Elemental

ELEMENTAL SECURITY PLATFORM

COMPLY with HIPAA and HITECH

Protecting Health Information (PHI)

To encourage the widespread use of electronic data interchange in healthcare, the U.S. Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II). HIPAA also requires the Department of Health and Human Services to establish national standards that address the security and privacy of health information. The Health Information Technology for Economic and Clinical Health Act (HITECH) was enacted in 2009 as part of the American Recovery and Reinvestment Act to promote the adoption of health information technology. HIPAA and HITECH were updated in 2013 when the Omnibus Rule was released. The challenge for IT departments lies in identifying the controls required to ensure the security and privacy of this data, and then proving to auditors that each control has been properly implemented, maintained, and monitored.

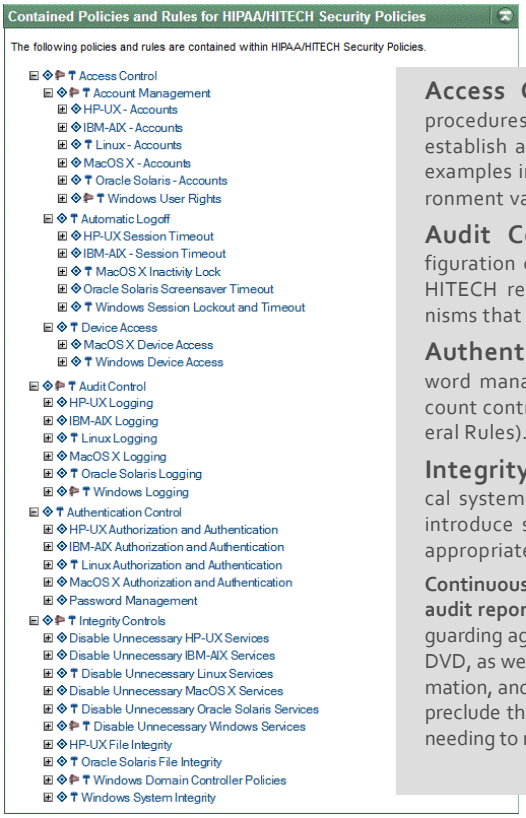
Elemental offers the most comprehensive integrated software platform to achieve, maintain, and control HIPAA/HITECH security compliance!

ESP deploys a robust HIPAA policy framework that is structured around HIPAA's Final Rule § 164.312 **Technical Safeguards**. Other ESP policy sets also address several requirements of the Rule § 164.308 **Administrative Safeguards**.

Elemental Cyber Security HIPAA/HITECH policy automation framework enables healthcare insurers and providers, universities, and other organizations that handle patient health information to adhere to HIPAA/HITECH best practices for network access control, host security configuration management, as well as systems and software inventory. Deploying a full range of policies in these categories enables organizations to effectively assess the security posture of the systems in a network that contain or use **protected health information (PHI)**.

The **Elemental Security Platform (ESP)** automates the arduous and often manual processes involved in making these assessments. In addition, it gives organizations the option of controlling access to these systems by placing network-based controls on those that process **electronic PHI (ePHI) data**, with access based on compliance with the organization's security policies. As a dedicated HIPAA/HITECH policy set incorporated into the ESP, the Elemental solution provides an automation framework for deploying and enforcing policies on computing resources that store and have access to ePHI. Using this approach, organizations can deploy security policies that address key aspects of the HIPAA standards for security:

Utilizing this policy set together with the advanced capabilities of the ESP, organizations can address HIPAA/HITECH requirements with **host-level security** that protects data where it resides, and with **policy-based access controls that dynamically adapt to changes** in the compliance or security posture of systems on the network.



Elemental HIPAA/HITECH Policy

Access Control – HIPAA/HITECH standards require organizations to implement technical policies and procedures that limit access to systems containing ePHI. The rules contained in Elemental's HIPAA policy establish a strong baseline for user identification and accountability across computer systems. Specific examples include policies to address automatic logoff, system account control, proper user account environment variables, and appropriate transitive trust control.

Audit Control – Elemental's audit control policies address the overall integrity and appropriate configuration of the platform logging subsystems. These policies are essential for complying with HIPAA / HITECH regulations requiring organizations to implement hardware, software and procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.

