



COMPLIANCE OF SUBPART C

Security Standards for
Protection of
Electronic Protected
Health Information





Definitions

EPHI: Electronic Protected Health Information, either patient administrative or clinic information.

The background of the slide is a dark, monochromatic image of a circuit board. A large, metallic padlock is positioned in the upper left quadrant, its body resting on the board. The text 'SECURITY STANDARD' is overlaid in the center, with 'SECURITY' on the top line and 'STANDARD' on the bottom line. To the right of the text is a vertical white line that separates it from a list of four bullet points.

SECURITY STANDARD

- Ensure confidentiality, integrity and availability of EPHI
- Protect against any anticipated threat or hazard
- Protect against any uses or disclosure
- Implement appropriately in accordance with the environment

SUBPART C

Security Standards for Protection of Electronic Protected Health Information

Rule	Description
§ 164.308	Administrative Safeguard
§ 164.310	Physical Safeguard
§ 164.312	Technical Safeguard
§ 164.314	Organizational Requirements
§ 164.316	Policies and procedures and documentation requirements

§164.308: Security Management Process

Implement policies and procedures to prevent, detect, contain and correct security violations

Implementation Specification	Activity to comply
Risk Analysis	Conduct an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of the EPHI.
Risk Management	Implement security measures to reasonably and appropriately reduce risks and vulnerabilities.
Sanction Policy	Define appropriate sanctions and apply them to workforce who fail to comply with the security and confidentiality policies.
Information System Activity Review	Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports.
Assigned Security Responsibility	Identify the security official who will be responsible for the implementation and applications of the policies and procedures.

INSTITUTIONAL POLICIES

§164.308: Workforce Security

Implement policies and procedures to ensure all members of the workforce have the appropriate access/restrictions to the EPHI

Implementation Specification

Activity to comply

Authorization

Implement procedures to authorize members of the workforce the access and restrictions to the EPHI.

Use BIZUIT® Users and Roles Module to create users and assign them the corresponding roles.



Workforce Clearance

Implement procedures to validate that the access of a workforce member is appropriate.

Validate BIZUIT® user interface to ensure that users have the appropriate access and restrictions.



Termination

Implement procedures to terminate the access to the EPHI when the workforce member ends.

Use BIZUIT® Users and Roles Module to delete or disable users.



§164.308: Information Access Management

Implement policies
and procedures to
authorize access to
EPHI

Implementation
Specification

Activity to comply

Isolating
clearinghouse
functions

The clearinghouse must implement policies and procedures that protect the EPHI of the clearinghouse from unauthorized access by the larger organization.

BIZUIT® Users and Roles module is restricted only to superusers.



Access
authorization

Implement policies and procedures for granting access to EPHI. For example, through access to a workstation, transaction, program, process, or other mechanism.

Use BIZUIT® Users and Roles module and grant the corresponding permissions.



Access
establishment and
modification

Implement policies and procedures that establish, document, review and modify a user's right of access to a workstation, transaction, program or process.

Use BIZUIT® Users and Roles module in conjunction with the processes security configuration to review and modify the corresponding user's permissions.



§164.308: Security Awareness and Training

Implement a security awareness and training for all members of the workforce

Implementation Specification	Activity to comply
Security reminders	Conduct periodic security reviews and updates.
	INSTITUTIONAL POLICIES RESPONSIBILITY
Protection from Malicious Software	Implement policies and procedures for guarding against, detecting and reporting malicious software.
	INSTITUTIONAL POLICIES RESPONSIBILITY (antivirus)
Log-in Monitoring	Implement policies and procedures for monitoring log-in attempts and reporting discrepancies.
	BIZUIT® System Audit Module to monitor log-in attempts
Password Management	Implement procedures to create, maintain and safeguard passwords.
	Use BIZUIT® Users and Roles Module to maintain passwords



§164.308: Security Incident Procedures

Implement policies
and procedures to
address security
incidents

Implementation
Specification

Activity to comply

Response and
Reporting

Identify and respond to suspected or known security incidents; mitigate to the extent practicable, harmful effects of the security incident that are known by cover entities or business associates, and document them and their outcomes.

