

Architecting Health

Building a Foundation for Health Connectivity

Michael Gill



Cisco Internet Business Solutions Group (IBSG)

Architecting Health¹

Building a Foundation for Health Connectivity

Executive Summary

Can an e-mail message be sent to all of a country's general practitioners simultaneously, as may be necessary in a national disaster or a rapidly spreading pandemic? When traveling away from home, can a patient access and share his or her medical information in case of emergency? Can timely information be brought to the point of care for chronic-care patients in a way that reduces national demand on acute-care resources?

In the current health sector, the answer to these questions is generally "no." Health is highly autonomous in terms of organization and delivery, and the current, ad-hoc, legacy networks have been built by different public and private providers for different reasons. These networks display a range of inconsistent and incompatible design and operational aspects, and only some are *interconnected*.

This paper will detail three key Connected Health² positions:

- The public Internet is not an appropriate *foundation* for *secure* health messaging.
- It is important to develop a foundational architecture.
- Connecting regionally and nationally based health services offers significant opportunities for both systemic and patient benefits.

Introduction

Forget most of what you know about using the Internet. Think instead about communities and families living across a region, and imagine how electronic healthcare services would support them.

Typically, across health-planning authorities with national responsibility and policy control, the emphasis tends to be on acute care, revolving around the politically charged areas of hospital access and demand. Rarely does one see alternative models;³ and there is little realization that connectivity is important. In this space, the word "Internet" reigns supreme. There is a widespread assumption that messaging and services can be transported across the Internet without any form of degradation or risk. If this were the case, banks and airlines would not be providing services via their own networks. Banks do offer points of access for customers via the Internet; this is essentially a gateway approach. At a recent National E-Health Transition Authority (NEHTA) conference in Sydney, Australia,

dealing with message standards and e-health, the principal speaker simply indicated that application-to-application messaging would “go via the Internet.” Questions of security, flexibility, and reliability were left unaddressed.

Today, the focus is increasingly on understanding the dynamics across multiple health agencies and developing an architectural information and communications technology (ICT) response. In this context, ICT architecture refers to the process of determining the principal design attributes associated with connecting people, entities, and services in a planned manner in order to optimize delivery, cost, and scalability. Significant activity is occurring in many regions and countries. The capability of ICT to be transformative⁴, particularly in terms of system efficiency, is not disputed⁵ and often claims to provide tangible benefits in specific areas such as health.⁶ In the European Commission report titled “National Strategy for e-Health,” an evaluation of 10 e-health case studies yielded the following observation: “. . . given the right approach, context, and implementation process, ICT-based solutions can indeed improve the quality, access, and efficiency of healthcare provision.” Realizing benefits takes at least two years. In a study by RAND Corporation, RAND modeled the impact of electronic medical-record adoption in the United States and estimated potential benefits amounting to US\$77 billion per year.⁷

Specific to health, ICT architecture objectives refer to helping ensure the following:

- All health entities can communicate securely.
- Information exchange is scalable and includes voice, video, and data.
- Local and national IT data infrastructures are interoperable.

ICT architecture includes the physical infrastructure, such as Fibre Channels and satellite links. It also includes access control, quality of service, and embedded network intelligence. It does not include third-party applications, which may connect to the infrastructure. In other words, ICT is the platform.

A Community Focus

People live in places and move across geographic areas. In doing so, they tend to form identifiable communities. Mixed in among these communities are general practitioners, specialists, pathologists, radiologists, elder-care facilities, community health services, and hospitals. People needing care regularly move through a geographic area seeking support and treatment. Patients are discharged from hospitals, sometimes requiring ongoing care from a general practitioner. Elderly patients and/or chronic-care patients may move between facilities and may require a wide variety of medical providers over extended periods. *Most health activity happens in the community, not in the hospital.* Health systems tend to be acute-centric and, as such, ignore the burden of care needed in a community setting, particularly for chronic-care patients. When primary care fails, the demand on the ambulatory system, such as outpatient care, increases. This increase can cause failures in the outpatient system, resulting in more hospital admissions.