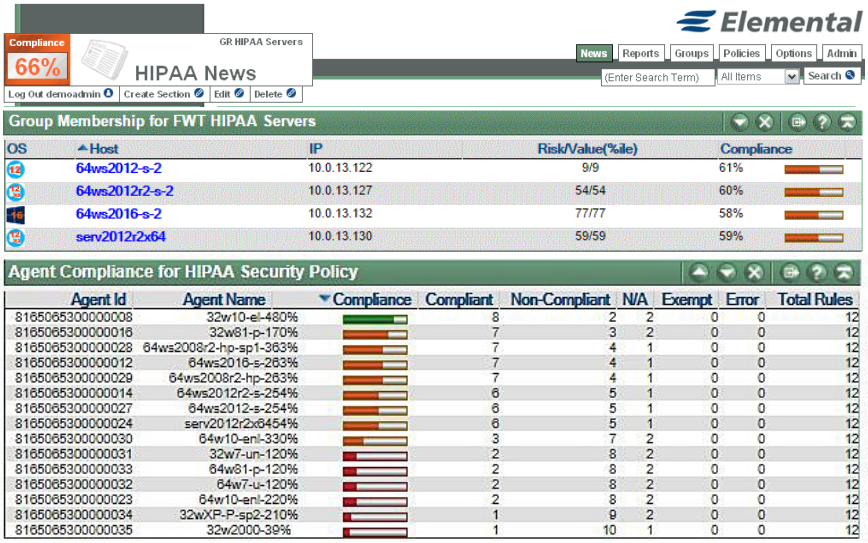
Authentication Control – The Elemental policy provides rules for complying with policies for password management and authentication integrity. These rules address aspects of authentication and account control required by HIPAA §164.312 (Technical Safeguards) and § 164.306 (Security Standards: General Rules).

Integrity Control – Elemental also addresses § 164.306 and § 164.312 requirements for securing critical system files and services. The ESP enables identification of unnecessary services — ones that may introduce security vulnerabilities with the potential to expose patient data. This policy also checks for appropriate system file permissions, reducing the chances of Trojan horse and denial of service attacks.

Continuous visibility into all the systems on a network further enables enforcement of these policies, as well as **audit reporting of status at any time**. Finally, the Elemental solution **protects private data at its point of use**, guarding against unauthorized use of removable and writeable media, such as USB flash memory sticks and CD/DVD, as well unauthorized printing of secured PHI documents. By combining this unprecedented visibility, automation, and broad range of policy-based capabilities, the Elemental solution enables organizations to effectively preclude the risks of failing to protect confidential patient health data. It also frees IT staff from the burden of needing to manually check and recheck systems to ensure they are in compliance with HIPAA best practices.

Maintain Compliance

The ESP enables organizations to **concisely report on their security and compliance objectives**. Executive level reports enable enterprise security and information officers to readily understand the overall security state of their information technology infrastructure, and to expose changes or trends in their compliance with HIPAA/HITECH regulations and controls. **Audit trails** provide compliance and policy management details tracking, and a clear understanding of security administrator entitlements and actions. Together this reporting framework enables organizations to demonstrate that required security controls are being implemented and maintained.



These views are supported by **detailed drill-down reporting** that provides an unparalleled level of transparency into the network environment. This enables operational staff to continuously monitor the security posture, inventory, compliance, and activity of machines on the networks. This enables **targeted investigation** of factors impacting compliance, and provides the ability to enact **appropriate remediation** to correct compliance drift as it occurs. The hierarchical and comprehensive reporting capabilities of ESP provide the alignment necessary between the technical controls required by HIPAA/HITECH and the business objectives of the organization. This alignment is supported by a **metrics-based framework** that enables clear demonstration of continued improvement, and is crucial in order to maximize the efficiency of security operations in protecting the interests of the organization.

The Bottom Line

Elemental provides a **comprehensive framework** for deploying and **enforcing policies** on computing systems that store confidential health data. Only the Elemental solution provides the **visibility** and **automation** necessary to continuously monitor and secure these systems in fast-changing enterprise environments, allowing organizations to effectively demonstrate and maintain compliance with HIPAA/HITECH best practices.

Elemental

www.ElementalSecurity.com