Bluebird: Security Compliance v4 5 Jan 2017

This paper will concentrate on documenting Bluebird's compliance with security standards and detail how that compliance is implemented.

The hospital group (covered entity) is responsible for the network, workstation computers and all software on those computers. Intelligent Medical Systems, hereafter IMS, is responsible for the Bluebird System. User authentication is usually done by the covered entity, but in the unusual circumstances where done by IMS, the details are also included in this document.

OVERVIEW OF SPECIFIC SECURITY MEASURES IMPLEMENTED BY BLUEBIRD

A) ACCESS CONTROLS

The aim is to protect ePHI (electronic patient health information) from unauthorized access, alteration, or deletion without denying or impeding authorized access. Because access control is the foundation upon which protecting ePHI rests, Bluebird maintains very careful control over access to the system. The intent is to recognize and prevent unauthorized activity. Bluebird Servers are kept in a physically secure environment behind a secure firewall. Bluebird has developed, and implements policies, procedures, and processes so that access is only allowed to persons that have appropriate Bluebird access rights and Bluebird denies access to unauthorized users. This is accomplished by means of:

I. *Unique user identification* - Each user is assigned a unique name for identifying and tracking their identity. No shared log-ins are permitted.
II. *Emergency access procedure* - procedures for obtaining necessary electronic protected health information during an emergency are defined. Bluebird has reliable backup procedures, and has developed a contingency plan appropriate to address the most likely emergencies.
III. *Automatic logoff* - The termination of inactive sessions is essential and is implemented in Bluebird. Bluebird automatically disconnects any user session that remains idle beyond a covered defined limit.

B) AUDIT CONTROLS

Activities which impact ePHI are recorded and Bluebird provides an audit trail for reviewing such activity. Bluebird tracks data creation and modification – where appropriate and relevant - as well as system access, and provides a mechanism for review (Audit log, Access reporting, Incident tracking).

C) INTEGRITY

Policies, procedures, and processes have been developed and implemented to corroborate that electronic protected health information within Bluebird has not been altered or destroyed in an unauthorized manner. The Bluebird environment is a controlled one where creating, editing, and deleting records is limited to authorized users under "proper" circumstances. (Data Integrity is ensured via Role- and Function-based Access Controls, User Authentication, Password Management, as well as the Audit Log). Bluebird 's audit trail is able to prove that unauthorized alteration or destruction has not occurred. Unauthorized activity is also prevented by a combination of measures employed to ensure the failure of unauthorized attempts to alter or destroy ePHI. (Access Reporting, Incident Tracking, Access Controls, Auto Log-off, Encryption, User Authentication, and Password Management).

D) PERSON OR ENTITY AUTHENTICATION

Bluebird incorporates Access Controls and User Authentication to validate the unique identity of each user and verify that a person or entity seeking access to electronic protected health information is the one claimed.

E) TRANSMISSION SECURITY

Bluebird utilizes access controls and network encryption (SSL) to protect against unauthorized access during all network transmissions.

I. *Integrity controls* - Bluebird implements security measures to ensure that electronically transmitted electronic protected health information cannot be modified without detection.
II. *Encryption* - This aims to prevent unauthorized users from accessing ePHI. Any time ePHI is sent outside of the boundaries of the network, it is encrypted using SSL.

MECHANISMS BLUEBIRD USES TO ADDRESSES THE SYSTEM REQUIREMENTS FOR COMPLIANCE:

1. Bluebird Audit log
2. Access reporting
3. Incident tracking
4. Access control
5. Contingency planning
6. User documentation
7. Auto log-off
8. Encryption
9. Data integrity
10. Data authentication
11. User authentication
12. Password management

The next section discusses these mechanisms in detail.

MECHANISMS BLUEBIRD USES TO ADDRESS PATIENT CONFIDENTIALITY AND SECURITY OF INFORMATION:

1. BLUEBIRD AUDIT LOG (BBAL)

The BBAL records any End User's creation or modification of clinical data.

