Document name: HIPAA Security Rule
Document #:
Date: 6.2021

CompuMed and the HIPAA Security Rule

This document details how CompuMed's Portal support the HIPAA Security Rule. The table below lists the Security Rule along with the relevant paragraph and discusses the features within the CompuMed Portal that can be implemented by the institution to assist in meeting the rule.
R = Required, A = Addressable

Rule	Paragraph	R/A	CompuMed Portal
General Requirements:			
Ensure integrity, confidentiality, and availability	164.306 (a) 1		**Integrity** of the data is maintained by many checks and balances that are built into the system upon receipt of the exam information. Examples include checking that the Patient and Exam ID's are unique. **Confidentiality** of the data is maintained at several levels. First, the user must have an ID and a password. Second, one the user log onto the system, they may just get a list of patients for whom they have viewing authority, as established from the organization. The system is also well protected from hackers through combination of turning off all ports not required for our application and keeping the system up to date with security patches. **Availability** The recommends CompuMed Portal runs on a highly available cluster hosted in Microsoft Azure
Protect against hazards / threats to security and integrity of data	164.306 (a) 2		There are several types of users on the system with different levels of access to the data. First, all users have a password and ID. Next, only users with system administrator's privileges can alter the data in any way. The system is also protected from access from the outside as discussed in 164.306 (a) 1. In addition to these security measures, CompuMed does support https for access to the data and the use Of VPNs that utilize IPSec and can be set-up with soft clients and keys.
Protect against uses or disclosures of information not allowed	164.306 (a) 3		In addition to the ID and password required to access the CompuMed Portal tools may limit a given user's access to just a subset of patients. The CompuMed Portal logs all access to data, providing a list of who accessed a given patient's exam by date and time.

Administrative Safeguards:			
Policies to Protect, detect, contain and correct security violations	164.308(a)1i		The CompuMed Portal and Microsoft Azure assist in this function by utilizing tools that look for unauthorized accesses and also through management of the operating system and other system software. This includes tracking available security issues and applying fixes.
Procedures to review records of system activity, system logs, security	164.308(a)1iiD	R	The operating system supports the function to track unauthorized attempts at access. Microsoft Azure provides tools, monitoring, and system protections against unauthorized access.
Implement access to electronic information	164.308(a)3iiA	A	The CompuMed Portal allows access through user ID and password or single sign-on. These must be assigned by the system administrator.
Procedures to ensure access is appropriate	164.308(a)3iiB	A	The CompuMed portal can limit access to a patient's record to only those users who 1) are listed as a physician on the order; 2) are members of a group with shared access; 3) are members of a different access group set up in The CompuMed Portal, or 4) given access by the system administrator.
Termination Procedures	164.308(a)3iiC	A	User access can readily be removed from the CompuMed portal. The user can be removed from the system; users can be removed from access groups and users can initially only be given access for a limited amount of time.
Policies and procedures for granting access	164.308(a)4iiB	A	The CompuMed portal have the tools for setting up user IDs and passwords and limiting access based on a wide variety of criteria, such as physician group affiliation, patient location and modality type, as required.
Policies and procedures for establishing, document, reviewing rights to access	164.308(a)4iiC	A	The CompuMed portal has extensive tools for implementing restricted access for viewing the images and reports.

Security Awareness and Training – Procedures for guarding against, detecting and reporting malicious software	164.308(a) 5ii (B)	A	The CompuMed Portal is hosted in a sand boxed environment through Microsoft Azure. Access is restricted and monitored.
Security Awareness and Training – Login Monitoring	164.308(a) 5ii (C)	A	All failed attempts are logged. After 5 attempts, the user ID is temporarily locked out.
Security Awareness and Training – Password Management – procedures for creating, changing and safeguarding passwords.	164.308(a)	A	Passwords are securely hashed and encrypted in the CompuMed portal. The passwords must be at least 8 characters in length, or a user may use an integrated Single Sign-on provider from Microsoft, Google, or Okta, determined by their organization setup.
Contingency Plan – Policies and Procedures for Responding to an emergency that damages systems that contain electronic PHI	164.308(a) 7(1)		
Backup Plan – Procedures to create and maintain exact copies of electronic PHI	164.308(a) 7(ii)(A)	R	The CompuMed Portal has extensive tools for backing up the exact data that was sent to them from the modalities. CompuMed implements Azure blob storage redundant technology for building a redundant system in real-time. Databases are incrementally backed up and allow point in time recovery. Applications can be scaled up, out, or redeployed in Microsoft Azure.

