

TECHNICAL SAFEGUARDS

Section	Standard	Implementation Specification	Required/ Addressable	CA's Solution	Methodology
164.312(a)(1)	Access Control	Unique User Identification	Required	eTrust™ Single Sign-On	Covered entities must assign a unique name and/ or number for identifying and tracking user identity. With eTrust™ Single Sign-On and its toolbar designed for shared workstations, covered entities can create convenient, yet secure access to clinical workstations. This significantly improves the likelihood that users will follow the established security policies and will stop sharing passwords.
		Emergency Access Procedures	Required	Internal Policies	Covered entities must establish (and implement as needed) procedures for obtaining necessary electronic protected health information (electronic PHI) during an emergency.
		Automatic Logoff	Addressable	eTrust™ Single Sign-On	Covered entities must implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. The station lock functionality of eTrust™ Single Sign-On allows covered entities to protect application sessions while a user is away from his/her workstation, without forcing the user or session to logoff. The user is then able to return to that session, in its original state, without having lost unsaved information. This allows an extended automatic log-off time, which improves convenience to the users.
		Encryption and Decryption	Addressable	eTrust™ PKI	Covered entities must implement a mechanism to encrypt and decrypt electronic protected health information. eTrust™ PKI allows covered entities to encrypt and decrypt information with public and private keys as it is sent over a public or private network.
164.312(b)	Audit Controls		Required	eTrust™ Single Sign-On, eTrust™ Audit, eTrust™ Security Command Center, eTrust™ Access Control	Covered entities must implement hardware, software, and/or procedural mechanisms to record and examine activity in information systems that contain or use electronic protected health information. To address this requirement, covered entities must enable the audit logging functions of their operating systems, databases, and applications. In many cases, they will also need to upgrade their applications to versions with logging capabilities. While this is taking place, covered entities can use the logging capabilities of eTrust™ Single Sign-On to determine who launched what applications from what locations at what time. eTrust™ Access Control enhances the logging capability of distributed operating systems in order to log information access and modification by root, or other super, users. The addition of these logging requirements creates a difficult, time-consuming and costly audit review process. Using eTrust™ Audit, or eTrust™ Security Command Center, event messages generated by system activities across an organization's various operating systems, databases, applications, and security

TECHNICAL SAFEGUARDS					
Section	Standard	Implementation Specification	Required/ Addressable	CA's Solution	Methodology
					devices can be collected, normalized and stored in a central repository. Database-driven querying, filtering and reporting can be carried out on demand, increasing operational cost savings while reducing the time required to perform a full enterprise auditing implementation. Centralized alerting can be automatically triggered upon detecting suspicious patterns of events, preventing potential damages to business-critical resources.
164.312(c)(1)	Integrity	Mechanism to Authenticate Data	Addressable	eTrust™ Access Control, eTrust™ Audit, eTrust™ Security Command Center	Covered entities must implement policies and procedures to protect electronic protected health information from improper alteration or destruction. eTrust™ Access Control allows covered entities to protect electronic PHI from improper alteration or destruction. eTrust™ Audit, or eTrust™ Security Command Center, add to this capability by providing a central location to enable historical reporting and analysis, helping to ensure that electronic PHI has not been improperly altered or destroyed. Additionally, alerts can be automatically triggered in near real time upon detection of suspicious activities, such as attempts to damage or illegally modify critical files.
164.312(d)	Person or Entity Authentication		Required	eTrust™ Single Sign-On	Covered entities must implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. Proper use of user IDs and passwords helps ensure that any user claiming access to a system is who he/she claims to be. However, in an environment where users are forced to remember multiple passwords, these passwords are often written down and proper use is not practiced. eTrust™ Single Sign-On reduces the number of passwords that the user needs to remember, improving the likelihood that the password policies will be followed. The addition of strong authentication, such as biometrics, significantly improves the likelihood that a person is who he/she claims to be when accessing systems.
164.312(e)(1)	Transmission Security	Integrity Controls	Addressable	eTrust™ PKI	Covered entities must implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. Using the public and private key encryption methodology of eTrust™ PKI, covered entities can guard against unauthorized access to electronic PHI that is being transmitted over electronic communications networks.
		Encryption	Addressable	eTrust™ PKI	Covered entities must implement a mechanism to encrypt electronic protected health information over open networks, and whenever deemed appropriate. eTrust™ PKI allows covered entities to encrypt electronic PHI, when appropriate, using both public and private keys.