

HIPAA Compliance Statement

Family Health Portrait by Estate++

Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	Required or Addressable
Access Control	164.312(a)(1)	Unique User Identification	Required
Rule Statement: Assign a unique name and/or number for identifying and tracking user identity.			
Solution: Use of unique usernames and passwords for all user accounts through RPX.			

Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	Required or Addressable
		Emergency Access Procedure	Required
Rule Statement: Establish (and implement as needed) procedures for obtaining necessary electronic protected health information (PHI) during an emergency.			
Solution: PHI can be accessed from any location via the Internet.			

Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	Required or Addressable
		Automatic Logoff	Addressable
Rule Statement: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.			
Solution: System automatically logs off all users after a predetermined amount of time. (15 minutes)			

Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	Required or Addressable
		Encryption and Decryption	Addressable
Rule Statement: Implement a mechanism to encrypt and decrypt electronic protected health information.			
Solution: All "in-flight" data is encrypted during transmission to and from servers using SSL. All "at-rest" data is encrypted before being saved.			

Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	Required or Addressable
Audit Controls	164.312(b)		Required
Rule Statement: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.			
Solution: A detailed audit trail of login information is recorded. This includes date, time, IP address, and available RPX information.			

Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	Required or Addressable
Integrity	164.312(c)(1)	Mechanism to Authenticate EPHI	Addressable
Rule Statement: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.			
Solution: To prevent unauthorized alteration or destruction of PHI, SSL is used while data is "in-flight", encryption is used when data is "at-rest". A digital signature is taken of XML and data file before being stored. The digital signature is verified before data is downloaded to the user's computer. If the digital signature cannot be verified, data will not be downloaded to the user's computer. PLEASE NOTE: PHI cannot be controlled once it has reached the intended recipient Each user must is responsible for alteration or destruction of data once received.			

Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	Required or Addressable
Person or Entity Authentication	164.312(d)		Required
Rule Statement:	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.		
Solution:	Username and Password are used for access control through RPX. We maintain a "For Your Eyes Only" privacy policy which strictly forbids viewing, moving, uploading, downloading, adding, updating, or deleting any user information without explicit permission of the user (unless there are extenuating legal circumstances). Encryption of data "in-flight" and "at-rest" ensures that only the intended recipient(s) of information can ever access it.		

Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	Required or Addressable
Transmission Security	164.312(e)(1)	Integrity Controls	Addressable
Rule Statement:	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.		
Solution:	SSL-based encryption is used while data is "in-flight" during the transmission of data to/from users. A digital signature is taken of XML and data file before being stored. The digital signature is verified before data is downloaded to the user's computer. If the digital signature cannot be verified, data will not be downloaded to the user's computer.		

Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	Required or Addressable
		Encryption	Addressable
Rule Statement:	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.		
Solution:	SSL-based encryption is used while data is "in-flight" during the transmission of data to/from users. AES encryption is used to encrypt data "at-rest".		

Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	Required or Addressable
Device and Media Controls	164.310(d)	Data Backup and Storage	Required
Rule Statement:	Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.		
Solution:	The live database is backed up weekly. PHI information is stored in Amazon S3, which is both redundant and distributed. This means that multiple copies of data files (redundant) are stored in geographically separate locations (distributed). If a file is lost or destroyed in one location, it is immediately available from another location.		

Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	Required or Addressable
Data Disposal			Required
Rule Statement:	Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.		
Solution:	Users can delete their data whenever desired. We maintain a "For Your Eyes Only" privacy policy which strictly forbids viewing, moving, uploading, downloading, adding, updating, or deleting any user information without explicit permission of the user (unless there are extenuating legal circumstances).		