Disaster Recovery Plan	164.308(a) 7(ii)(B)	R	The CompuMed Portal has extensive tools for restoring the backup copy of the data. Systems are designed to meet customer requirements for the length of time to have a fully functional system, up to providing fully redundant systems available in near real-time.
Emergency mode operation and Testing and revision procedures	164.308(a) 7(ii)(C)(D)	R / A	CompuMed considers this part of the overall Disaster Recovery Plan and will work with the customer to document procedures and practice for emergencies.
Evaluation – period evaluation based on environmental or operational changes and how they effect the security plan	164.308(a) 8		CompuMed's role is to support the customer in these areas and provide recommended changes based on customer changes. CompuMed also continues to monitor the regulations for changes and required actions.
Business associate contracts and other arrangements	164.308(a) 8(b) (1) – (4)	R	CompuMed often requires access to PHI for support of the system and often signs Business Associate Contracts.
Physical Safeguards – Facility Access and Control	16.310(a)		
Contingency Operations	16.310 (a)(1)	A	CompuMed has plans to support customers and our site in case of emergencies. The server operations are managed through Microsoft Azure.
Facility Security Plan		A	The CompuMed portal is hosted in a secure distributed cluster of data centers through Microsoft Azure.
Access Control and Validation Procedures		A	Physical access is managed through Microsoft Azure.
Maintenance Records		A	Maintenance records are managed through Microsoft azure.

Workstation Use – policies that address functions and environment	16.310 (b)	R	Workstation access is managed by the customer.
Workstation Security – physical safeguards	16.310 (c)	R	This is mainly customer driven
Device and Media Controls	16.310 (d)	A	Data backup and storage are handled in Microsoft Azure. Microsoft is responsible for physical media. All information stored is encrypted.
Technical Safeguards –	16.312		
Access Control - policies and procedures to restrict access	16.312(a)(1)		The CompuMed Portal has extensive tools for restricting access to patient files by information received in the order, in the study, by group affiliation or through system manager granted authority. All accesses are tracked.
User ID	16.312(a)(1)	R	Using The CompuMed Portal, all users must have an ID. All accesses are tracked by user and reports are readily generated and printed.
Emergency Access Procedure	16.312(a)(1)	R	This is part of the Disaster Recovery and Business Continuity Plan. Also CompuMed Portal allows the system manager to grant access to any user for any patient. The system can allow users with privileges to a patient's file to grant these privileges to other users.
Automatic Logoff	16.312(a)(1)	A	The CompuMed Portal automatically logs the user off after 4 hours of inactivity. This can be configured by the system administrator.
Encryption and Decryption	16.312(a)(1)	A	All information received, stored, and sent through the CompuMed Portal is encrypted at transit through TLS encryption, and at rest using AES or equivalent level encryption and decryption at the server or file level.
Audit Controls	16.312(b)	R	The CompuMed Portal records all user access to ePHI.

Integrity – mechanism to authenticate ePHI	16.312(c)(1)	A	The CompuMed Portal protects against unauthorized access by maintaining a secure environment. Security is assessed at the end point through third party auditing and application penetration testing.
Person or Entity Authentication	16.312(d)	R	The CompuMed Portal uses ID and passwords to authenticate the user, or through Single Sign-on.
Transmission Security - technical measures to guard against unauthorized access over electronic communication networks.	16.312(e)1		
Integrity Controls	16.312(e)1	A	Only users with proper authority can modify the data and all changes to data are logged.
Encryption	16.312(e)1	A	Over the Internet, CompuMed implements https, as a minimum. CompuMed can also implement IPSec through the use of VPN devices. CompuMed will also work with the customer to implement their standard security.