

Patient-Staff Communications

Impact on Healthcare Facility Information Systems



imagination at work

Network communications is the de-facto standard for easily interfacing disparate systems.

Patient-staff communications is less and less a stand-alone nurse call product. Today's healthcare enterprises are requiring interfaces to pagers, wireless phone systems, cellular phones, staff location systems, patient record systems, bed management systems, and call/staff response activity reporting. Network communications is the de-facto standard for easily interfacing these disparate systems. Desktop workstations are the logical means of displaying correlated data from these systems when space is at a premium and mobile/remote access is imperative.

Patient-staff communications purchase approval, installation and maintenance, long the "exclusive" domain of Clinical/Biomedical Engineering, is now beginning to cross into the jurisdiction of other departments. Information Systems, networking, desktop, servers, and telecommunications can each involve a separate department, and the installed patient-staff communications may affect each of them. Information sharing and cooperation are the keys to a smooth installation.

These groups are typically extremely knowledgeable, well organized, adhere to strict procedures, and have concerns in many areas. Answers are often needed to each of the following details:

- Hardware platform (desktop specs, server specs, hardware sourcing)
- Software platform (OS, database)
- Interoperability (sharing desktops, ADT interface, sub-system integration)
- Maintenance (preventative, backups, storage requirements)
- Security (sharing privileges, logins, password protection, virus protection, firewalls)
- Network requirements (bandwidth, IP addressing, naming conventions, VLANs, dedicated LANs)
- Reliability (supervision, error reporting, MTBF)
- Business Continuity (backup and restore)
- Scalability
- Upgrade and maintenance options for future growth

GE Patient-staff Communications Network Architecture

GE Security's Communication Hub architecture (Figure 1) takes full advantage of the power of networking to integrate multiple sources of information to a variety of output devices and applications. This single server administers the licensing and registration of each client, manages real-time transactions, and maintains global status, configuration, and diagnostic information for easy backup and recovery.

Each client registers into the hub's Transaction Server with subscriptions (built into the software) for specific event types. When an application publishes an event, it does not need to know of every client that subscribes to the event. The hub acknowledges its receipt of the event, and insures that it is delivered to all appropriate subscribers or informs the publisher of a failure. This facilitates system expansion and flexibility, the addition of new client types, and limits network traffic by delivering on a "need to know" basis.

While the hub's Transaction Server is appropriate for real-time transactions, additional means are necessary to keep applications in sync with each other over the long term. As applications turn off and on, previous transactions are no longer available, and a full current status must be retrieved. MS SQL Server is used to accomplish this in a fully scalable implementation.

The communications core also makes extensive use of browser technology (ASP, IIS) to enable thin client applications to run on any IE6 or greater PC, making enterprise distribution and maintenance of the GE Application Suite across a facility campus feasible.

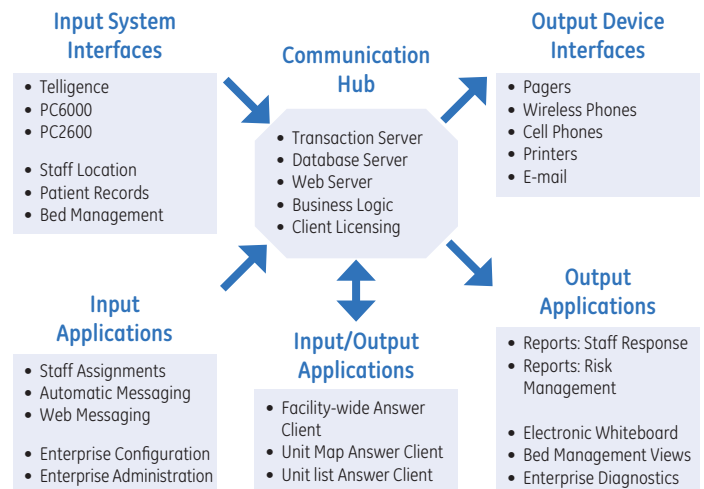


Figure 1 Interface Architecture

Regulatory Concerns

Per most state, regional, and local Authority Having Jurisdiction (AHJ) building codes, any acute care facility must include a fundamental patient-staff communications system listed to a nationally recognized life safety standard. UL 1069 is the de-facto testing and performance standard, and is referenced whether the listing mark is via UL or ETL. Within 1069, UL has clearly defined what constitutes fundamental patient-staff communications system. This includes the patient station and master, the equipment required to place a call from the patient room (pillow speakers, call cords, patient stations, staff stations) and announce that call at the nurse station (master stations, annunciators), and everything in between (centrals, hubs, power supplies...). Also included is any equipment used to cancel a patient call.

