Bluebird Platform

Security Policies and Procedures

A cloud based organizational framework designed to improve Patient Safety

Latest Review: Sep 2023

Table of Contents

Introduction

The Bluebird Security Compliance Statement is available here: www.intelms.com/1i. This manual documents ***Internal* Policies and Procedures** that IMS staff follow in order to meticulously protect private patient information.

Policies and Procedures

Staff Training: Privacy and Security of Personal Information

OVERVIEW

Intelligent Medical Systems (Pty) Ltd, hereafter IMS, was founded specifically to protect personal health information (PHI) and we take our responsibility to provide regular Security Awareness Training to the Bluebird Support and Operations workforce extremely seriously. That Security Awareness Training is designed to ensure each and every staff member is intimately familiar with the IMS policies and procedures that were specifically designed to protect personal health information (PHI).

Patient confidentiality procedures/policies are communicated to staff each quarter and formal training regarding company Security Policies is provided annually, or whenever there is a material change in any policy or procedure. Following such a change, the affected staff member/s is retrained within 1 calendar month, or sooner, as may be appropriate.

Training sessions are logged and audit-able.

Besides **certified support staff**, select **senior management** including the Chief Technical Officer and the Designated Security Officer (who is responsible for developing and implementing information about our security policies and procedures) also have access to PHI. Wesley Hendricks is the Operational Security Lead whose responsibilities include monthly testing of the Disaster Recovery Process.

IMS train our workforce using both national (POPIA) and international (HIPAA) guidance to optimize privacy of personal information. Strict attention is paid to the requirements spelled out in both POPIA and the HIPAA security rule. Workforce training is executed through normal or existing organizational educational operations. We maintain ongoing updates and retain our documentation for a minimum of six years from the implementation date.

Support staff are specifically instructed never to disclose PHI during support calls or by email. Any End User requesting PHI is directed to log onto the Bluebird system to view that information. If that EndUser requires information which they cannot access on the system, they are instructed to ask an End User that has the appropriate level of access and that interaction is logged.

IMS will apply appropriate sanction against any workforce member who is found to have violated IMS privacy policies.

SANCTIONS

These are the possible sanctions which are based on both the outcome of the investigation and the category of the violation:

1. Verbal warning and additional training.
2. Verbal warning, additional training and removal of data access.
3. Written warning and additional training.
4. Written warning, additional training and removal of data access.
5. Written warning, additional training and permanent removal of data access.
6. Termination of employment.

As soon as a privacy violation is reported, the staff member being investigated has their access to PHI removed pending the result of an investigation. The investigation will follow within 2 days after the violation was reported and should be completed within a further 3 days. The severity of the sanction is based upon the outcome of the investigation. Sanctions, as appropriate are implemented once the investigation is complete and the outcome has been discussed with the workforce member.

VIOLATION CATEGORIES

Category 1: Accidental or inadvertent violation. This is an unintentional violation of privacy or security that may be caused by carelessness, lack of knowledge, lack of training, or other human error. Examples of this type of incident include directing PHI via mail, e-mail, or fax to a wrong party or incorrectly identifying a patient record.

Category 2: Failure to follow established privacy and security policies and procedures. This is a violation due to poor job performance or lack of performance improvement. Examples of this type of incident include release of PHI without proper patient authorization; leaving detailed PHI on an answering machine; failure to report privacy and security violations; improper disposal of PHI; failure to properly sign off from or lock computer when leaving a work station; failure to properly safeguard password; failure to safeguard portable device from loss or theft; or transmission of PHI using an unsecured method.

Category 3: Deliberate or purposeful violation without harmful intent. This is an intentional violation due to curiosity or desire to gain information for personal use. Examples of this type of incident include accessing the information of high profile people or celebrities or accessing or using PHI without a legitimate need to do so.

Category 4: Willful and malicious violation with harmful intent. This is an intentional violation causing patient or organizational harm. Examples of this type of incident include disclosing PHI to an unauthorized individual or entity for illegal purposes (e.g., identity theft); posting PHI to social media web sites; or disclosing a celebrity's PHI to the media.

Sanctions may be modified based on mitigating factors. These factors may reflect greater damage caused by the violation and thus work against the violator, ultimately increasing the penalty.