**ADHERE TO INSTITUTIONAL
POLICIES**

§164.308: Contingency Plan

Implement policies and procedures for responding to critical disasters, failures and damages to EPHI

Implementation Specification	Activity to comply
Data Backup	Implement procedures to create and maintain retrievable exact copies of the EPHI. Comply DB backup and external storage policies and procedures.
Disaster Recovery Plan	Implement procedures to restore any loss of data. Comply DB restore from external storage policies and procedures.
Emergency Mode Operation Plan	Implement procedures to enable continuity of critical business processes. Platform + BIZUIT® horizontal and/or vertical redundancy
Testing and Revision Procedures	Implement procedures for periodic testing of contingency plan. INSTITUTIONAL POLICIES RESPONSIBILITIES
Application and Data Criticality Analysis	Assess the criticality of specific applications and data in support of other contingency plan components. INSTITUTIONAL POLICIES RESPONSIBILITIES



§164.310: Physical Safeguards

Implement policies and procedures to limit physical access to EPHI

Implementation Specification

Activity to comply

Facility Access Controls

Implement policies and procedures to limit physical access to its EPHI systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed.

Workstation Use & Security

Implement policies and procedures that specify the proper functions to be performed.

Implement physical safeguard for all workstations that access EPHI, to restrict access to authorized users.

Device and Media Control

Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility.

INSTITUTIONAL POLICIES RESPONSIBILITY

§164.312: Access Controls

Implement technical policies and procedures to allow access to EPHI for information systems

Implementation Specification

Activity to comply

Unique User Identification

Assign a unique name and/or number for identifying and tracking user identity.

BIZUIT® Users and Roles Module will only permit a user creation with a unique username.



Emergency Access Procedure

Implement procedures for obtaining necessary EPHI during an emergency.

N/A: since EPHI transmission can only be audited but not accessed for CRUD transactions.

Automatic Logoff

Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

BIZUIT® dashboard will logoff a session after a customized time of inactivity.



Encryption and Decryption

Implement a mechanism to encrypt and decrypt EPHI.

BIZUIT® can encrypt/decrypt data for DB storage, and work with encrypted communication channels.



§164.312: Audit Controls

Implement
procedures that
record activity

Implementation
Specification

Activity to comply

Audit Controls

Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.



BIZUIT® record all general activity and detailed activity within traceable structured logs.

Users can examine this information using BIZUIT® Dashboard with an authorized user.

§164.312: Integrity

Implement policies and procedures to protect EPHI from improper alteration or destruction

Implementation Specification

Activity to comply

EPHI authentication

Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.



BIZUIT® does not permit any physical modification or deletion.

BIZUIT® implements versioning for modifications, and disabling for logical deletion.

BIZUIT® stores and traces all operations.

§164.312: Person and Entity Authentication

Implement procedures to verify a person or entity

Implementation Specification

Activity to comply

Person or Entity Authentication

Implement procedures to verify that a person or entity seeking access to EPHI is the one claimed.



BIZUIT® security layer within BIZUIT® EventManager validates/authorizes all access to the system, whether they are made by a person or another system (integration scenario).

Both the GUI and all Processes (integration and business processes) running over BIZUIT® Engine are validated/authorized before execution.

§164.312: Transmission Security

Implement technical security measures to guard EPHI transmissions

Implementation Specification

Activity to comply

Integrity Controls

Implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of.

All BIZUIT® transmissions are encrypted whether by the channel (https and/or VPN) or by encrypting the message if required.

Encryption

Implement a mechanism to encrypt EPHI whenever deemed appropriate.

BIZUIT® can handle encryption and decryption, upon requirement, at data, transport or communication to other systems or to the presentation layer (https).



§164.314: Organizational Requirements

Implementation Specification

Activity to comply

Business Associates Contracts

The contract will ensure that any business associate member of the workforce (both internal or subcontractor) that create, receive, maintain or transmit EPHI on behalf of the cover entities agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement.

Any business associate will report any security incident of which it becomes aware, including breaches of unsecured EPHI.

Group Health Plans

Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the EPHI that it creates, receives, maintains, or transmits on behalf of the group health plan.

Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information.

Report to the group health plan any security incident of which it becomes aware.

INSTITUTIONAL POLICIES RESPONSIBILITY

§164.316: Documentation

Implement policies and procedures to maintain a written record of action, activity or assesement

Implementation
Specification

Activity to comply

Time Limit

Retain the documentation for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

Availability

Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

Updates

Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the EPHI.

Compliance

BIZUIT® graphic design with zero code implementation + the auto-documentation module enable to keep online and up to date documentation all the time and every time that the documentation is required.