A Listed patient-staff communications system is required to provide the following fundamental functions:

1. Call annunciation at a nurse's station (audible and visual)
2. Call annunciation at a dome light
3. Call placed indicator on the patient station
4. Zone annunciation (audible and visual)
5. Call reset/cancellation

Life safety listing is not required (nor is it feasible to obtain) for the supplemental portion of the system which performs non-fundamental or redundant annunciation and may rely on facility network or telephony equipment. Therefore, all PC and network-related functions are considered supplemental to the patient-staff communications system, and patient-staff communications must include electrical isolation at any point at which a physical interface to the supplemental devices exists.

Fundamental patient-staff communications is designed to be inherently more reliable than the supplemental functions. System users should have a clear understanding of the fundamental patient-staff communications system capabilities, and should be prepared to operate using only that portion of the system should any problems arise within the supplemental infrastructure.

For additional details, refer to GE White Papers entitled:

“Integrating Patient-staff communications to Wireless Phone Systems”

“Integrating Patient-staff communications to Staff Location Systems”

PC and Application Related Frequently Asked Questions

What OS do the GE applications require?

These are subject to change as newly released OS platforms mature. As of the beginning of 2006, all server components run on Windows 2003 Server for facilities looking for the highest quality solution, or on Windows XP for facilities looking for a more cost effective solution. Current desktop applications run on Windows XP. Thin clients just need a machine running IE6 or greater, and windows '98 or greater.

What hardware platform specifications are required?

These change annually, and are available through our technical documentation department. They are typically mid-level servers and desktops, and can be purchased through GE, through the authorized channel partner, or by the facility itself.

Can the applications run on the facility's existing desktops?

Yes. All non-24/7 viewing, messaging, and browser-based applications are typically installed on existing machines to save front-end cost, ongoing maintenance, and valuable desk space. While 24/7 applications can also share a host, NetBoard and Call Answering Clients often are installed on dedicated desktops. Legacy ProCare 6000 Video Masters and servers in particular require dedicated machines. Centralized Answering Clients are also typically dedicated, as they require custom hardware installation, and are frequently in 24/7 use.

Can the facility purchase its own PC's?

Yes. While some customers prefer to purchase a turnkey system from the authorized GE Channel Partner, many have established purchasing agreements, hardware preferences, and configuration and application standards to simplify deployment and maintenance. Facilities may purchase their own PC's as long as they meet the GE specifications, and that they load their own images onto them.

What are the security implications of the applications?

Since many of the applications are supplemental to the patient-staff communications/life safety system, they run 24/7 with multiple potential users at each workstation. Logins are therefore automated, and shared by all users of that host. The system contains multiple levels of passwords and privileges to minimize the chance of patient-staff communications disruption by unauthorized personnel, but the IS group should implement the OS security measures as on any other PC's within the facility.

Impact on Healthcare Facility Information Systems

Other applications, including some types of viewing and reporting, are typically not run 24/7. They may implement login procedures to restrict viewing privileges and to save user preferences.

New GE desktop applications invoke a user account, so do not require administrator privileges. Legacy applications, including Video Master, ProCare 6000 Bridge, and Central Answering require administrative privileges to read / write from the registry. Extra measures may be required by the desktop department to insure that this does not provide access to otherwise restricted functions across the network.

Is virus protection included?

Virus protection is an ongoing maintenance issue. Rather than install a package that is incompatible with the facility's current anti-virus procedures, the choice, installation, and maintenance of an anti-virus plan is left to the jurisdiction of the facility.

Are Security Patches included?

Security patches are an ongoing maintenance issue. Rather than invoke a process that is incompatible with the facility's current security procedures, the timing, installation, and maintenance of

a security patch plan is left to the jurisdiction of the facility.

Does the system have any HIPAA compliance issues?