This scenario is the foundation for two emerging concepts. The first is that health-related information and services need to be available and accessible *throughout* a region and *across* all patient and health provider segments if quality, safety, and inclusivity are to be equitable. Information availability and accessibility are directly tied to significant, positive, and improved health outcomes.⁸ The second concept is that a systemic failure in one part of the health system can have major ramifications on other parts of the system. Because costs tend to be high in the hospital and low in the community, systemic failures magnify cost, often exponentially. Put another way, errors and mismanagement cost much more to recover at the hospital end than at the community end of the care spectrum, yet relatively little effort is expended to improve community care. Think of it this way: an inpatient admission represents a failure of ambulatory management.

Patients and their families “move” through the regional, state, or national health system. The efficiency and effectiveness of their “journey” bear directly on improved health outcomes. This is, for example, reflected in a reduction in waiting times for emergency treatment or surgery, or in reduced admission rates for diabetes sufferers because of improved case management. This journey also impacts how families and individuals seek medical support, particularly in chronic-care areas. Mental health is typical among these.

The Need to Connect

The fundamental proposition is that providers and patients need to connect in a timely and appropriate manner. That connection via electronic means is the primary opportunity given the principles of a patient’s journey—which can start at his or her home, neighborhood, or village—through the system. Only when one is connected reliably and securely can the exchange of information and electronic services take place. Clearly, there is an underlying point here of empowerment and patient-centricity. On the provider side, the implication is that communication is a catalyst for collaboration—the more interactive the nature of connection, the higher the probability of successful collaboration actually taking place. In other words, providers can obtain and exchange information and services at the point of care in order to reduce errors, create faster flow-through, improve patient satisfaction and, in short, help ensure better healthcare. The following examples illustrate this point.

Connectivity Across All Providers

Special authorities for selected drug prescriptions took weeks to process a prescription from the time a general practitioner forwarded the request until the time the patient actually received the authority by mail. The deployment of an architected electronic message transport system will deliver consistent performance and a connection base across all health providers. The deployment of electronic provider connectivity will offer a much improved match between doctor and patient information demands at the point of consultation.



Health Network Delivers Essential Information

Dr. Van is a general practitioner in a thriving, remote practice. In the evening and on weekends, he likes to keep up to date with the latest health news and information. He has received an e-mail detailing a 10-minute avian (bird) flu video he can watch on the health network, from the comfort of his own home. On Saturday afternoon, he connects to the health network via his broadband Internet connection. He is asked for his username, health identifier, and password. The health network authenticates Dr. Van according to rules that have been established for general practitioners. The health network establishes a secure connection for him via an encrypted tunnel across the Internet to the health network.

ICT Can Improve Chronic Care

Health authorities are moving rapidly to target chronic patients in an effort to reduce their drain on expensive hospital services while at the same time providing improved patient care. A particular health authority has adopted the position that it is cheaper to pay other service providers (including general practitioners) additional funds to support these patients than it is to manage their conditions via hospital-based services. The underlying theme emerging here is to involve patients so that they become part of the case-management team.



This experience indicates that for every dollar spent on non-hospital services, approximately \$1.40 is returned to the system, depending on the type of chronic condition.⁹ There has also been approximately a 70 percent reduction in chronic patients checking into hospitals.¹⁰ External chronic-care management revolves around the provision of accurate clinical information and test results to the care provider through a secure IT communications infrastructure. Case management is possible through the provision of alerts, benchmark normative measures, and reminders sent to patients via e-mail. Graphical information displays showing health trends allow both the patient and the practitioner to participate in making health decisions.