Unauthorized alteration of clinical records is prevented by access controls and by locking records once they are signed off.

The BBAL can be examined regularly by administrative staff for inconsistencies or unauthorized activity. *HIPAA's Information System Activity Review* [164.308(a)(1)(ii)(D)] states: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

2. ACCESS REPORTING

A mechanism for review of system access is necessary for compliance and Bluebird makes this accessible to the appropriate individuals in order for the covered entity to monitor activity and verify that only authorized individuals have been granted access to the system. Bluebird's Access Log includes identifying information about the user, in addition to the specifics of when access was provided. Where possible, Bluebird also documents when access ended. To ensure that a user's access is always reported, Bluebird does not allow entry to the system without the creation of a session record. If the user logs out of Bluebird, the end-of-session time-stamp is recorded. If a user disconnects from the network without logging out, Bluebird will not record a logout event at that time. However if the user later reconnects to the network and tries to continue working, they will be forced to log in again if their login session has expired.

3. INCIDENT TRACKING

Trackable incidents are defined as:

- Login failures
- A user's rejection of the stated terms of use
- Attempts to view, modify or delete ePHI for which the user does not have appropriate privileges are prevented and logged for auditing.

Bluebird monitors this log and real time reporting is available to the appropriate person nominated by the covered entity.

In addition to documenting any identified incidents, appropriate response measures are also followed, Bluebird closes the session and, in the case of multiple log ins, blocks further attempts from that IP address, if not on the Bluebird safe list, for a period.

4. ACCESS CONTROL

The primary intent of the Security Rule is to protect ePHI from unauthorized access, alteration, or deletion, *without denying or impeding authorized access*. Bluebird therefore maintains very careful control over access to the system in order to recognize and prevent unauthorized activity.

Bluebird Servers are kept in a physically secure environment behind a secure firewall and the Server discs are encrypted so that, even if stolen, the data is still protected.

All users have assigned roles against which user activity is validated.

The granularity of Bluebird's Record-level Access controls allows us to implement user-specific, role-based, and situational access restrictions.

Activity logs and audit trails track users activity.

5. CONTINGENCY / EMERGENCY PLANNING

An emergency is any event with the potential to render protected data unavailable. This might include catastrophic events such as fire, flood, hurricanes, earthquakes, and other natural disasters. It also includes short-term events such as equipment failures, power failure, sabotage, theft, or other unexpected disruption.

ePHI is stored on Bluebird's Servers, never on the local access devices.

Bluebird ensures the availability of ePHI in the event of an emergency as follows:

A) DATA BACKUP

Bluebird maintains "exact retrievable copies" of ePHI.

The Bluebird server cluster - it actually consists of up to 16 (but typically 3) servers, that are seen as one unit - has multiple hard drives which replicate the data locally. The data on this server cluster is also backed up daily (or more, if requested by the covered entity) to an offsite server, which, if requested by the covered entity, can be in a second regional zone.

Bluebird's design allows any of these servers to fail without impacting on the end user. Each server has redundant power supplies and the datacenter similarly has redundant power supplies.

These servers are virtual machines. If a failure occurs, Bluebird's staff can create a new virtual machine within minutes.

In some countries Bluebird utilizes Amazon's Web Service. In this case, the built-in MySQL clustering/failover works with two nodes. These servers are in separate availability zones, so if one of the machines dies or one of the availability zones dies, the other database server will take over. It is possible to also have another database server set up in a third availability zone using asynchronous replication for further redundancy if a disaster makes both of the other database servers inaccessible.

B) CONTINGENCY, EMERGENCY MODE OPERATION AND DISASTER RECOVERY PLAN

The backup servers are easily escalated to act as the primary servers during an emergency. Similarly, data backed up on these servers is easily restored to the primary server once that server is reconstituted.

6. USER DOCUMENTATION

Intelligent Medical Systems is able to provide system-specific user training and comprehensive documentation, as well as, security awareness and training programs, for all members of the covered entity. Intelligent Medical Systems staff undergoes training programs, which include security awareness.

