Infosys Technical Security and Compliance Guide

1. Introduction

Infosys is a client–server application designed for healthcare organizations, integrating local Windows-based installations with web and mobile app extensions. The platform uses selective synchronization to ensure that only the minimum operational data required for functionality is transmitted, while sensitive or identifiable patient data remains within the organization's secured environment. This document details the data storage, security controls, compliance framework, monitoring mechanisms, and vendor responsibilities relevant to hospital IT and compliance teams.

2. Hosting and Security Framework

Server Hosting: HostGator shared platform (Database-as-a-Service).
Encryption: TLS 1.3 for all inbound and outbound traffic.
Validation: TLS configuration independently tested (see: cdn77 TLS test).
Compliance Objective: Prevent transmission of PHI and ensure operational data is protected at rest and in transit.

3. Data Storage and Synchronization

3.1 Local Installation (Windows PC)
- Data stored in a structured main folder with subfolders for each subprogram.
- Access restricted to organizational network/domain administrators.
- No external transmission of local data except selectively synced values.

3.2 Web and Mobile App Extensions
- Selective data sync to HostGator MySQL database via HTTPS and PHP scripts.
- HIPAA Safeguard: No PHI synced.
- Example: Patient Tracker only syncs wait times, queue length, and alarm status; patient names excluded.
- Data transmitted via parameterized HTTPS requests validated server-side.
- MFA required for administrative database access.

3.3 Example of Selective Sync
- Not Synced: Infection Control data (remains on local/shared drive).
- Synced: Device names, queue metrics, temperature readings, and metadata.

4. Access Control

4.1 Windows PC Installation
- No Access Control: Employee Directory, Phone Directory, Calendar.
- Full Access Control: Occupational Health Finance Manager, Interpreter Requests, Lab Standing Orders (username/password + admin password).
- Selective Access Control: MSDS Finder, My OTC Meds, Attendance Tracker (tiered user/admin roles).

4.2 Web and Mobile Extensions
- Login requires Facility Code, Username, and Password.
- Security features:
• Auto logout after 5 minutes inactivity.
• Credentials synced with Windows installation (removal from PC revokes web/app access).
• Credential recovery/reset available.

5. System Architecture

Client-Side:
- Web built with HTML + JavaScript.
- Mobile apps (iOS/Android) are wrapped web apps.
- JavaScript structures HTTPS requests with facility/user context.

Server-Side:
- PHP scripts handle all database interaction.
- Database credentials stored server-side, never exposed to clients.
- Input validation enforces structured command syntax.

Command Listener:
- Infosys PC client polls database for command strings.
- Commands generate structured .dat files within local shared directories for real-time updates.

6. Data Retention

- Local (PC): Data retention depends on subprogram; some purge/archive automatically, most retain indefinitely.
- Web/Mobile (HostGator): Data retained indefinitely. Login/account information deleted upon deactivation.
- Backups: Example: CMH facility performs daily network drive backups.

7. Monitoring, Logging, and Auditability

Infosys maintains layered monitoring for accountability and compliance:
- Login History: Tracks successful logins (user, device, facility, timestamp, outcome).
- Failed Login Tracker: Locks account after 10 failed attempts; requires admin reactivation.
- Daily Sync Logs: Records success/failure of sync events with error details.
- Error Reporting: Critical errors auto-emailed to administrators and logged in-app.
- Web Request Logs: Records all client-side requests (endpoint, parameters, user context, response).
- User Activity Log: Tracks module usage, actions, and timestamps.
- Retention: Logs stored indefinitely on shared drives, subject to local IT backup policy.

8. Security and Compliance

8.1 Data Protection
- End-to-end encryption (TLS 1.3).
- Only operational (non-PHI) data synced externally.
- PHI remains within hospital-controlled environment.

8.2 Authentication & Authorization
- Server-side credentials not client-exposed.
- MFA for HostGator database access.
- Auto account lockout after failed attempts (Windows, Web, App).
- Web sessions expire after 5 minutes idle.

8.3 Unauthorized Access Response
- Locked accounts apply across all platforms.
- Admin response options: Reactivate, Reset Password, Remove User.

8.4 Compliance Alignment
- HIPAA: Designed with safeguards ensuring PHI remains local; system aligns with HIPAA security principles.
- HITECH: No formal certification completed.
- BAA: Active Business Associate Agreement (BAA) with Hillcrest; available for review.

9. Software Updates & Patch Management

- Updates released as needed (security patches, features, bug fixes).
- Update distribution over TLS 1.3 from secure host.
- Daily sync checks for new versions.
- Execution model: Local copy of Infosys.exe run from temp directory to prevent concurrency issues.

10. Reporting & Regulatory Support

- Custom Reports: Available for compliance or operational needs.
- Audit Readiness: Logs and monitoring provide traceability for inspections.
- Export: Logs viewable in-app; export function can be implemented if required.

11. Summary

Infosys enforces a selective synchronization, encrypted transmission, and role-based access model to ensure:
- PHI never leaves the hospital-controlled environment.
- All operational data in transit and at rest is protected by TLS 1.3.
- Multi-layered logging, monitoring, and access controls support audit readiness.
- Updates, patches, and backups align with standard healthcare IT requirements.

This architecture provides a secure, compliant, and auditable framework suitable for deployment in hospital IT environments.