PHYSICAL SAFEGUARDS					
Section	**Standard**	**Implementation Specification**	**Required/ Addressable**	**CA's Solution**	**Methodology**
164.310(a)(1)	**Facility Access Controls**	Contingency Operations	Addressable	Internal Policies and Physical Access Control	Covered entities must establish (and implement as needed) procedures that allow facility access to support the restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
		Facility Security Plan	Addressable	Internal Policies and Physical Security	Covered entities must implement policies and procedures to safeguard the facility and equipment from unauthorized physical access, tampering or theft.
		Access Control and Validation Procedures	Addressable	*e* Trust™ Access Control and Physical Security	Covered entities must implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. Covered entities can protect access to critical workstations and servers by utilizing an effective physical access control method. Supplementing this with *e* Trust™ Access Control protects critical systems and information from unauthorized users who are allowed access to physical devices.
		Maintenance Records	Addressable	Internal Policies	Covered entities must implement policies and procedures to document repairs and modifications to physical structures, where these changes are meant to enhance security.
164.310(b)	**Workstation Use**		Required	*e* Trust™ Single Sign-On	Covered entities must implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. Using *e* Trust™ Single Sign-On, covered entities can effectively lock-down a workstation — requiring all users of that workstation to go through single sign-on. Based on their role, the users would then be able to access and/or use only those functions for which they are authorized.
164.310(c)	**Workstation Security**		Required	Internal Policies and Physical Security	Covered entities must implement physical security safeguards to restrict access to workstations that access electronic protected health information to authorized users only.
164.310(d)(1)	**Device and Media Controls**	Disposal	Required	Internal Policies	Covered entities must implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information (electronic PHI) into, within and out of the facility.

PHYSICAL SAFEGUARDS					
Section	**Standard**	**Implementation Specification**	**Required/ Addressable**	**CA's Solution**	**Methodology**
		Media Re-use	Required	Internal Policies	Covered entities must implement policies and procedures designed to eliminate electronic PHI from all media, before that media is made available for re-use.
		Accountability	Addressable	Unicenter® Asset Management, Unicenter® Argis Portfolio Asset Management	Covered entities must maintain a record of the movements of hardware and electronic media and any person responsible therefore. Through the use of Unicenter® Asset Management and Unicenter® Argis Portfolio Asset Management, covered entities can log all resources — IT and non-IT — that contain electronic PHI. In addition, they can track the location, movement and depreciation related to the contracts and responsibilities of that information.
		Data Backup and Storage	Addressable	BrightStor® Portal, BrightStor® Storage Resource Manager, BrightStor® Enterprise Backup, BrightStor® ArcServe Backup	Covered entities must create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment. Using products from the BrightStor® family of storage solutions, covered entities can meet this requirement.