Moreover, Bluebird's design helps to reduce training requirements with it's logical, easy-to-use and consistent interface.

7. AUTO LOG-OFF

The termination of inactive sessions is essential and is implemented in Bluebird. Bluebird automatically disconnects any user session that remains idle beyond a defined limit.

8. ENCRYPTION

HIPAA's Security Rule requires a mechanism to encrypt and decrypt ePHI. Bluebird accomplishes this by:

- Storing all data centrally
- Encrypting that storage volume so that even if the hard drive was stolen the encrypted data would not be useful.
- Only allowing access to the central storage through SSL.

Drive level encryption fulfills the Access Control section of this well, as only an authenticated person with the correct credentials can access the data. It also ensures integrity - the data cannot be improperly modified, as the encrypted volume appears as random data with the correct key. It also ensures entity authentication via the login process.

9. DATA INTEGRITY

To ensure that data has not been modified or deleted in an unauthorized manner Bluebird has created a controlled environment where create, edit, and delete functionality is limited to authorized users under "proper" circumstances.

This is accomplished by using a combination of access controls, user authentication, password management, audit trails, incident tracking, and user training. In addition to controls intended to limit system access to authorized users, we also institute measures that appropriately restrict authorized users from performing unauthorized actions.

Bluebird only allows authenticated users access to functionality commensurate with their security clearance.

10. DATA AUTHENTICATION

Following audit trail activity, one is able to authenticate the validity of ePHI in Bluebird. ePHI is never transmitted via unsecured means, such as unencrypted email and Bluebird is able to authenticate that the data has not been modified in transit. Features including CheckSum are used to verify that data remains unaltered upon receipt. The Bluebird audit trail is an important tool used to meet statutory data authentication requirements.

11. USER AUTHENTICATION

The ability to accurately identify each specific user is the foundation upon which all other Bluebird security controls depend, so it was critical that we followed sound practices when implementing user authentication. This is what we do:

Typically Bluebird uses the hospital groups (covered entity) own authentication mechanism either via their active directory or via a secure SOAP service. This ensures that the covered entity has full control over access.

System verification is done on log in, and an automatic log out occurs if the user is inactive for longer that a set time.

12. PASSWORD MANAGEMENT

If authentication is handled via the covered entity's own authentication infrastructure, Bluebird cannot enforce password changes which are then handled by the covered entity's authentication infrastructure.

Bluebird's external server authentication uses LDAP, the industry standard. Password management is done by the end user. To ensure that only the individual user knows their own password, new accounts require that the password be changed at initial login. Shared login accounts are prohibited. Each user has a separate user name and duplicate user names are prohibited.

Passwords have a minimum length (6 characters by default) and must be changed regularly (every 30 days by default).

If corporate standards exist in the covered entity for other password-protected systems, Bluebird is able to follow those same standards e.g. minimum password length, change frequency, maximum password length, both alpha and numeric characters required etc.

13. ELECTRONIC SIGNATURES, NON REPUDIATION AND DOCUMENT INTEGRITY

Electronic signatures are considered the legally binding equivalent of handwritten signatures. As such, Bluebird implements a number of controls to ensure their irrefutability.

These controls include:

- Authentication of the signer's identity. Each User has a unique Username and Password, which is verified on login
- Binding of the signature to the clinical document. The user ID is stored in the record when it is signed along with the date and time that the record was signed. The user ID and timestamp are stored in the record in fields that the user cannot access.
- The signature process includes attaching user-identifying elements to the document in such a way, as those elements cannot be altered. These identifying elements are based on that user's authentication and the user has no access to the elements themselves.
- Non-alterability of the document after the signature has been affixed. Once the record has been signed, the system prevents editing of the record. e.g. if a user opens the HAI form after it has been signed, the system checks that the form has been signed, and displays a read-only version of the form.