HIPAA plays a role in how the systems should be set up. Some of GE's 24/7 patient-staff communications views do not automatically log-off after idle time, nor do they require a login. Each customer must decide what fields are appropriate for display based on the location of the PC and others' accessibility to it. All applications have fully configurable displays to include or exclude any sensitive fields as needed.

What database applications are involved?

GE's "PC Connect" and ESM host applications utilize MS SQL Server for all applications. Patient Record and Bed Management interfaces use MS SQL Server to store patient and bed data for access by the desktop clients. Automatic Location interface uses MS Access to store transactions for real time status, and optionally MS SQL Server to store transactions for reporting. Legacy applications, including ProCare Video Masters use a variety of solutions to store real time data.

What are the backup and ongoing maintenance requirements for the system?

SQL Server automatic backup procedures should be implemented for all "PC Connect", ESM and ADT database servers. Each client should perform a backup of its configuration data through the menu options upon installation and any reconfiguration. GE recommends both electronic and hard copies maintained on-site and with the authorized GE Channel Partner. The location server requires periodic purging of the database if logging is enabled, to prevent the Access database from growing beyond its capabilities.

Where are the PC's located?

Any middleware application PC (no day to day user interface) should be located in a secure area. This includes servers, and bridge applications to third party systems (phones, pagers, etc.). These are easiest to maintain if they are all together in a "server farm" in the IS department. One exception to this occurs frequently with third party systems that require an RS232 connection. Bridge application PC's may be located next to the paging system, to eliminate the need for custom cabling and short-haul modems in those cases.

Network Related Frequently Asked Questions

Can the system run on the facility LAN, or does it need a dedicated network?

The supplemental portion of the patient-staff communications system, including phones, pagers, PC clients, and interfaces, can run on the facility LAN. Occasionally, customers prefer the security of running on a dedicated LAN, on dedicated segments, or on a VLAN. That is strictly up to your networking department. There is no requirement to deploy any of these restrictions.

Automatic Location (by Versus Technology) is one exception to this situation, and requires a dedicated LAN, segments, or a VLAN with 2 network ports on its server.

To meet NRTL (Nationally Recognized Testing Lab) standards, fundamental patient-staff communications requires a dedicated network with UL 1069 listed components. This is not an issue with many older non-network based fundamental patient-staff communications. GE's new Telligence patient-staff communications leads the industry as the first IP based patient-staff communications. While it does run on a LAN, it must be a dedicated LAN using GE UL 1069 listed switches, routers, and power supplies. As other patient-staff communications vendors progress to IP based systems, they will face similar regulatory issues and will have similar solutions.

Impact on Healthcare Facility Information Systems

Are there any special requirements of the LAN?

Yes, location concentrators must run on a 10Mbps segment: they will not perform properly at 100Mbps. This is the reason that the location system should be isolated on its own VLAN or dedicated segments.

What traffic loads will the system place on the network?

Real-time Patient-staff communications transaction traffic through the ESM/PC Connect server is typically small packets and relatively infrequent bursts. The system architecture and ESM/PC Connect ensure that the traffic is all point to point (no broadcasts) to minimize the traffic loads.

Database applications (HL7 ADT Bridge, Centralized Answering Client, Bed Management, Net-Board, PC Assignments, and ListView and MapView Answer Clients) will perform a background resynch to records in the database 1-4 times per minute, again with small packets.

Location traffic typically results in 80% to 90% of the total GE/Dukane system traffic. It is steady, and directly related to the number of active badges and concentrators. Each badge sends out a message every 3 seconds, and concentrators bundle them into packets which are sent across the network every 2 seconds.

Even a fully loaded system sends out very little traffic from a network bandwidth perspective. A typical nursing unit generates 0.00084Mbps (0.0084% load on a 10Mbps backbone). With location and HL7 interface, this can jump to .0057 Mbps, or 0.057% of a 10Mbps LAN.) Appendix C shows calculation details for each scenario.

What communications protocol does the system use?

Patient-staff communications uses a WinSock control to implement TCP/IP protocol. Location uses a combination of UDP (from the embedded software residing in the concentrators) and TCP/IP to all PC clients.

What are my ongoing IT support needs for this system?

Anti-Virus updates, and Microsoft OS and Database updates are the responsibility of the facility.

