# PHYSICAL AND IT SECURITY CONVERGENCE

Beyond Compliance - Managing Risk for the Healthcare Enterprise

Delivering quality healthcare is a combined effort requiring close cooperation between provider networks, hospitals, medical specialties as well as lab and testing services. Add to this the dimension of prescription management, pharmaceutical supply chain and retail pharmacy. The claims and delivery management systems for health insurance carriers, HMOs and PMOs all need access to medical records.

Patient information must flow seamlessly across all delivery organizations and health insurers. Regulations like HIPAA and industry best practice frameworks like HITRUST require that primary healthcare providers not only vigorously protect patient privacy, but also take responsibility for enforcing the same standards of Security and Safety due diligence for their partner providers.

REGULATIONS AND STANDARDS

- *HIPAA*
- *Sarbanes-Oxley*
- *NIST SP800-xx*
- *ISO 27001/ 27002*
- *HITRUST*
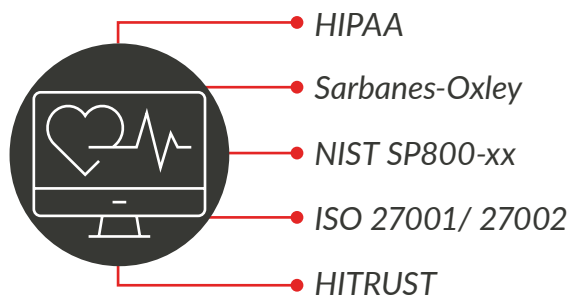
ALERTENTERPRISE SOLUTIONS

G ENTERPRISE GUARDIAN

S ENTERPRISE SENTRY

I IDENTITY INTELLIGENCE TECHNOLOGY

V ENTERPRISE VISITOR IDENTITY MANAGEMENT

FEATURES

- Real-time validation of certification and credentials during access provisioning
- Manage deprovisioning process and cross-linkage of access termination from multiple systems simultaneously – physical, logical and operational
- Identify compliance gaps in real-time and suggest remedial actions to remain in compliance with HIPAA, Sarbanes-Oxley, NIST SP800-xx, PCI and ISO-2700x standards
- Identification of risks based on validating employee and contractor access to critical applications and healthcare facilities
- Enforcement of security policies and procedures across vendor and partner ecosystems following HITRUST provisions
- Visual risk and remediation modeling with ability to display key assets on geo-spatial maps with drill-down details on event and asset criticality; ability to integrate physical security alerts and surveillance video

POTENTIAL COSTS FOR VIOLATIONS AND NON-COMPLIANCE CAN BE EXTRAORDINARY

COMPLIANCE & AUDITING

PCI REQUIREMENTS

$7,500

The amount the organization could be expected to pay in the event a compliance findings is identified related to Personal Credit information compliance.

COMPLIANCE & AUDITING

HIPPA VIOLATION

$1.5M

The amount the organization could be expected to pay per year per finding related to HIPPA compliance violations.

COMPLIANCE & AUDITING

SARBANES-OXLEY ACT

$5M

The amount the organization could be expected to pay in the event of a SOX compliance violation.

DATA BREACH - GENERAL

$7.35M

The average cost of a data breach of PCI, PHI, PII, etc. data due to malicious or criminal cyber / insider attacks, system or human errors.

–Ponemon Institute Research, 2017

INSIDER THREAT

$8.78M

The average total cost of insider threat and careless or negligent employees and contractors are the root cause of most incidents.

–Ponemon Institute Research, 2018

COMPLIANCE & AUDITING

LOSS OF BUSINESS / CONTRACT

$10M+

While the total cost is unknown, depending upon the type of breach or violation, a healthcare enterprise could be at risk of losing existing business and new business should its reputation related to protecting data be damaged.

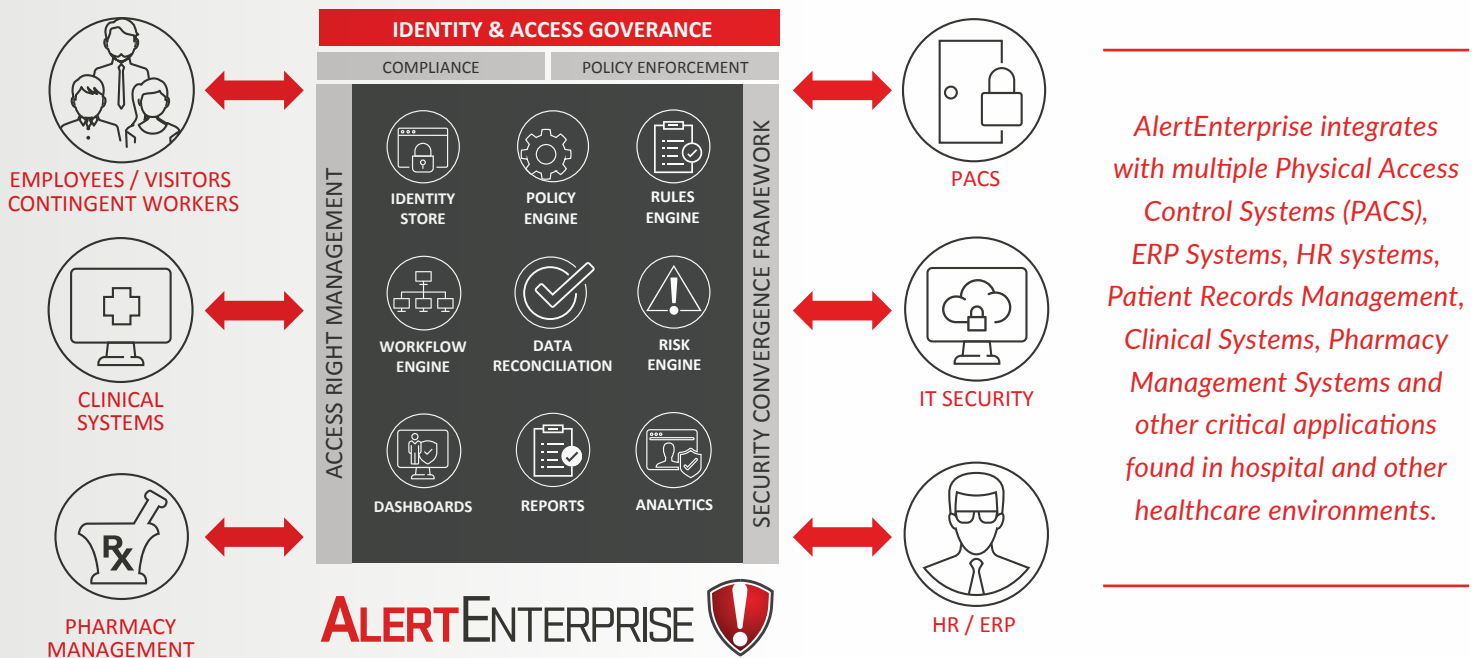Fines and violation figures are approximations and may vary.

