Somansa White Paper

Somansa Data Security and Regulatory Compliance for Healthcare

How Somansa can protect ePHI- electronic patient health information and meet the requirements for healthcare compliances, HIPAA and HITECH Act.

SOMANSA

CONTENTS

INTRODUCTION

Healthcare compliance is required by law throughout the United States which regulates billing and coding compliance for treatments, risk assessment, practice ethics, referral laws, and patient rights legislation. The proper billing for services rendered needs to be accurate to ensure that problems with the government do not arise. Proper documentation and itemization of charges for treatments and services are important to provide proof of service during an audit or adjustment by integrity contractors. The compliance of healthcare providers also prevents improper treatments, lawsuits and various problems which occur between patients and insurance claims.

Protection of the organization of healthcare providers can only be done by following the strict laws and regulations set for compliance. To prevent government examination and inquiries, healthcare organizations must analyze and correct all factors which could lead to such audits and adjustments. Proper compliance also leads to less conflicts with insurance claims and offers efficient processing for healthcare providers.

As patient medical records are in electronic format and being transferred via email, FTP, and other electronic mediums, healthcare organizations face a host of HIPAA Security Rule compliance and HITECH Act challenges, including securing Electronic Protected Health Information (EPHI)

Who is required to follow the HIPAA requirements?

- Healthcare providers
- Private sector health plans
- Government health plans

Personal Information must be protected by Healthcare Organizations.

- Social Security Numbers
- Medical ID Numbers
- Credit Card Numbers
- Drivers License Numbers
- Home Address and Telephone Numbers
- Diseases, Medical Record Numbers

Key questions for healthcare organizations that need to secure ePHI and meet requirements for HIPAA and HITECH.

- How do you know an ePHI breach occurred?
- How can an ePHI breach be prevented?
- In case of an audit, can you provide an audit trail for ePHI disclosure?

HIPAA Compliance

HIPAA is the Health Insurance Portability and Accountability Act passed in 1996. The law regulates a number of healthcare areas, including privacy of patient information and security of information systems used by healthcare organizations under U.S. jurisdiction. Individuals and organizations regulated by HIPAA include the following parties - all healthcare providers, health plans and healthcare clearing houses. Concerning digital communications, the HIPAA's most important requirement is that healthcare organizations must implement "appropriate administrative, technical and physical safeguards to protect the privacy of patient information"

Email and Electronic Communications

The requirement to protect the privacy of PHI extends to electronic transmission of PHI between two parties, such as an email message or file accessible to both parties. The law requires the individuals and organizations it regulates to assess the risks of using email and to take steps to reduce or eliminate risks that using email, both internally and externally, poses. Those risks include all unauthorized interception of messages in transmission and receipt of messages by unauthorized persons.

Penalties

HIPAA is the first federal law of U.S. to impose criminal penalties for improper use or disclosure of PHI. Criminal violations will be investigated and prosecuted by the United States Department of Justice and Federal Bureau of Investigation and can carry a fine up to 10 years in prison and $250,000 for violating the law with malice or for profit. HHS will investigate civil violations with penalties ranging up to $25,000 a year for any given type of violation.

HITECH Act

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) legislation created to stimulate the adoption of electronic health records (EHR) and supporting technology in the United States. President Obama signed HITECH into law on February 17, 2009 as part of the American Recovery and Reinvestment Act of 2009 (ARRA), an economic stimulus bill.

The HITECH act stipulates that, beginning in 2011, healthcare providers will be offered financial incentives for demonstrating meaningful use of electronic health records (EHR). Incentives will be offered until 2015, after which time penalties may be levied for failing to demonstrate such use. The Act also establishes grants for training centers for the personnel required to support a health IT infrastructure.

Other

California 1386.

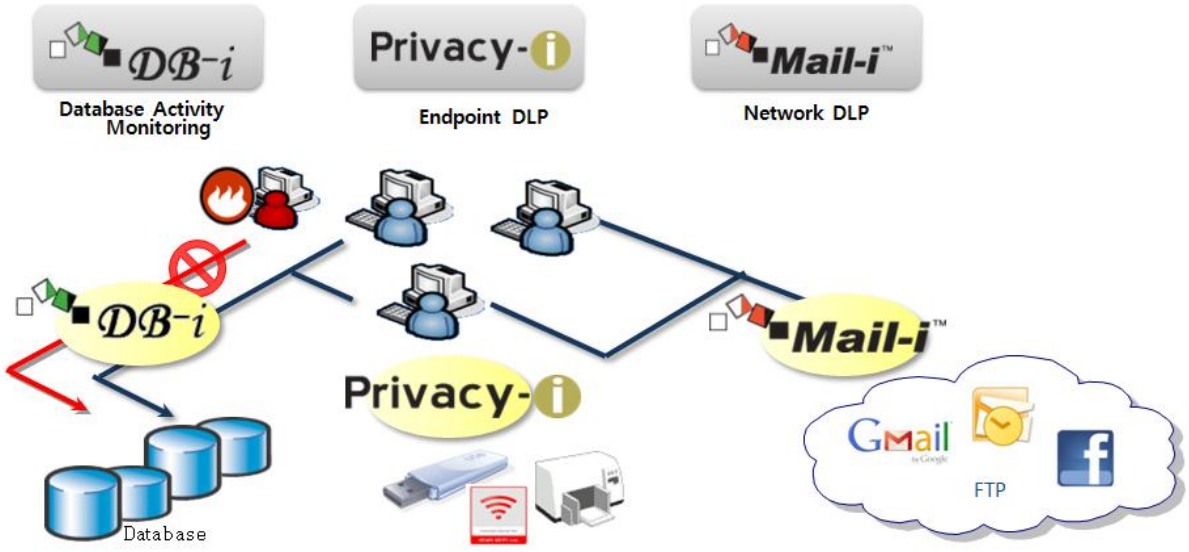
Effective July 2003, this regulation mandates public disclosure of computer security breaches in which confidential information of California residents may have been compromised.