Appendix A HIPAA Standards Compliance Chart

Note: Each of the privacy and security features identified below have been specified as desirable by some GE customers. Per individual facility requirements, some features are more important than others, and certain features may mitigate the risks caused by the absence of others. The combination of available features is more important than any single feature.

| HIPAA | Compliance | Problems/Issues Regarding Compliance |
|--|------------|--|
| Each user has an individual login: No shared logins | Yes | 24/7 applications count as a user: i.e. PEDS Desk |
| Caregivers and non-caregivers have different levels of system access. Caregivers (people who are actually treating the patient) can get into sections of the patient record that non-caregivers cannot. Non-caregivers are only able to see the types of patient data required in order to do their job. ("Minimum necessary" rule, part of Role-Based Access.) | Yes | System privileges are granted per login by the administrator |
| Users are only able to see patients assigned to them (or to their team / unit / facility). The system restricts users from accessing a patient's record unless the patient has been assigned to that user (or their team or facility). If a user needs to access a patient not assigned to them, the user is required to declare a relationship with the patient before access is granted. ("Need to know" rule, part of Role-Based Access.) | Yes | Nursing unit privileges are granted per login by the administrator |
| Physicians are only able to view the specific encounters (episodes of care) they are connected to, or which the patient has authorized them to see. The system requires physicians to "declare a relationship" with each encounter before being granted access to that encounter. ("Authorization requirement.") | NA | System typically not used by physicians |
| If the application produces patient directories, or other widely-distributed lists of patients, the application contains functionality for not displaying the names of "no information" patients (those who have requested not to appear in patient directories). | Yes | No patient directories or distributed patient lists available. Unit room lists at nurse station 24/7 applications are exceptions |
| If the application contains patient addresses, it contains functionality to support the use of a temporary or secondary address for all correspondence with the patient. | Yes | No patient addresses are available |
| The application "times out" a user session after a specified period of non-use (no greater than 15 minutes if the application is used on shared Clinical workstations). | Yes | Nurse station 24/7 applications are obvious exceptions |
| If the application contains auto-faxing functionality, the ability to create or update fax numbers is restricted to designated individuals. The system keeps a log of all auto-faxes. | Yes | No auto-faxing available |
| Encrypted Internet transmission of individually identifiable patient data. | Yes | No internet transmission available |
| User passwords are set to automatically expire periodically. | No | |
| 3 month Patient Record Access audit trail showing login, which patient's record, and the date and time accessed. | No | |
| 3 month Patient Record Printout audit trail showing login, which patient's record, and the date and time printed. | No | |
| 3 month Individually Identifiable Patient Report audit trail showing login, which report and patient, and the date and time printed. | No | |

Impact on Healthcare Facility Information Systems

Appendix B IS Standards Compliance Charts

Note: Each of the privacy and security features identified below have been specified as desirable by some GE customers. Per individual facility requirements, some features are more important than others, and certain features may mitigate the risks caused by the absence of others. The combination of available features is more important than any single feature.

| Platform | Compliance | Comments |
|--|------------|--|
| Current OS Versions and Service packs | Yes | Servers: Microsoft 2003 Server Desktops: Microsoft XP Professional |
| Facility Standard Server Hardware | Yes | |
| Facility Standard Server Image | TBD | Specifications compatible with most images |
| Facility Standard Desktop Hardware | Yes | |
| Facility Standard Desktop Image | TBD | Specifications compatible with most images |
| Blade Servers | Yes | |
| Server Clusters | Yes | |
| Shared Database | No | |
| Multiple applications on one Patient Record port | Yes | |
| Multiple facilities on one Patient Record Port | No | |
| Multiple facilities on one reporting package | No | |
| Multiple Facilities on one server | No | |
| Facility domain Standards | Yes | No domain restrictions for GE |
| Web Enabled | Yes | Software is intranet enabled. Internet access is up to the facility. |
| CCOW compliant | No | |
| Communications Protocol | TCP/IP | |
| Ethernet switch, subnet, router environment | Yes | |
| All server applications run as a service | No | Some, but not all. As GE moves forward, newer applications are predominantly developed as services. |
| Thin-Client | Partial | Mix of resident and browser applications |
| Citrix Compatible | TBD | Determination is up to the facility |
| VMware certified | No | |
| Desktops run without administrator privileges | Yes | Except legacy "Video Master" application Requires specific topology (All bridge hosts in secured areas) |

