HIPAA: Standard 164

Electronic Records, Electronic Documents, Digital Signatures White Paper

SoluSoft N2 Workflow and Document Management System Compliance with HIPAA: Standard 164

HIPAA stands for the Health Insurance Portability and Accountability Act of 1996. HIPAA is a federal law that requires companies to adopt administrative, physical and technical measures to protect the security, privacy, integrity and availability of every individuals' health information. Strict auditing and severe fines are both components of these sweeping regulations that have changed the way the healthcare industry does business.

Who

HIPAA applies to "Covered Entities." This law defines the term to include:
(1) Health Plans—plans that provide or pay for the cost of healthcare;
(2) Health Care Clearinghouses—entities that process/facilitate information relating to an individual's health, health care or health care payment; and
(3) Health Care Providers—doctors, dentists, hospitals, clinics, medical groups or other providers of medical services that maintain or transmit health information in an electronic form.

What

HIPAA applies to "Protected Health Information"(PHI), which is information that:
(1) relates to the provisions for payment of health care for an individual;
(2) contains details that can be used to identify the individual (name, address, SSN, etc.), and;
(3) is either created or received by a Covered Entity.

PHI can be created or received in a number of ways. These include not only obvious examples such as medical records or medical bills, but also employee health plan enrollment forms and claim payment or health savings plan information submitted to employee group health plans. The security provision of the HIPAA is applicable to PHI in paper, electronic or any other format. The Security Rule applies solely to PHI in an electronic format, whether in transit, residing on a network or stored in portable media.

Why

HIPAA compliance standards are the result of concerns about the computerization of medical information which was subject to risk of unauthorized disclosure due to errors, misfeasance or computer exploits. HIPAA and its regulations were created to stop the negligent, intentional and sometimes careless manner in which private health information was being handled.

The Covered Entities need to maintain reasonable and appropriate administrative, technical and physical safeguards:
(1) to ensure integrity and confidentiality of PHI;
(2) to protect against any reasonably anticipated threats or hazards to the security, integrity, or unauthorized uses or disclosures of PHI, and;
(3) to ensure compliance by officers and employees of the Covered Entity with HIPAA.

#	HIPAA Compliance Requirement	Standards Implementation Specifications (R)=Required, (A)=Addressable	Type of Requirement	SoluSoft N2 Compliance with HIPAA
Technical Safeguards				
1	164.312(a) (1)	**Access Control (R)**	Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).	N2 provides authentication and authorization. N2 integration with Microsoft Active Directory Services (ADS) provides central single sign on authentication. This method provides strong login and password controls with policies for the format, length, and re-use of user login and passwords with central user and N2 system resource management. The authorization uses roles and access control list (ACLs) to protect and prevent unauthorized access to database records, documents and system resources. The roles and ACLs are created as per company business procedures, rules, and regulations. Digital signature will provide strong non repudiation to maintain authenticity of records.
2	164.312(a) (2)(i)	**Unique User Identification (R)**	Implement procedures to assign a unique name and/or number for identifying and tracking user identity.	User login IDs are used for identification and auditing purposes.
3	164.312(a) (2)(ii)	**Emergency Access Procedure (R)**		For 7x24 availability, set up redundant N2 systems for high availability (HA)
4	164.312(a) (2)(iii)	**Automatic Logoff (A)**		N2 provides timed automatic session logoff
5	164.312(a) (2)(iv)	**Encryption and Decryption (A)**	Implement procedures to describe a mechanism to encrypt and decrypt ePHI.	N2 integrates with third party products to encrypt and decrypt database records and file systems.
6	164.312(b)	**Audit Controls (R)**	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information	N2 ensures transaction non-repudiation by recording every transaction so that a complete audit trail, including authorization and authentication information

			systems that contain or use ePHI.	that is provided, is available in situations where repudiation could be an issue. This is implemented through Digital signatures, Time Stamping and extensive logs.
7	164.312(c)(2)	**Mechanism to Authenticate Electronic PHI (A)**	Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	N2 uses digital signature technology to maintain the authenticity of database records and file system
8	164.312(d)	**Person or Entity Authentication (R)**	Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	N2 provides authentication and authorization. N2 integration with Microsoft Active Directory Services (ADS) provides central single sign on for authentication. This method provides strong login and password controls with policies for the format, length, and re-use of user login and passwords with central user and N2 system resource management.
9	164.312(e)(1)	**Transmission Security**	Implement technical security policies and procedures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.	N2 can utilize secured socket layer and https protocol to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.
10	164.312(e)(2)(i)	**Integrity Controls (A)**	Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.	N2 can utilize secured socket layer and https protocol to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.
11	164.312(e)(2)(ii)	**Encryption (A)**		N2 can integrate with third party product to encrypt and decrypt database records and file systems.