General DataComm
The Best Connections in the Business

Connectivity and Internetworking in the Healthcare Industry HIPAA Compliance

Introduction

The first-ever federal privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers took effect on April 14, 2003. Developed by the Department of Health and Human Services (HHS), these new standards provide patients with access to their medical records and more control over how their personal health information is used and disclosed. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes provisions designed to encourage electronic transactions and also requires new safeguards to protect the security and confidentiality of health information. All health insurers, pharmacies, doctors and other health care providers are required to comply with these federal standards, which went into effect April 14, 2003. (Paraphrased from the U.S. Department of Health and Human Services)

In this paper, we will identify and discuss some of the issues associated with the HIPAA requirements and how technologies available today from GDC can be part of a comprehensive network design and security policy to ensure safe and secure communications between the various entities and components in the Healthcare Industry.

Overview

Few industries have greater security concerns than healthcare. From regulators and insurers to patients and the public, healthcare providers are under tremendous pressure to keep medical data safe and confidential. This can be a daunting task considering the sheer number of entities with electronic access to patient medical information. Some of these include:

- Physicians and Nurses now enter patient information and diagnosis electronically to a centralized computer.
- Coders require electronic access to patient information to apply ICD9 and CPT codes for billing purposes.
- Insurance companies need electronic access to patient information for payment or reimbursement.

To meet security mandates, healthcare providers must protect all aspects of their networking operations; both from internal and external means. They have to defend the enterprise network against intruders intent on accessing medical information. They must safeguard communications with other medical facilities, pharmacies, and insurers. A security breach anywhere has costly consequences and erodes patient confidence.

Small and Medium Providers

Small and medium-sized providers, however, lack the substantial IT staff and budgets of large enterprises. This means that, although they require the same robust safeguards as larger medical organizations, their solutions must be affordable and easy to deploy and** manage.

Figure 1 depicts a typical Physician Group Practice and how products such as GDC's InnovX FastRoute and InnovX FastSwitch can provide intrusion security with port and MAC based security and filtering from both internal and external security threats.

Physicians Group Practice

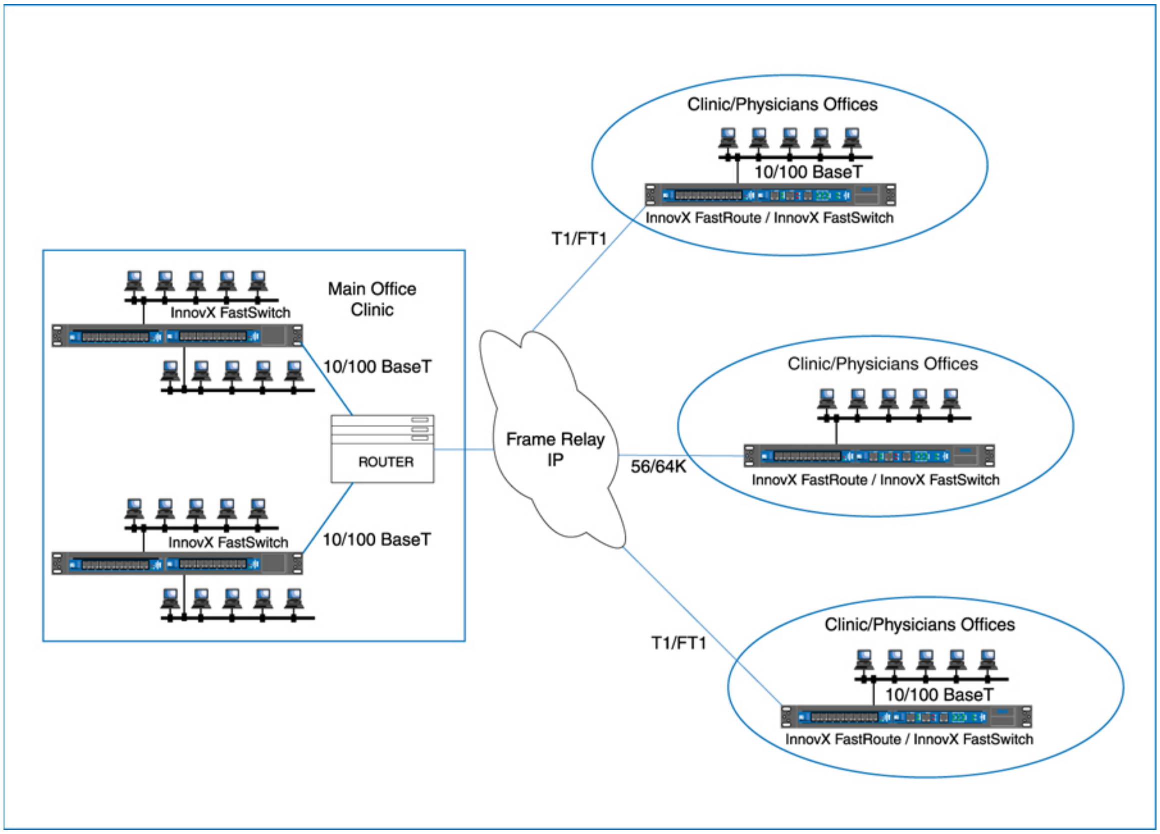
Clinic/Physicians Offices
10/100 BaseT
InnovX FastRoute / InnovX FastSwitch
T1/FT1
InnovX FastSwitch
Main Office
Clinic
10/100 BaseT
Frame Relay
IP
Clinic/Physicians Offices
ROUTER
56/64K
InnovX FastRoute / InnovX FastSwitch
InnovX FastSwitch
10/100 BaseT
T1/FT1
Clinic/Physicians Offices
10/100 BaseT
InnovX FastRoute / InnovX FastSwitch