| Database | Compliance | Comments |
|--|------------|---|
| Current DB Versions and Service Packs | Yes | Servers: Microsoft SQL Server 2005 Desktops: Microsoft MSDE |
| Automatic Failure notification by e-mail | Yes | |
| Automatic Maintenance (Backup) | Yes | Nightly |
| Can others access the database (ODBC) | No | The database design and updates are proprietary, and fully tested with GE applications. It is not intended for unauthorized access. |

| Security of Data Storage & Transmission | Compliance: | Comments |
|---|-------------|--|
| Server storage encryption (patient or financial data) | No | |
| Workstation storage encryption (patient or financial data) | Yes | All data storage is in servers |
| Internet transmission encryption (patient or financial data) | Yes | No internet communication is available within the system |
| Remote access security (preferably via VPN, dedicated line, or strong password protection and modem controls.) | Yes | Remote Access Security is determined by the facility |
| Encryption of wireless transmissions (including Cisco's LEAP/TKIP technology, or PEAP (stronger encryption and authentication than WEP)) | NA | Wireless transmission protocols are determined by the wireless vendor. |
| List of all ports required by the system and the application(s) associated | Yes | Pocket Paging / Emergin / ascom phones: <ul style="list-style-type: none"> • Industry standard RS232 TAP 1.8 protocol, continuous connection Spectralink Wireless Phone: <ul style="list-style-type: none"> • Spectralink proprietary RS232 OAI Protocol Other Wireless Phone: <ul style="list-style-type: none"> • Industry standard TCP/IP NEMA protocol Patient Records - listen only: <ul style="list-style-type: none"> • Industry standard HL7 TCP/IP port Bed Management: <ul style="list-style-type: none"> • Industry standard HL7 TCP/IP port PBX phone interface: <ul style="list-style-type: none"> • Analog phone line with loop drop disconnect Automatic Location system: <ul style="list-style-type: none"> • Versus proprietary TCP/IP |
| Facility Port Numbering Standards | TBD | Default Ports as follows: 25201 ESM Clients 1433 ESM SQL 2000 Versus 2005 Versus 2200 PC 6K manager 2222 Messaging 2223 Patient Record Bridge 2224 Assignments 2225 Whiteboard |
| Encryption of network wireless transmissions (preferably Cisco's LEAP/TKIP technology, or PEAP (stronger encryption and authentication than WEP)) | Yes | Network wireless transmissions are under the jurisdiction of the facility |

| Maintenance | Compliance | Comments |
|---|------------|---|
| Security Patch management policy | Yes | Security patches are under the jurisdiction of the facility |
| Anti-virus policy | Yes | Anti-virus protection is under the jurisdiction of the facility |
| Maintenance agreements | Yes | Maintenance agreements are available, per the final contract |
| Service agreements | Yes | Service agreements are available, per the final contract |
| Performance Monitoring (disk, memory, CPU utilization, or Database) | Yes | SQL Server based DB monitoring |
| Automatic Failure Notification by Pager | Yes | Logged failure events anywhere within the system |
| Automatic Failure notification by e-mail | Yes | SQL Server based DB failure |
| Automatic Backup and Recovery | Yes | SQL Server based backups |
| Disaster Recovery Plan | Yes | Backup and restore guidelines are published by GE. Specific plans are under the jurisdiction of the facility. |
| Remote Access Available | Yes | Under the jurisdiction of the facility |

Impact on Healthcare Facility Information Systems

| User Authentication | Compliance: | Comments |
|--|-------------|--|
| Unique individual login ID for each user | Yes | |
| System allows 2+6 username format (2 first name, 6 last name) | Yes | |
| System stores password in encrypted format | Yes | |
| Automatic logoff after specified time | Yes | Except 24/7 applications at the nurse station |
| Screensaver | Yes | This is accomplished by the automatic logoff above |
| Old passwords expire immediately upon new one being set | Yes | |
| Security administrator can view user's current password | Yes | |
| User initiated password change | Yes | |
| Password Encryption | No | Passwords are displayed as '*'s on screen |
| Periodic password change enforced (no reuse) | No | |
| Strong passwords (alpha, numeric, & special characters OK, no 3x repeating characters, no user name or ID) | No | Passwords are unrestricted |
| Minimum password length enforced (6 character minimum) | No | Passwords are unrestricted |
| User account is locked after x invalid password attempts | No | |
| User notified of invalid password attempts | No | |
| Alternatives to passwords (biometrics, smart cards, hardware tokens, digital certificates) | No | |
| Accounts automatically disabled after extended non-use | No | |