NEW STAFF

No staff member is granted access to PHI until:

1. References are reviewed

2. A non disclosure agreement is signed and thereafter reviewed at least annually and that review documented and emailed to DSO@intelms.com with the Subject “Annual Confidentiality Review”
3. The probation period (a three month training and evaluation period) is complete
4. Bluebird training on PHI policies and procedures appropriate for that staff member’s role is complete and documented
5. A further evaluation period (generally another **3 months**) implemented specifically to ensure that only experienced and trusted members of the workforce are certified to be allowed access to PHI

DOCUMENTATION

1. Policies and procedures are formally documented and stored electronically.
2. Any communication regarding this policy is required to be in writing and that document is kept for the retention period.
3. If an action, activity, or designation is required by POPIA or HIPAA to be documented, we maintain an electronic record of such an action, activity, or designation
4. Staff training is documented.

DOCUMENT RETENTION

IMS retains the documentation detailed in this section for six years from the date of its creation or the date when it last was in effect, whichever is later.

SUPPORT BY STAFF MEMBERS NOT YET CERTIFIED TO ACCESS PHI

During the period while new staff are awaiting certification, IMS provides a separate, fully functional training system, loaded with dummy data.

WHO IS TRAINED

IMS’s defines workforce as "employees, volunteers, trainees, and other persons whose conduct, in the performance of work, is under the direct control of IMS, whether or not they are paid by IMS." IMS requires that all workforce members receive relevant training on IMS privacy policies and procedures, as necessary and appropriate to carry out their function. We define our training audience according to our operational structure and through careful consideration of a workforce member's access to PHI, responsibilities that present potential compliance risk and contractual relationships that rely on access to PHI.

SPECIFIC TRAINING TOPICS COVERED

IMS’s security awareness and training program includes the following specifics, all of which are covered in detail in the Security Policy:

- **Confidentiality**: Training is given to all members of our workforce, including management. The focus of training is: New User Creation and Access, protecting patient information and reporting possible privacy violations. The policy regarding information requests from patients is also reviewed during this training session.
- **Breach investigations**: Training is given to members of our IT operations department.
- **Security Updates:** Training is given to all relevant staff members.
- **Procedures for guarding against malicious software**: Training is given to members of our IT operations department.
- **Procedures for monitoring suspicious log-in attempts**: Training is given to members of our IT operations department.
- **Procedures for managing passwords:** Training is given to all members of our workforce, including management.

Change Management

Bugs and new feature requests are formally logged in a ticketing system. Bugs reported by End Users are investigated by Bluebird's QA department to ensure that it is, in fact, a bug, and to investigate how best to resolve the issue.

New feature requests are investigated by Bluebird's clinical team who consult with the relevant users before writing the specification. IMS's Medical Director then prototypes the new feature in a proprietary 4th generation programming language. The specification is then checked and fleshed out by the head of the development team, before assigning a developer to implement the feature.

After a bug has been fixed or a new feature has been implemented it is checked by another member of the development team. The change is then migrated to the QA environment for verification by the QA team. Only once the QA team has verified the change and checked that no regressions have been introduced the ticket is signed off. Once the ticket has been signed off, the change can be migrated to the production environment.

Source Code Management

IMS, like many tech companies uses Git to establish an efficient programming workflow. Git is a sophisticated version control system that allows our DEV team to:

- View the history of an existing Bluebird project
- Save versions of a particular project
- See all the versions that have been saved
- Checkout a previous version
- Keep track of multiple versions of a file
- Compare two different versions
- Track bugs by reverting to previous working versions of a file
- Seamlessly collaborate with other developers on our team

The Git repository for the Bluebird System is private with access only granted to authorised members of the Bluebird Development (DEV) Team. DEVs develop on a development branch. When the change is complete it is committed and pushed to the central source code repository. Another developer will then fetch the changes and review them. The QA team then fetches the changes and deploys them to the QA environment for testing. The QA team tests and signs off the change, after which the change is deployed to the production environment. Git allows the developers to work on different changes in parallel, even on the same file if necessary.

Roles and Responsibilities

Michael Wood (CTO) is responsible for approval of the policy and oversees change management and ensures it is performed in line with international standards.

Wesley Hendricks (Security Lead) generally supervises deployment of changes.

Nicola Kelly (DSO and POPIA Deputy Information Officer) is responsible for setting procedures and creating change management documentation.