ACTIVE POLICY ENFORCEMENT FOR IT AND BUILDING ACCESS

Hundreds of access points, thousands of employees and scores of service provider organizations make up the extended healthcare enterprise. Determining risk to this broad enterprise involves managing roles and critical access for each. Do employees or contractors have the right training and certification to access personal health information? Safeguarding confidential personal health and financial information also means monitoring who has physical access to the records. Did the badge access and system access for terminated employees get turned off at the right time?

AlertEnterprise software delivers real-time integration of Identity Access Governance with Physical Access Control and Human Resource applications. The converged security approach automates policy enforcement and compliance, helping you automatically validate employee background checks, training and certification, authorization to view patient information and other vendor services.

THE INTEGRATED ALERTENTERPRISE SOLUTION

EMPLOYEES / VISITORS CONTINGENT WORKERS

CLINICAL SYSTEMS

PHARMACY MANAGEMENT

IDENTITY & ACCESS GOVERANCE

COMPLIANCE | POLICY ENFORCEMENT

ACCESS RIGHT MANAGEMENT

IDENTITY STORE

POLICY ENGINE

RULES ENGINE

WORKFLOW ENGINE

DATA RECONCILIATION

RISK ENGINE

DASHBOARDS

REPORTS

ANALYTICS

SECURITY CONVERGENCE FRAMEWORK

ALERTENTERPRISE

PACS

IT SECURITY

HR / ERP

AlertEnterprise integrates with multiple Physical Access Control Systems (PACS), ERP Systems, HR systems, Patient Records Management, Clinical Systems, Pharmacy Management Systems and other critical applications found in hospital and other healthcare environments.

YOU'VE IDENTIFIED THE RISK. NOW WHAT? ALERTENTERPRISE DELIVERS THE NEXT STEPS

Identifying the risks alone is not enough. Organizations need to make sure that immediate steps are being taken to mitigate risks. AlertEnterprise automates remediation and helps you to analyze risks, and visualize remediation paths before taking action. Business analysts, IT security and physical security teams can collaborate visually and implement the next steps – which may include reviewing correlated risk recommendations for selected employees and removing physical access to certain parts of the facility or system access to certain applications that contain sensitive data.

UNIQUE CUSTOMER BENEFITS

IMPROVE COMPLIANCE & ENFORCE POLICIES

- Training, PRA compliance
- Certification requirements
- Healthcare Content Packs: SOX, GDPR, HIPAA, HITRUST, Health Level 7 (HL7) Integration
- Full audits controls and chain of custody
- Access review and recertification
- Immediate badge deactivation and access removal for offboarding, termination and expired training/certification
- Access rights and approvals to secure areas
- Visitor screening and approvals

REDUCE COSTS OF BREACH, RISK & DAMAGES

- Risk-based security controls
- Unique identity / reconciliation of IT and Physical Security
- Segregation of duties
  - Privilege users
  - Secondary approvals
- Segregation of data
  - Privacy / Encryption
  - Secondary approvals
- Eliminate access creep
- Eliminate orphan accounts

STREAMLINE SECURITY ADMINISTRATION & SUPPORT COSTS

- Automate manual data entry
- Automate manual paper process
  - HR driven
  - Access requests
- Eliminate duplicates, errors
- Streamline badge operation
- Improve security investigation
- Automate manual audit, reports
- Leverage existing investments
- Partner Channel Access Management with Self-Service Portal

NEW COVID-19 HEALTH & SAFETY ACCESS GOVERNANCE AND INTELLIGENCE MODULES

As attention turns to restarting and recovering the global economy, AlertEnterprise is helping organizations put technology to work to defend their workforces from the COVID-19 contagion. The new Health & Safety Access Governance and Intelligence modules helps you return to work with confidence, automating and proactively enforcing policies and plans for re-entry, workspace physical distancing and infection response.

LEARN MORE: HTTPS://ALERTENTERPRISE.COM/COVID-19/

ALERTENTERPRISE

INFO@ALERTENTERPRISE.COM
ALERTENTERPRISE.COM