Fig. 1

Large Providers

Large hospitals and medical organizations are under great pressure as well to contain, if not lower their costs to make healthcare services more affordable and to sustain profitability while maintaining HIPAA compliance. To do so, they must enhance communications, streamline operations, improve efficiencies, and reduce operating expenses.

These healthcare organizations must deliver reliable, high-speed networking throughout the enterprise, including distributed sites. Caregivers need to quickly capture and share data, exchange large files, and use timesaving technologies.

They must expedite back-office processing and speed transactions with insurers, vendors, and patients. Moreover, healthcare organizations require connectivity solutions that are easy to use relieve pressure on IT budgets, and reduce the time needed for staff training.

For large healthcare organizations, these objectives are particularly challenging. They must support extensive medical services and larger, more distributed staffs, which demands robust communications systems that are reliable, versatile, and easy to manage

To improve services, healthcare enterprises must ensure that doctors and nurses can quickly access patient records, x-rays, test results, insurance forms, billing information, and medical research. They need to unify their facilities into seamless communication infrastructures, integrating disparate databases and systems. They must offer staff easy access to labs, pharmacies, insurance providers, medical devices, and other resources, empowering them to make faster and more informed decisions. Providers must offer tele-radiology and videoconferencing so staff can rapidly collaborate with colleagues, regardless of their geographical dispersion, and access specialized procedures and expertise.

Figure 2 illustrates a Hospital Campus LAN which is comprised of a Hospital and associated professional buildings with physicians offices, labs, and patient services.