Jacques Kotze (General Manager) oversees the quality assurance team and ensures that any changes are throughly tested before being deployed to production.

Backups

Backups of the Git repositories are automatically encrypted and transferred off site (to Amazon S3) each night.

Monitoring

Results of the backup are mailed to Bluebird Operations and Bluebird Support.

Filtering rules show the logs where there was an error, so that the script can be re-run.

DB Cluster Disk Encryption

DECRYPTION

To ensure that that data is encrypted at rest as well as in transit, each of the database cluster nodes has full disk encryption enabled.

Decrypting the storage is done before the operating system has booted up, so decrypting needs to be done by physical access to the servers or via remote management.

If the server is being booted remotely, connect to the remote management web interface via the VPN and boot up the server.

During the boot process it will prompt for the encryption pass phrase. Enter that pass phrase.

After entering the pass phrase the server will continue booting.

PASS PHRASE

Michael Wood, Jacques Kotze and Wesley Hendricks keep the pass phrase in their password managers, which means that they are the only personnel that are able to boot the database cluster. The password managers are secured with a long, complex master password.

In case the above personnel are not available or the support office is not accessible, as an emergency recovery measure, the pass phrase is stored in an encrypted text file here:

https://s3.amazonaws.com/bluebird/servers/DB-cluster-pass-phrase.txt.gpg

This file can only be downloaded by senior Bluebird personnel (who are the only staff with access to Bluebird's Amazon Web Service) and the encryption password is only known to this subset of senior IMS staff: Michael Wood, Jacques Kotze and Dr. D. G. Vine (POPIA Information Officer).

Firewall

The Bluebird Firewall utilizes Linux iptables firewall software.

RULES

Rules have been set up to log connection attempts to ports that should not be accessed:

MONITORING

Blocked connection attempts are logged.

UPDATING

Senior IMS Operations staff (currently Michael Wood and Wesley Hendricks) are responsible for firewall updates as required. Changes to the firewall rules are made if access needs to be granted to something that was previously blocked, or something that was previously allowed needs to be blocked.
Operations keep track of the versions of the firewall rules using Git.

RULE REVIEWS

Formal reviews of the firewall rules are scheduled for November each year. If Operations implement a new service or shut down an old service Operations change the rules and review the other rules at that time.

Intrusion Detection

IMS operations utilizes host-based intrusion detection software. **AIDE** (Advanced Intrusion Detection Environment) is used to monitor changes to system files. For Endpoint Detection & Response we use **SAGAN**, a high performance, real-time log analysis & correlation engine to help ensure malicious activity is detected immediately and action taken.
Fail2Ban is used for blocking IP addresses based on entries in log files. So e.g. if the system sees multiple failed login attempts from a particular IP address it can block the IP address for a period.
Chkrootkit tests for hidden files, hidden ports, hidden processes, processes listening on unexpected ports and files created by known malware.

Network-based intrusion detection systems are not useful because all of Bluebird network traffic is encrypted.

MONITORING

Both AIDE and chkrootkit run daily and the results are automatically e-mailed to Bluebird Support. That email account is organized for easy retrieval.

UPDATING

Senior IMS Operations staff (currently Michael Wood and Wesley Hendricks) are responsible for AIDE and chkrootkit updates (important security updates are installed automatically, routine updates are prompted). One only needs to update the AIDE config if we install new software or make changes to the way we are using the filesystem that would cause AIDE to give warnings for files that we expect to change, or because we want AIDE to monitor some files that it was not monitoring in the past. chkrootkit updates are triggered by the built-in Ubuntu software update system called APT.

VERSION TRACKING

IMS Operations keep track of the versions using Git.

REVIEW

Formal annual reviews of the intrusion detection rules were initially planned. However, because both Operations and Support receive daily reports of changed files or other problems that policy was updated so that Operations only need to review the config in the event that they are prompted to do so.

Monthly Service Level Performance Report

UPTIME

This monthly report is sent by Bluebird Operations as an email to DSO@intelms.com with the **Subject** “Monthly Uptime”
The body has this format: Uptime for the month [MonthName] was xxx% (typically 100%).