Legal documents (such as the HAI form) produced by Bluebird are stamped with the User Name of the person who created that document. Such documents are electronically signed with both the User Name of the person that signed off that document, as well as a time-stamp. Adding the electronic signature requires an explicit action on the part of the user to sign off the document and, once signed, the document cannot be altered.

These features ensure that Bluebird documents, signed with an electronic signature, cannot be repudiated and document integrity is ensured.

NON TECHNICAL SAFEGUARDS

Though not technical in nature, the following Administrative safeguards implemented in Bluebird are of particular relevance to the development of a compliant system.

1. BUSINESS ASSOCIATE CONTRACTS (BAC) AND OTHER ARRANGEMENTS

Bluebird provides a standard BAC to conform with the following HIPAA requirements:

A covered entity, in accordance with §164.306, may permit a business associate to create, retrieve, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a) that the business associate will appropriately safeguard the information.

A covered entity must obtain satisfactory assurance in the form of a written contract prior to allowing a business associate to access the PHI for which covered entity is responsible (see §164.308(b)(4)).

Please contact privacy@intelms.com.au for Bluebird's BAC.

2. WRITTEN CONTRACT OR OTHER ARRANGEMENT

Bluebird's Business Associate Contract (BAC) meets the applicable requirements of HIPAA §164.308(a) and documents the assurances required by paragraph (b)(1) of this section.

Please note that the execution of this BAC does not transfer the burden of compliance from the covered entity to Bluebird, however, the Bluebird BAC does create a contractual obligation for which Bluebird is responsible.

3. PROTECTION FROM MALICIOUS SOFTWARE

There are many forms of malicious software that can impact data and networking systems. Bluebird takes the following measures to ensure that it's Servers are free of malicious software:

- Regular Security Updates. The CTO or his delegate reviews the logs periodically and documents that the review has been completed.
- Monitoring suspicious attempted log ins
- Antivirus software
- Breach Detection Software. IMS's CTO (Chief Technical Officer) is responsible for investigation of any breach detected by the intrusion detection software.

The covered entity also needs to have procedures in place to protect it's network and all it's computers.

CONCLUSION

This document has been written to demonstrate Bluebird's compliance with national security standards. Please feel free to address any question to privacy@intelms.com.au

REFERENCES

1.Security Standards; Final Rule. 45 CFR Parts 160, 162, and 164. February 20, 2003. Please note that Part 164 begins on page 8374 of the Federal Register, after a 40-page preamble.

http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf

2. Security Rule Guideline Matrix. Easy-to-read chart presents administrative, physical, and technical guidelines of the Security Rule grouped by “required” or “addressable”. In addition, identifies wether or not responsibility is shared between the covered entity and developer. Matrix covers 45 CFR §164.308 through §164.312.

http://www.harmonic-data.com/hipaamatrix.pdf

3.Proposed Rule. On August 12, 1998, the U.S. Department of Health and Human Services published the proposed Security Rule. Based on public comment, the Proposed Rule was stripped of specificity and made vague.

http://www.cms.hhs.gov/SecurityStandard/Downloads/securityproposedrule.pdf

4. HIPAA Glossary. The Workgroup for Electronic Data Interchange (WEDI), a national consortium of public and private corporations and organizations within the health care industry, focus on the electronic delivery of electronic health care information. WEDI maintains a comprehensive glossary of HIPAA-related terms and acronyms.

http://wedi.org/snip/public/articles/hipaa_glossary.pdf

5. 21 CFR, Part 11—The Final Rule. On March 20, 1997, the Federal Drug Administration (FDA) published regulations that provide criteria for acceptance by the FDA of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures written on paper. Please note that the actual regulation begins on page 13464 of the Federal Register, after a 34-page preamble.

http://www.fda.gov/ora/compliance_ref/part11/FRs/background/pt11finr.pdf

6. 21 CFR, Part 11—Industry Guidance. This document is intended to describe the Food and Drug Administration’s current thinking (circa 2003) regarding the scope and application of CFR 21 Part 11; Electronic Records; Electronic Signatures.

http://www.fda.gov/Cder/guidance/5667fnl.pdf

