HIPAA Security Rule 45 C.F.R. §§, 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(d)

*Administrative Safeguard - Security Management Process (Risk Management functions)*
– physical devices and systems within the organization are inventoried.

TechR2®'s support these safeguard requirements through the inventorying of data center assets which are required for these functions. Data Centers typically are the central repository of electronic medical record databases and provide access to large quantities of protected health information.

HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(B), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii)

*Administrative Safeguard – Security Management Process (Risk Management functions)*
*Physical Safeguard – Facility Access Controls*
*Physical Safeguard – Device and Media Controls*
- Physical access to assets is managed and protected

TechR2® supports these functions through the inventory management and tracking services capabilities. Ensuring that inventoried equipment does not leave the designated location in an unauthorized manner. This in turn supports Risk Management requirements by providing assurance to leadership that large amounts of PHI are not being removed from designated locations. Additionally, it addresses the requirement for the proper disposal of electronic PHI as well as establishes accountability for hardware and electronic media.

HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1), 164.310(d)(2)

*Administrative Safeguard – Security Management Process (Risk Management functions)*
*Physical Safeguard – Facility Access Controls*
*Physical Safeguard – Device and Media Controls*
*NIST SP 800-53 MP-6*
- Assets are formally managed throughout removal, transfers, and disposition

TechR2®'s service does this and ensure proper policies, procedures, and processes are in place to provide accountability for the disposal of electronic PHI.

HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)

- Policy and regulations regarding the physical operating environment for organizational assets are met

TechR2®'s takes the burden of managing the associated documentation required to demonstrate the proper disposal of electronic PHI.

HIPAA Security Rule 45 C.F.R. §§ 164.310(d)(2)(i), 164.310(d)(2)(ii)

- Data is destroyed according to policy

TechR2®'s services address this requirement by maintaining training requirements and ability to evidence adherence to processes and procedures.