DATABASE BACKUPS

Bluebird Operations get separate emails *each day* to indicate the success of the daily database backup (email Subject “[OPS] DB Backup SUCCESS - yyy-mm-dd
(or FAILURE)”).
This monthly report is sent by Bluebird Operations as an email to DSO@intelms.com with the **Subject** “Monthly Database Backup Report”.
The body has this format: There were xx days in [MonthName] and the daily backup was successful each day (or, if not successful, an explanation documenting how that unsuccessful backup was resolved is shown for that specific date).

SOURCE CODE BACKUPS

Bluebird Operations get separate emails each day to indicate the success of the *daily* source code backup on git hub (email Subject “[OPS] Software Backup SUCCESS - yyy-mm-dd (or FAILURE)”).
This monthly report is sent by Bluebird Operations as an email to DSO@intelms.com with the **Subject** “Monthly Source Code Backup Report”
The body has this format: There were xx days in [MonthName] and the daily Git backup was successful each day (or, if not successful, an explanation documenting how that unsuccessful Backup was resolved is shown for that specific date).

FIREWALL

This monthly report is sent by Bluebird Operations as an email to DSO@intelms.com with the **Subject** “Firewall Monthly Report” and will indicate whether any changes to the firewall rules were made in the month that has just ended and, if so, document what those changes were.
The body has this format: No changes in Firewall rules were required during [MonthName] (or document the changes that were done).

INTRUSION DETECTION

This monthly report /summary of the *daily* AIDE and chkrootkit monitoring are sent by Bluebird Operations as an email to DSO@intelms.com with the **Subject** “Intrusion Detection Monthly Report”.

The body has this format: The daily intrusion detection monitoring did not show any intrusion during [MonthName] (or document what was detected and how the situation was resolved).
Note: Both AIDE and chkrootkit run on a *daily* schedule and the results are automatically e-mailed to Operation's email account where they are reviewed each day and form the data for this monthly report.

SERVER CLUSTER MAINTENANCE

This monthly report is sent by Bluebird Operations as an email to DSO@intelms.com with the **Subject** "Server Health Monthly Report".
The body has this format:
Month end hard drive free space: xx%
Expected time until next hard drive expansion: >12 months (or x months).
Peak Memory usage during [MonthName]:
Peak Network usage during [MonthName]:

Bits In	xx
Bits Out	xx

If anything was done during the month, this should be comprehensively documented, e.g.
Hard drive space was xx% at the end of the previous month, therefore on dd/mm/yyyy a new RAID array was created. That was added to the volume group. The filesystem containing the SQL database was expanded to take up the newly added space. In all, x 8 additional 2 terabyte SSD hard drives were configured and installed into x machines in the Server Cluster. At the end of the month free hard drive space was xx%

DATABASE MAINTENANCE

This monthly report is sent by Bluebird Operations as an email to DSO@intelms.com with the **Subject** "Database Monthly Report".
The body has this format:
The SQL Database did not require any maintenance this month.

If anything was done during the month, this should be comprehensively documented, e.g.
"Because Operations needed to upgrade the RAM in the Server Cluster, the buffer pool size had to be increased to xx.

Operational Alerts

OVERVIEW

Script sends email alert to support with a specific subject line ending with either SUCCESS (= no problem) or ERROR (problem). All ERRORs get c.c. to operations (which forward to MW and WH). Support's Gmail auto flags ERROR with the ToDo flag. Removing that flag implies an email to operations explaining how the issue was resolved – i.e. support has ownership until resolved. Similarly ERROR c.c. to operations get auto flagged on their ToDo Gmail account and removal of that flag only happens when the resolution from support arrives and Operations is happy with that resolution.
Separate labels will be set up for the separate types of e-mail, in addition to being flagged as TODO.

Database Backups

Email subject:

Success Subject: [OPS] DB Backup SUCCESS - yyyy-mm-dd

Failure Subject: [OPS] DB Backup ERROR - yyyy-mm-dd

Failure – Check the email and see what the error was. Check why the backups have failed and if it can be resolved. If not possible to resolve, escalate to Operations. If not resolved by Support and escalated to Operations, follow up hourly until resolved.

Resolved – Document what steps were taken to resolve the error and flag as resolved.

Git repository backups

Email subject:

Success Subject: [OPS] Git Backup SUCCESS - yyyy-mm-dd

Failure Subject: [OPS] Git Backup ERROR - yyyy-mm-dd

Failure – Check the email and see what the error was. Check why the backups have failed and if it can be resolved. If not possible to resolve, escalate to Operations. If not resolved by Support and escalated to Operations, follow up hourly until resolved.

