HIPAA COMPLIANCE AND RES

RES can address compliance issues across the broad range of HIPAA requirements.

The HIPAA Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of protected health information (PHI).

The Security Rule is made up of three parts.

1. Technical Safeguards
2. Physical Safeguards
3. Administrative Safeguards

IT related issues typically fall under the technical category, so we will focus on how RES helps hospitals achieve technical compliance.

TECHNICAL SAFEGUARDS

The Technical Safeguards focus on the technology that protects PHI and controls access to it. The standards of the Security Rule do not require you to use specific technologies. The Security standards are designed to be "technology neutral."

There are five standards listed under the Technical Safeguards section.

1. Access Control
2. Audit Controls
3. Integrity
4. Authentication
5. Transmission Security

When you break down the five standards, there are nine capabilities that IT organizations need to implement. RES can address challenges across all nine requirements, helping IT meet the needed safeguards while enabling clinicians to focus on the quality of patient care.

HIPAA TECHNOLOGY REQUIREMENTS	RES CAPABILITIES AND SOLUTIONS
Access Control	
Unique User Identification: *Assign a unique name and/or number for identifying and tracking user identity.*	**Automated Provisioning and Deprovisioning** — Utilizing the automated onboarding functionality RES facilitates unique user account creation in a variety of EMR platforms as well as other relevant apps and services within the clinician workspace. Additionally, the offboarding features enable instant removal when access is no longer needed or relevant based on the clinician context. **Compliant Logins** — Many organizations have historically used anonymous logins to access Active Directory and then a unique ID for the EMR system. RES facilitates rapid creation and integration of unique Active Directory accounts to bring the organization into compliance. **Self-Service for Pre-Access Training** — Many organizations require employees to complete training or sign a policy prior to receiving access to an EMR system. RES will facilitate the organization in allowing users self-service access to this training or policy signoff and then automatically provision their account when the training is completed or policy is signed.

Continued on the back

Emergency Access Procedure: *Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.*	**Exception Access** — RES will enable organizations to allow employees to request emergency access to an EMR platform. This can be configured to make the employee enter a justification and will automatically remove the access after a specified period of time. All of these automated actions are auditable and reportable to cover any audits with ease.
Automatic Logoff: *Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.*	**Access Time Out** — RES enables organizations to quickly create and deploy a policy to log users off of a system after a pre-determined time. This policy can also be context aware. For instance, if a doctor is accessing the system from a patient exam room during a general practice appointment, the logoff can be set to two minutes. If that same doctor is performing surgery and needs to see the records on a large display throughout the procedure, the logoff can be set to indefinite in the OR.
Encryption and Decryption: *Implement a mechanism to encrypt and decrypt ePHI.*	**Encrypted Disk Policy** — RES facilitates simple creation of policies that can force any ePHI to be saved to an encrypted disk. **Encrypted Disk Migration** — RES facilitates the simple creation of an automated runbook that will move any unsecured data to an encrypted storage component.
Audit Controls	
Audit Controls: *Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems containing or using ePHI.*	**Audit Tracking** — By utilizing RES for account creation and termination, all functions will be automated, consistent and auditable. All of these actions can be easily exported in a report to answer any audit inquiries related to account access, rights, application usage and account termination.
Integrity	
Integrity: *Mechanism to Authenticate ePHI (addressable): Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.*	**Automated Processes** — By Utilizing RES ONE Enterprise to automate access, account creation and share permissions, the integrity of each resource is further enhanced as all accounts are created and terminated in a consistent manner every time.
Authentication	
Authentication: *Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.*	**People-Centric Policy Controls** — Utilizing RES, simple policies can be created to limit access to specific users or devices. For instance, if an assistant logs into a doctor's laptop, the EMR client installed on that laptop will not launch. When the doctor logs back in, then it will function as normal.
Transmission Security	
Integrity Controls: *Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.*	**Email Policy Controls** — There are many requirements here that RES can facilitate. One example is the requirement for encrypted or digital signing of email. Through a simple policy creation, the users can be forced to utilize encrypted email or digital signatures. **Signature Controls** — The digital signatures required to reside on the end point device can be roamed from device to device using RES ONE Workspace.
Encryption: *Implement a mechanism to encrypt ePHI whenever deemed appropriate.*	**Context Aware Security** — RES has the ability to easily create context aware policies that will limit access from devices or locations that are not appropriate or secure to access ePHI. For example, a doctor may be able to access a full range of data while using his laptop in his office, yet when he takes that same laptop to Starbucks, he is not able to access the same data.

ABOUT RES

RES creates, automates and secures digital workspaces to improve the experience and productivity of the workforce while lowering IT costs. RES takes a people-centric approach to making technology access secure, even in complex multi-device/multi-location scenarios, across physical, virtual and cloud environments. RES boasts numerous patented technologies, fast time to value, and superior customer support for more than 2,500 companies around the world. For more information, visit www.res.com, contact your preferred RES partner, or follow updates on Twitter @ressoftware.

RES®