks seamlessly. Easy to deploy and maintain, Cyberoam appliances provide visibility into network, security and user activities. Cyberoam’s Layer 8 Identity-based security helps track end user activities even in environments where multiple users share computers. It also helps healthcare institutions to meet the provisions of HIPAA compliance with ease. A good comprehensive approach towards security and compliance is inevitable for HCOs, hence relying on a single product or solution may not be the right choice, instead a holistic approach would be ideal.