Resolved – Document what steps were taken to resolve the error and flag as resolved.

Database Maintenance

Email subject:

Subject: [OPS] DB maintenance SLOW

Slow queries

Support will receive alerts about any queries that are taking long to complete.

Support will need to log a bug.

The bug needs to be assigned to Development so that the query can be optimized.

Support to follow up with Development every 24 hours until resolved.

Intrusion Detection – AIDE

Email subject:

Success Subject: [OPS] AIDE SUCCESS – yyyy-mm-dd

Failure Subject: [OPS] AIDE ERROR – yyyy-mm-dd

Failure – Check if the failure is a result of false positives. If so, update the AIDE database and check that the problem has been resolved. If Support is unable to resolve the problem, escalate to Operations. If not resolved by Support and escalated to Operations, follow up hourly until resolved.

Resolved – Document what steps were taken to resolve the error and flag as resolved.

Intrusion Detection – chkrootkit

Email subject:

Success Subject: [OPS] chkrootkit SUCCESS – yyyy-mm-dd

Failure Subject: [OPS] chkrootkit ERROR – yyyy-mm-dd

Failure – Check if the failure is a result of false positives. If so, update the AIDE database and check that the problem has been resolved. If Support is unable to resolve the problem, escalate to Operations. If not resolved by Support and escalated to Operations, follow up hourly until resolved.

Resolved – Document what steps were taken to resolve the error and flag as resolved.

Virus Scanner

Email subject:

Success Subject: [OPS] AV SUCCESS – yyyy-mm-dd

Failure Subject: [OPS] AV ERROR – yyyy-mm-dd

Failure – If there was a failure to update the signatures, manually update the signatures. Otherwise, if a virus was detected, investigate the source, restore infected files from backup or delete them as appropriate.

Resolved – Document what steps were taken to resolve the error and flag as resolved.

SSH authentication

Email subject:

Success Subject: [OPS] SSH auth SUCCESS – yyyy-mm-dd

Failure Subject: [OPS] SSH auth ERROR – yyyy-mm-dd

SSH authentications from outside our network are logged to a log file.

Failure – Check the email and see what the error was. Escalate to Operations to identify and block the threat.

Resolved – Document what steps were taken to resolve the error and flag as resolved.

Firewall

Email subject:

Success Subject: [OPS] Firewall SUCCESS – yyyy-mm-dd

Failure Subject: [OPS] Firewall ERROR – yyyy-mm-dd

Failure – Check the email and see what the error was. Escalate to Operations to identify and block the threat.

Resolved – Flag as resolved once the engineer has documented his changes.

Internal Server Errors

Email subject:

Subject: [OPS] BBW Internal Server ERROR – yyyy-mm-dd

Support will receive alerts about an internal server error for the web interface.

Support will need to log a bug.

The bug needs to be assigned to Development so that the issue can be found and fixed.

Support to follow up with Development every 24 hours until resolved.

Ideally Internal Server Errors should be resolved the same day.

Lab Reports

- Missing labs: Subject: [Lab name] Recon
- Malformed XML: Subject: Old files@vault.radiology.co.za service is CRITICAL
- Malformed HL7 Subject: Old files@bbihs-prod4.bluebird.co.za service is CRITICAL

Scripts will send alerts to Support for issues encountered while processing Lab reports.

ADT Messages

- Missing ADT: Subject: [Hospital group name] HL7 Recon
- Malformed XML: Subject: Old files@vault.radiology.co.za service is CRITICAL

- Malformed HL7 Subject: Old files@bbihs-prod4.bluebird.co.za service is CRITICAL

Scripts will send alerts to Support for issues encountered while processing ADT reports.

Pharm. Messages

- Missing ADT: Subject: [Hospital group name] HL7 Recon
- Malformed XML: Subject: Old files@vault.radiology.co.za service is CRITICAL
- Malformed HL7 Subject: Old files@bbihs-prod4.bluebird.co.za service is CRITICAL

Scripts will send alerts to Support for issues encountered while processing Pharm. reports.