Hospital Campus LAN

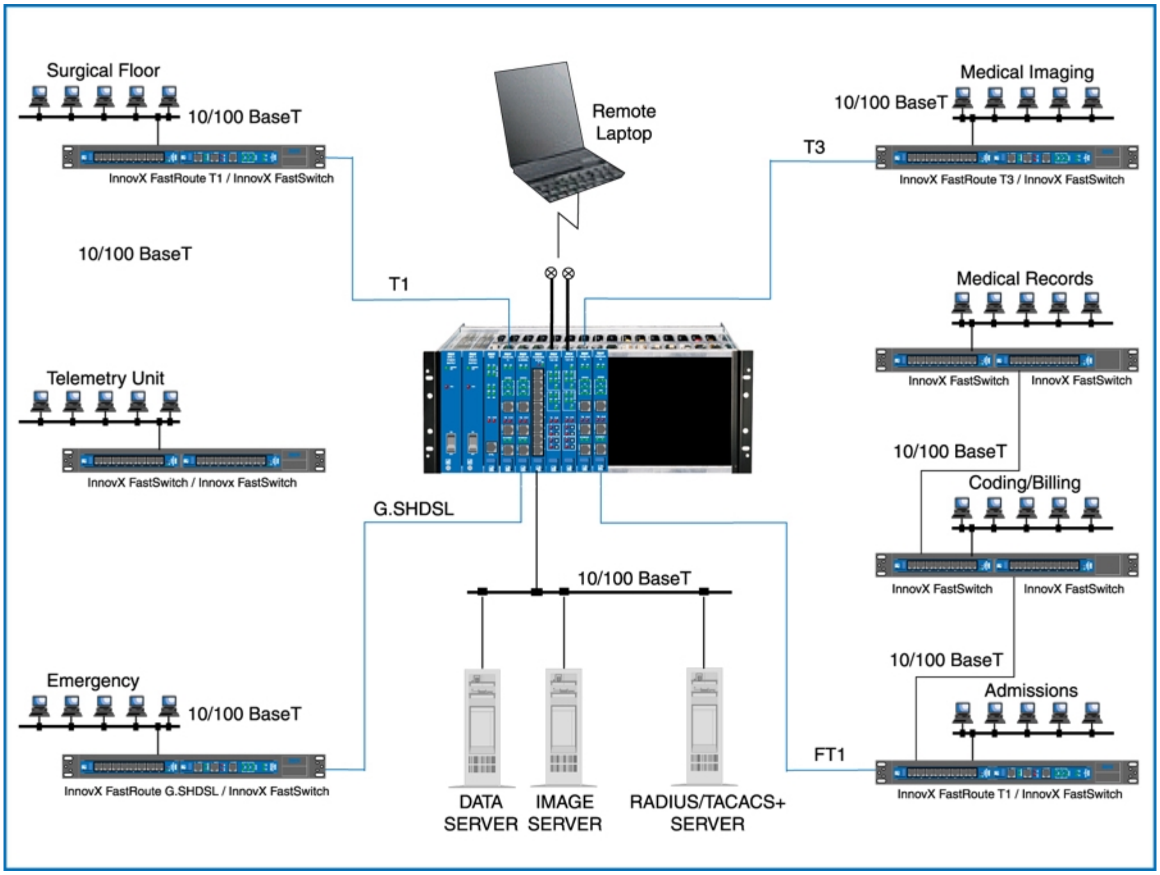

Fig. 2

Growth & Flexibility

Healthcare providers require high-value communications systems that are scalable, flexible, and inexpensive to own. There can be no compromise between a provider's financial needs and the needs of its patients. Solutions must be cost-effective for high returns on investment. They must expand easily and affordably to support growth and new technologies. They must be resilient to ensure the continuity of critical medical care. Should disaster strike, these systems must deliver the versatility that allows services to be restored quickly.

Due to trends like aging populations, medical advances, and new technologies, healthcare providers require versatile networking solutions that can adapt to change without substantial costs. They need standards-based systems to avoid interoperability issues with legacy or future systems. Their networks should support the delivery of care where and when it is needed across a range of devices and locations.

Moreover, providers' networks must scale cost-effectively to support new users and future generations of medical and business applications. They need to provide bandwidth and functionality as needed to deliver web-based systems, telemedicine, and other healthcare innovations. Their solutions must be resilient and always available, ensuring the continuity of essential medical services. When disaster does strike, they must be able to restore communications rapidly. Their networks must be all of this as well as comply with the HIPAA requirement dictating:

- Audit Trail
- Authentication
- Intrusion Detection both host based and on the network
- Denial of Service, both internal and external
- Disaster Recovery

Conclusion

General DataComm products provide this flexibility and fail safe resiliency by applying intrusion protection at the edge of the network. GDC has incorporated features such as IronGate security in all LAN and LAN access devices that insure protection against security breaches from within or from outside the physical network location. GDC's line of routers, Ethernet switches and LAN extension devices also support robust authentication such as TACAC+, and like GDC's modems with Steadfast security and RADIUS, they offer the same type of multi-level protection against internal or external physical intrusion.

General DataComm
The Best Connections in the Business

General DataComm, Inc. WORLD HEADQUARTERS: Naugatuck, Connecticut, USA 06770 Tel.1-203-729-0271