An IT communications infrastructure provides patients with many benefits, including:

- Reinforcing patient-care plans
- Reducing hospital admissions
- Provisioning structured care
- Sharing information
- Sharing and updating healthcare plans via the Internet

Local Control

Unlike a banking or government general services network, connectivity in health usually occurs among multiple, autonomous provider entities. This situation introduces a huge set of complexities not addressed in simpler networks found in banking and transportation. Connectivity in healthcare is fundamentally of a higher order than any other network configuration due to the need to develop design and governance responses compliant with local ownership requirements. In addition, the amount of data transmitted, such as data from radiology images, far exceeds that of bank transactions. Furthermore, the level of security required is variable, and the ability of the network to deliver services and information *at the point of care* can often have severe physical consequences for the patient if a network failure occurs. Another point of differentiation is that many of the provider entities have already developed electronic responses to varying degrees of maturity and sophistication, and may have upward of 400 old and new applications that need to function and exchange information.

User Needs Drive Services

Reliance on the Internet without a critical assessment of user needs, security,¹¹ and service reliability is akin to sailing without a compass. The volume of medical reference material, the size and complexity of CAT (computerized axial tomography) scans and X-ray images, the move to video-based consultations, and the need to preserve confidentiality are all factors that have to be taken into account to find new approaches to healthcare delivery. The health industry is required to know that the information has been sent and received, is free from computer viruses, and is intact, irrespective of its complexity or volume, particularly in crisis health environments. General practitioners require secure e-mail, automatic hospital discharge summaries, and the ability to access the latest patient condition information quickly. Such service guarantees are not possible across the Internet; there is no guarantee that the e-mail you sent to a family member overseas will actually arrive. This is simply not good enough for critical health information. And if we introduce telemedicine or general practitioner-to-medical-specialist videoconferencing across a region, for instance, the volume of video-based traffic could exceed the connection capacity normally available for the Internet. At a system level, national health monitoring for conditions such as arthritis, and for access to databases and financial information, is increasingly required in real time to aid planning and insurance outcomes.

Currently, it is not possible to add features onto pre-existing, older networks. The ability to scale from a few ad-hoc, video-based conferences among clinical practitioners to multipoint conferences on a regular basis needs to be designed into the network from the start. Such a network architecture response takes into account the quality of service requirements in a scaled system so that consistency and quality are evident across the entire geography and the entire electronic network as well.

Security for networked communications is complex. The model adopted in the financial services sector tends to resemble a “fortress” orientation where all access points are limited and access is restricted, irrespective of need. For the healthcare industry, such

a model will not work because of the numerous, autonomous provider entities. Access to the electronic assets of a health system would be based on communities of interest and on the need to connect to a service or database. For example, general practitioners may require their own electronic community with its own access control in the form of passwords and authentication, or hospitals may require quite a different model with access gateways between general and specialist hospitals. And, elder-care facilities and medical specialists may require their own electronic community that interconnects with selected providers such as pathologists and pharmacists. In other words, security in health is multilayered and should be built on a foundation of double redundancy and virtual private networks.

Modern network technology design is moving in such a way that many intelligent functions can be performed by the network itself. Such functions include virus detection and denial of service attacks, combining messages, and thorough data packet inspection. These developments imply that the provision of network-based electronic services in healthcare is much more than simply providing connectivity. Managing compliance with a specified security policy probably needs to be centrally managed. The security model deployed in healthcare is much more akin to that of an airport where “passengers” are allowed access to different areas based on their needs.

A Multilayered Approach

Architecting health connectivity means recognizing that different geographic regions and health provider entities have different access, service, and security needs. This is partly due to the level of current electronic network maturity, and to differing needs. Innovation and specialization in, for example, diabetes management may be localized in one region while electronic discharge capability may be limited to a cluster of regions. In other words, there is a patchwork of connection and electronic service capabilities. In many ways this can be referred to as *horizontal capability*. Investigating a little further into a vertical realm suggests additional complexity associated with *vertical capability*. The level and nature of information exchange between a general practitioner and the local hospital will be significantly different from that of a specialist and the multiple medical provider entities he or she services.