Bluebird Cloud Location

IMS uses AWS (Amazon Web Services) wherever possible. AWS enables superior scalability and robust hardware redundancy. AWS is a secure, durable technology platform with industry-recognized certifications and audits: PCI DSS Level 1, ISO 27001, FISMA Moderate, FedRAMP, HIPAA, and SOC 1 (formerly referred to as SAS 70 and/or SSAE 16) and SOC 2 audit reports. Their services and data centres have multiple layers of operational and physical security to ensure the integrity and safety of the data. For all these reasons, in countries where AWS is available, Amazon is our preferred platform.

Where AWS is not available or a client has specific requirements we own and operate Bluebird Server Clusters in local data centres. Southern African clients are serviced by the Bluebird Cape Town Server Cluster.

Securing the Bluebird SQL Servers

Whatever cloud option is chosen, this is how IMS implements the important security measures that have been shown to secure SQL Database Servers:

Securing the Bluebird SQL servers

IMS ensures that only necessary services are run on Bluebird SQL Servers. The servers are fire-walled and access is only allowed to services that need to be accessible. The Bluebird SQL Server Cluster is not directly accessible from outside the Bluebird data center network. Bluebird Operations access the servers via a VPN, generally from the Operations office. Offsite access creates an email alert to the Bluebird Support Team who verify that there was a legitimate reason for that offsite access. A host-base intrusion detection system is installed on the Bluebird Servers to detect modified system files and a virus scanner runs every 24 hours and scans for malware, hidden processes, hidden files, hidden network connections, etc.

Ensuring server OS and databases are kept up to date with patches

IMS patches the servers as patches are made available by the OS or database vendors.

Limiting Physical Access to the Bluebird SQL Servers

Amazon's data centers are all certified to the highest international standards, please see: https://aws.amazon.com/compliance/data-center/controls/

This paragraph therefore only applies to Bluebird Server Clusters located in a professional third party data centre. In this case, the servers are housed in locked server cabinets in locked data centres. To gain access to the data centre, Bluebird personnel are required to provide government issued identification and be chaperoned by a data centre agent whose access is via Biometrics (usually fingerprint scanner). The data centres have raised flooring to avoid flood damage and assist with cooling. They have fire suppression systems and portable fire extinguishers which are serviced regularly. The temperature is kept to between 12 and 18 degrees Celsius.

Segregating Bluebird Operations Users and limiting their Permissions

Only senior staff members, who have been certified, have admin access to the Bluebird SQL database. Other Bluebird Operations staff have restricted access. Separate User Roles are created with different access. Applications, including the Rails (End User Bluebird Application) and Rake Tasks each have separate accounts with different permissions. Each User has a unique username and password and these Users are only granted the access privileges they require to perform their role. SQL statements run by Bluebird Operations are logged for auditing purposes.

Using Coding Practices that avoid SQL Injection Attacks

IMS develops the applications that connect to the database in such a way as to avoid SQL injection attacks. This is accomplished by avoiding the construction of SQL statements by concatenating strings containing user-provided data and by using parameterized SQL queries.

Separating the Application Servers from the Database Servers

Applications that access the database are run on servers separate from the Bluebird Database Cluster. This limits exposure of the database servers if the application servers ever become compromised.

Implementing and Enforcing Secure Password Standards

In general, IMS requires Bluebird Users to utilise a complex password and requires that password to be changed every 30 days. Most hospitals choose the option to utilise their own Active Directory for Bluebird authentication and, in that case, password policy is implemented by the hospital.

Bluebird Database Maintenance

Periodic tasks

- **Restore an offsite backup** each month to a preconfigured test machine on AWS and Log in to ensure that the data is accessible.
- **Check all tables** in the database, from command line once a month: $ mysqlcheck -u root -p --check --databases dbname
- **Optimize all tables** in a database, from command line once a month: $ mysqlcheck -u root -p --optimize --databases dbname. The check command runs the optimize command. Completion of this procedure is reported monthly.

Database Backup

AWS

A snapshot of the database is created every night. There is a configurable retention period for how long to store the backups. We offer regional redundancy. With AWS "Multi-AZ Deployments" the second server is in standby mode and is promoted to the primary if the original primary becomes non-operational. Please see intelms.com/494 for further detail

Bluebird Server Clusters

This Bluebird Service is typically implemented as a database cluster with three nodes (with up to 15 as an option). If one server goes down the service will continue to work from the other two while the Bluebird Operations team repairs the failed hardware. The End User should not see any impact.