Somansa Data Security and Compliance solutions to protect ePHI

As more corporate data and confidential information is being exchanged through the network via email, instant messenger, FTP, and stored/transferred to USB's and portable storage, the liabilities and amount of resources exhausted for healthcare institutions and providers have also increased. Confidential and sensitive information leakage, meeting compliance regulations, decreased work productivity, and legal lawsuits related to email can all lead to financial and resource loss for organizations.

Somansa is an affordable data security solution designed for organizations to meet regulatory compliance in the healthcare industry such as HIPAA and HITECH while protecting sensitive company data. Somansa provides healthcare organizations with a complete data security solution that includes network and endpoint DLP features to Monitor, Protect, and Discover confidential and customer data.

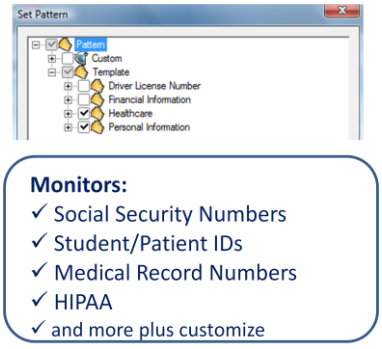
HOW IT WORKS



Somansa Monitors, Discovers, and Prevents sensitive data in the company network

POLICY SETTINGS

Based on defined policies, Somansa DLP monitors and detects sensitive healthcare and patient data in motion (Network) or at rest (Endpoint). Policies can be defined according to Sender/Receiver, IP Address, Protocols, Keywords- Patterns related to specific industries or Compliances including:

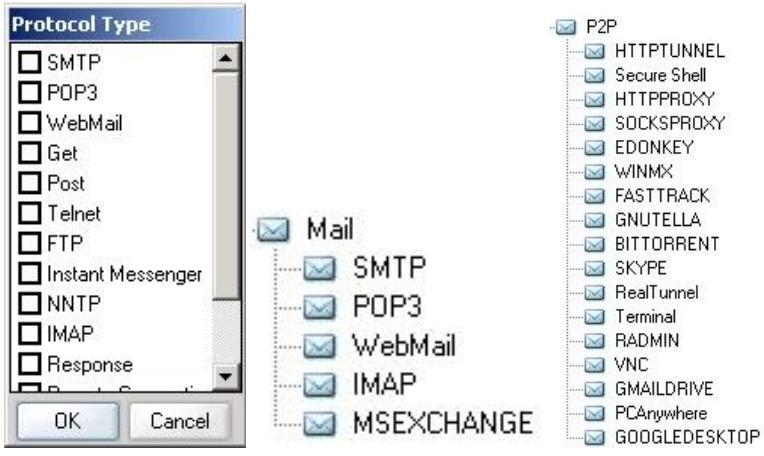


- Social Security Numbers
- Credit Card Numbers
- Medical Record Numbers
- ABA Bank Routing Numbers

Monitor and Prevent Data Leakage through Network Protocols, Email, Webmail, FTP, Network Share and Removable Storage, USB, iPods, and Printing.

Discover on endpoints by scanning and locating confidential data on desktops and laptops based on pre-defined and customizable detection methods and polices.

