

Baxa Corporation

HIPAA Compliance

Technical Paper

Understanding how Baxa products comply with the US
Department of Health and Human Services, Health
Insurance Reform: Security Standard, 45 CFR Part 164


Baxa Corporation
14445 Grasslands Drive
Englewood, CO 80112
tel: 303-690-4204
fax: 303-690-4804
www.baxa.com

Introduction

The Code of US Federal Regulations (CFR) indexes the general and permanent rules published in the Federal Register by the Executive departments and agencies of the federal government of the United States. The CFR is divided into 50 titles that represent broad areas subject to federal regulation. Each title is divided into chapters, usually bearing the name of the issuing agency.

Title 45 of the CFR is owned and controlled by the department of Health and Human Services and is subtitled the Health Insurance Portability and Accountability Act (HIPAA). Part 164 of Title 45 addresses organizational, administrative, and technical requirements relating to security and privacy of patient information. Subpart C addresses security standards for the protection of electronic protected health information. Organizational and administrative requirements are the responsibility of the healthcare organization.

Baxa automated compounder products are designed to comply with the safeguards identified in 45 CFR Part 164. The products may accomplish these safeguards through built-in features, product configuration, or may rely on the existing healthcare infrastructure. Additionally, Baxa products are configurable. Baxa may recommend specific configurations to accomplish safeguards. We cannot ensure HIPAA compliance if customers do not implement these recommendations. The following paper addresses Baxa recommendations and product compliance to HIPAA.

Background

Baxa provides several products in various forms that use electronic patient health data. Baxa may offer an application as an executable file, as an application with a desktop computer, or an application may be installed on an embedded device. All product instances are addressed in the following discussion.

Several older-generation compounder products (Exacta-Mix™ 600 and MicroMacro™ 12 and 23) and the order entry software (Abacus™) may be supplied on desktop computers. Baxa installs an operating system and a small number of applications specific to the solution being provided. The Exacta-Mix 2400 (EM2400) Compounder application is installed on an embedded computing device that uses an embedded operating system.

Baxa products maintain a limited set of patient data including patient name, date of birth, age, sex, healthcare facility account number, and total parenteral nutrition (TPN) ingredient formulations. The patient account number is the only required patient health information.

Interpretation

The regulation defines requirements in numbered section paragraphs. Some requirements are followed by 'implementation specifications.' An implementation specification further clarifies the intent of the requirement. Additionally, the implementation specification indicates whether the explanation is 'required' or 'addressable.' By prior note in 45 CFR Part 164, a specification that is 'required' must

be implemented. 'Addressable' requirements must be implemented if deemed necessary and appropriate by analysis.

The italicized text below indicates text reproduced verbatim from the Code of Federal Regulations, Title 45, Part 164, Subpart C, Appendix A, paragraph 164.312, Technical Specifications.

Section (a) (1) Standard: Access Control

Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in paragraph 164.308(a)(4).

Section (a) (2) Implementation Specifications:

Sub-Section (a) (2) (i) Unique User Identification

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

Compliance: All Baxa automated compounder products are accessed through Microsoft® operating systems and rely on the authorization (username) and authentication (password) methods of the operating system. Additionally, the order entry applications and compounders have their own distinct and separate authorization and authentication mechanisms to further restrict access to appropriate personnel.

Data files are shared between Baxa applications through the Microsoft file sharing feature. Only authorized and authenticated users may access the data contained in the common file shared space.

Technical policies and procedures are the responsibility of the facility. Baxa can only recommend configurations and equipment usage.

Recommendation: Individual users of Baxa automated compounder products should have accounts including a unique username, password and access rights. Users should use only their account to operate equipment.

Sub-Section (a) (2) (ii) Emergency Access Procedure

(Required) Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

Compliance: All Baxa automated compounder products provide an administrator account for access in an emergency.

Recommendation: The administrator username and password should be unique and distinct from typical users. Typical users should not operate equipment and applications through the administrative account. Abacus, Exacta-Mix 2400 and Exacta-Mix 600 applications should be configured for automatic backup to permanent and recoverable storage locations.

Sub-Section (a) (2) (iii) Automatic Logoff

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

Compliance: All Baxa automated compounder products are accessed through Microsoft operating systems and use the native user account facilities. Microsoft user account facilities may be configured to terminate electronic sessions after a predetermined time of inactivity. The Abacus, Exacta-Mix 2400 and Exacta-Mix 600 products each may be configured for automatic logoff, as well.

Recommendation: When it is deemed necessary and appropriate, customers should configure the user accounts, both machine and application, with a timeout period in accordance with their facility's policies and procedures.

Sub-Section (a) (2) (iv) Encryption and Decryption

(Addressable) Implement a mechanism to encrypt and decrypt electronic protected health information.

Compliance: Baxa products do not provide encryption / decryption utilities for protected health information. Encryption applications are addressable by the customer installing an application that encrypts / decrypts all network transmission or data storage operations.

Recommendation: When it is deemed necessary and appropriate to encrypt / decrypt electronic protected health information customers are recommended to add a public key encryption application compatible with healthcare facilities.

Section (b) Standard: Audit Controls

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

Compliance: All Baxa automated compounder products contain logging utilities that record operations performed by users. Embedded computing devices contain log files that record operator actions and machine command/response messages. Log files are stored on the system and are recoverable by the administrator for backup, storage or retrieval.

Recommendation: The customer should add procedures to back up databases and log files and print daily activity reports for quality auditing.

Section (c) (1) Standard: Integrity

Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Section (c) (2) Implementation specification: Mechanism to authenticate electronic protected health information

(Addressable) Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Compliance: All user operations are logged in Baxa automated compounders and may be used to corroborate actual results. Customers may corroborate results with log file data to ensure protected health information has not been altered or destroyed in an unauthorized manner.

Recommendation: When it is deemed necessary and appropriate, customers may cross reference actual equipment results with log file data and independent electronic protected health information to authenticate information integrity. These processes should be defined in procedures and catalogued for periodic audit.

Section (d) Standard: Person or Entity Authentication.

Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Compliance: Baxa automated compounder equipment uses Microsoft operating system accounting facilities, in addition to application authentication and authorization. Procedures for verifying, allocating and configuring user accounts are the responsibility of the healthcare facility.

Recommendation: Healthcare facilities should develop the appropriate practices and procedures such that individuals do not share common accounts and that user accounts are properly verified, allocated and configured.

Section (e) (1) Standard: Transmission Security.

Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

Section (e) (2) Implementation Specifications:

Section (e) (2) (i) Integrity Controls

(Addressable) Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

Compliance: Baxa automated compounder products rely on multiple layers of computer networking and customer quality systems to ensure health information is not improperly modified. Network protocols include Transmission Control Protocol and Internet Protocol. Together they employ parity, frame-check sequences, and retransmission capabilities. Universal Serial Bus interfaces employ frame-check sequences, cyclic redundancy checks and retransmission capabilities. Inter-processor communications employ retransmission and polling methods. Collectively, these methods provide a high degree of data reliability and integrity.

Recommendation: Customers should employ multiple quality audits, review and confirmation of order entry formulation, TPN compounding operations and final bag order delivery as part of their quality system as added protection to the existing integrity controls.

Section (e) (2) (ii) Encryption

(Addressable) Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Compliance: Baxa automated compounder products do not provide encryption utilities for patient information. Encryption applications are addressable by the customer installing an application that encrypts all network transmission, decrypting all receptions.

Recommendation: When it is deemed necessary and appropriate to encrypt electronic protected health information, customers are recommended to add a public key encryption application compatible with the healthcare facility's policies.