The database cluster in the datacenter replicates from there to a RDS instance on AWS. The RDS instance is backed up by using the built in RDS back up mechanisms, and we can promote it to the primary in the event of a failure of the database cluster in the datacenter. A local copy is also kept.

In the very unlikely event that the entire Bluebird Server Cluster is non operational, one is able to restore from backup. The restore procedure is to fetch the local backup, or, if necessary, the encrypted off-site backup, decrypt it and move it into place on the database server. When the database software starts up it automatically performs a check on the data files. The Bluebird Operations personnel check the database logs to make sure no problems were found with the restore. If the local backup can be used the process should be complete within less than 60 minutes.

IMS also operates Bluebird Servers on AWS in Australasia and North America. At the clients request multi zone AWS replication is available.

Monitoring

IMS uses Nagios to monitor the database cluster to make sure that the cluster nodes are synchronised with each other. In addition, the Support team monitors to ensure that they can connect to the cluster, that the time to connect is fast and that there are not too many connections to the database. Confirmation is documented in the day end support logs.

Maintenance Reviews

We review Maintenance procedures annually.

End User Account Creation

Initial creation of End Users is part of the New Hospital Take On Process documented in the **UserDetails.pdf** found here: www.bluebird.co.za/endusertakeon

After set up, modification of End Users, and new End User creation, is best done using Bluebird's secure **End User Creation Web Service**. A manual service is provided for hospitals that do not have the capability to utilize this web service.

Note:

Authentication of End Users at log-in, is via that hospitals Authentication Gateway (web service) which enables Bluebird to interact with the hospital's Active Directory. Most hospital groups prefer to develop their own Gateway based on this Bluebird specification:

If required, Intelligent Medical Systems can code the application for your hospital. This means that authentication is the responsibility of the client hospital. If an End User needs to be disabled, the hospital disables the account in their Active Directory which immediately prevents that End User from accessing Bluebird. It also means that password policy is set and implemented by the client hospital.

MANUAL TAKE-ON PROCESS

Hospitals that have not yet implemented Bluebird's User Creation Web service are required to submit the standardized excel spreadsheet found at: intelms.com/usertakeon

support@bluebird.co.za will only accept requests from a verified manager with a verified email address at the hospital group.

Bluebird Support will manually create the End User account with the details provided on the spreadsheet.

Manual requests to change a user's role will similarly, only be actioned, when submitted by the designated manager at the client hospital.

END USER CREATION WEB SERVICE

This Bluebird web service allows hospitals to securely submit new End User details or User modification instructions to Bluebird. The service, in effect, allows the hospital to control their End User details.

The specification for this service can be found here: intelms.com/UC

Further detail is provided in our Security Compliance document - page 3 BB Audit log.

Appendix 1: Instruction to Bluebird Staff to Minimize Potential Hacking

1. Never click on a link in an email.
2. Using an office computer or device for personal use (websites, Facebook, Snapchat etc.) is a **fireable offence**. As part of your duties you have privileged access (which always needs to be documented - see #5 below) to confidential patient information. Unauthorized websites may assist a hacker gain access to your authentication credentials.
3. Ensure your user name and **password is unique** when logging on to the live system. Passwords must never be shared or disclosed to anyone, including other Bluebird staff - another **fireable offence**.
4. Passwords must be changed at least every **30 days.**
5. Except in emergencies, access to production (live system) is only allowed from the office and only using an **office device** (never a personal device). If, in an emergency, live data is accessed from outside the office, this must be explained in the email in #6 below along with a description of the emergency.
6. Each time an employee accesses a server with identifiable patient data (live or backup), an email must be sent to access@intelms.com with the hospital group as the subject. The body of the email must have these 3 subsections
   - **Reason:** (he reason why access to confidential data was required e.g. QA on the live system to confirm that a recent update (name it) was working appropriately on production. Or a request from a User (name them) to review x information etc etc.)
   - **Process:** (What was done - for example Hospital x data was accessed)
   - **Resolution:** (most times this will just be "logged off and browser closed", but if data was downloaded to a PC one would have to explain what was done to ensure no unencrypted confidential information was left on the PC at the end of the process - ideally even encrypted data should be deleted and deleted from the trash)