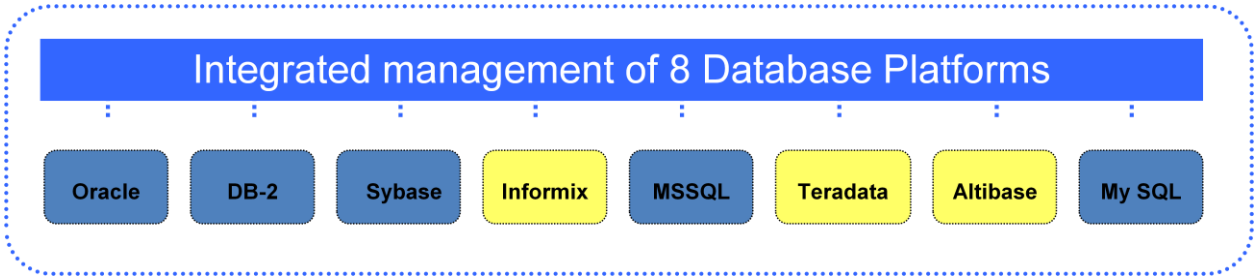
PROTOCOLS



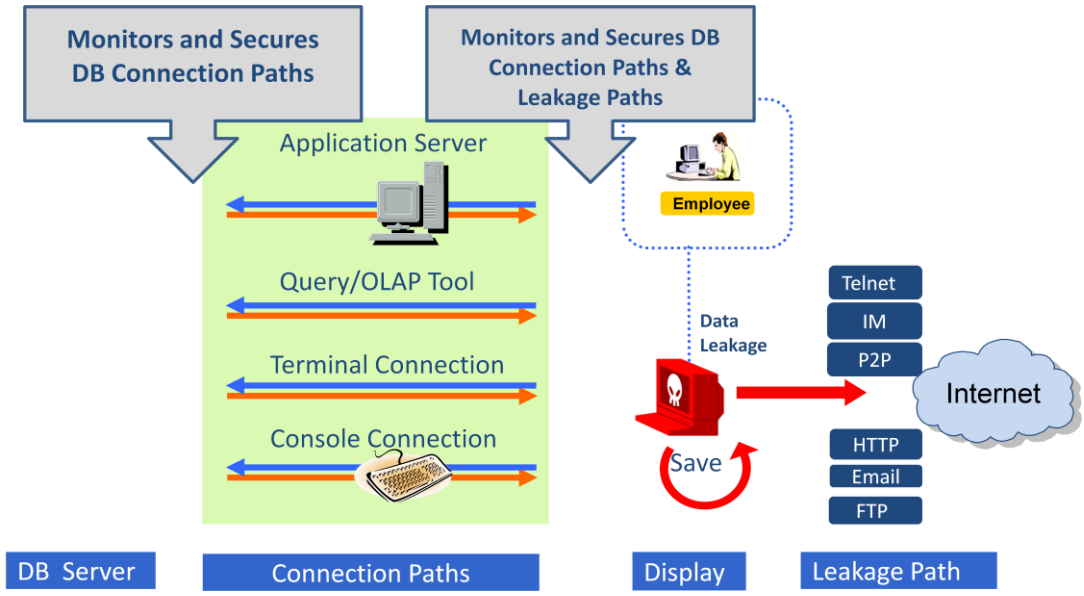
Somansa supports more messaging protocols than any other product

SOMANSA

DATABASE AUDIT & PROTECTION (DAP)

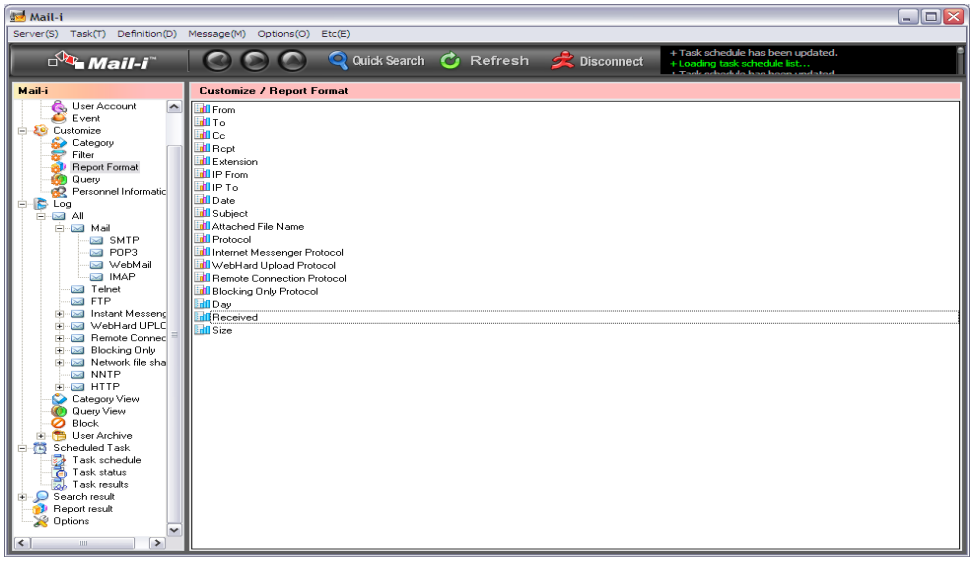


- **Central Management:** Supports various database platforms.
  Uses Mirroring, In-line, Proxy methods to monitor data.
- **Monitors and Records:** Monitors data from all access points to the database, including Console Access, AP Server, and Query Tool.
- **Security:** Access and Change Control by ID and Password validation, Policies settings, User Audit, and Real-time Alerts.
  - Plus, Data Masking



SOMANSA

REPORTING



Somansa provides status user/event reports as well as audit trails

About Somansa

Somansa is a global leader in Data Security and Compliance solutions designed to protect valuable company information from leakage and help meet regulatory compliance requirements.

Using its advanced packet and protocol analysis technology, Somansa provides a total security solution to Monitor, Protect, and Discover sensitive company data in motion and at rest including network protocols, email, IM, FTP, endpoints such as USB and database activity to meet regulatory compliance requirements while protecting valuable company information.

www.somansatech.com

For more information please contact:

Tel: (408) 701-1302

Email: info@somansatech.com

SOMANSA