| Access Controls | Compliance: | Comments |
|--|-------------|----------|
| Access to files or online functions can be restricted based on User ID, Group, or Role | Yes | |
| Access profiles can be based on Role or Group, or User ID | Yes | |
| Security can limit which screens a user can access. | Yes | |
| Security can limit which individual records a user can access. | Yes | |
| Security can limit which fields a user can access on a screen. | Yes | |
| Access rights can be based on multiple parameters (e.g. combinations of UserID, role, physical location, function, etc.) | Yes | |

| Logging and Monitoring | Compliance: | Comments |
|--|-------------|----------|
| User self-audit.(automatic display of "last access date") | No | |
| Audit trail of read-access | No | |
| Audit trail of write-access | No | |
| Audit trail of use of print functions within the application | No | |
| Audit trail of account activity (use of applications) | No | |
| Formatted reports to display or print the audit trail | No | |
| Formatted reports to display security violations | No | |

Appendix C Theoretical Patient-staff communications Network Loading

| Output type | System Servers | Unit Desktop | Centralized Answering | Reporting Server | Wireless Phone IF | Pager Interface | Census Board | Location View | Event Totals | Bandwidth (Mbps) | Bandwidth % (10Mbps LAN) |
|--|----------------|--------------|-----------------------|------------------|-------------------|-----------------|--------------|---------------|--------------|------------------|-------------------------------|
| Quantity | x | 1 | 3 | 1 | 1 | 1 | 1 | 3 | | | |
| Peak actions / hour (typical 25 bed unit) | | | | | | | | | | | |
| Patient Call w/ Auto-Messaging | 25 | 150 | 0 | 150 | 150 | 500 | 50 | 50 | 0 | 1050 | |
| Answer | 25 | 200 | 0 | 300 | 100 | 500 | 0 | 0 | 0 | 1100 | |
| Remind Set | 15 | 60 | 0 | 180 | 60 | 0 | 0 | 50 | 0 | 350 | |
| Manual Messaging | 20 | 80 | 0 | 0 | 80 | 320 | 40 | 0 | 0 | 520 | |
| Total Patient-staff communications | | 490 | 0 | 630 | 390 | 1320 | 90 | 100 | 0 | 3020 | 0.00084 0.0084% |
| HL7 Census Transaction | 10 | 40 | 0 | 0 | 20 | 0 | 0 | 0 | 0 | 60 | |
| Patient Record DB Update | NA | 360 | 480 | 1440 | 120 | 0 | 0 | 120 | 0 | 2160 | |
| Total Patient Records | | 400 | 480 | 1440 | 140 | 0 | 0 | 120 | 0 | 2580 | 0.00072 0.0072% |
| Concentrator (1) Transmissions | 1800 | 3600 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3600 | |
| Location Movements | 600 | 1200 | 1200 | 3600 | 600 | 0 | 0 | 1200 | 3600 | 11400 | |
| Total Location | | 4800 | 1200 | 3600 | 600 | 0 | 0 | 1200 | 3600 | 15000 | 0.0042 0.042% |
| Grand Totals | | 5690 | 1680 | 5670 | 1130 | 1320 | 90 | 1420 | 3600 | 20600 | 0.0057 0.057% |

Notes:

1. Assumes 1.0 kByte message packets
2. Assumes 600 badge movements
3. Calculations = # msgs x # packets/msg x # destinations x events
4. Calculations assume max load case (wireless phones, central answering station, or unit console)

GE
Security
Sound and Communications

U.S.
T 888 GE SECURITY
F 800 483 2495

Canada
T 519 376 2430
F 519 376 7258

www.gesecurity.com

© 2006 General Electric Company
All Rights Reserved

Telligence is a registered trademark
of GE Security, Inc.



imagination at work