Specialization within medical specialist areas such as gynecology and pharmacology complicates this picture even further. From an architectural perspective, vertical and horizontal capability assessment¹² of the provider base suggests important architectural requirements peculiar to health. Some of these requirements include the following:

- Allowing services to be scaled across a region
- Converging voice, data, and video services, and embedding these inside the network
- Deploying a multilayered security model¹³ across the communications channel
- Allowing providers to access different levels of service and associated security in proportion to their local service requirements—a proportional response

- Enabling the information from older systems, such as nurse-scheduling applications and picture-archiving communication applications, to be transported
- Supporting a single integration response to build and maintain data directories
- Managing national or regional measurement, user and service identities, and consequent, centralized compliance
- Connecting mobile services such as those associated with community nursing and specialist groups

Special Features

Architecting a consistent and standard approach to mobile communication services and connecting these services to an IP-based network presents significant, positive opportunities for delivering care to rural and remote areas. There is much research on this already. From an architectural perspective, however, mobility presents two major issues. An open-connectivity-standards approach is essential as mobile data and voice services are increasingly being provided by a variety of new service providers. In addition, mobile data security needs to be customized for different user communities; information security and patient privacy can be guaranteed via the use of electronic certificates and passwords, which may differ across domains. It will be important to consider how service-level agreements in a mobile environment can be guaranteed and made to scale.

A word of warning: the typical response to an “organic” perspective that recognizes the reality of many autonomous groups in the health sector with multiple networks is to adopt the position of the federation. That is, to agree that certain functions will be shared, that autonomy will remain at all levels, and that network interconnection points are all that are needed. This approach, however, will not work for the following reasons:

- The endpoint model becomes unsustainable as network size increases. Such a model is not able to maintain reliability and service quality.
- Mobility links cannot be architected and, hence, will not be consistent.
- Such a network is unable to sustain video-based multicasting reliably.
- It will be costly to maintain and upgrade.
- Small health areas and functions may need to be “peered” with larger ones (see footnote 14). This raises the question as to who will provide the service and who will guarantee service standards.

Architecting for health connectivity is important as a first plan of action to deliver major platform support. The diversity and heterogeneity across the health sector means that decisions made by a consensus model are far more likely to succeed. It is also essential that ICT development is by design, according to both a health information strategy and a high-level network architecture. Local innovations should be encouraged

where they fall within the design parameters. One innovation is a Medical-Grade Network,¹⁴ which becomes, in effect, the sole reference point going forward. Various health groups and stakeholders can use the network architecture to guide their own ICT implementation plans to help ensure things such as open standards, security compliance, adequate transmission capacity, and connection of mobile services.

There are two main differences between a Medical-Grade Network and an older healthcare network. First, older networks tend to be built by different groups for different reasons. This gives rise to a mismatch in services delivered, and in the capacity to transport different or new services. Second, older networks are just that—at different evolutionary stages in terms of their technology, governance, and service focus. They display a range of inconsistent and incompatible design and operational aspects. The common response is to build interconnection points, but this tends to be technically limited and costly. A Medical-Grade Network built specifically for healthcare recognizes and preserves autonomous arrangements, while at the same time providing the common transport and security fabric necessary to allow a multiplicity of services to be accessed throughout a region or country.

In the end, however, the entire aim is to improve the health of the patient and the population.

Conclusion

In the current health sector, which is a mix of public and private providers, the transmission of messages, services, and images is done through a series of networks, some of which are interconnected. From a geographic perspective, some simple questions reveal the consequences of this reality:

1. Can an e-mail be sent to all general practitioners throughout the country at the same time, as may be necessary in pandemic conditions?
2. If traveling away from home in another part of the country, can a patient share his or her medical information in cases of emergency?
3. Can information be brought to the point of care for chronic-care patients in a way that reduces national demand on acute-care resources?

Establishing national health connectivity will likely lay the foundations for building connectivity in other services areas such as education, public safety, and regional economic development. Much of this thinking is currently encapsulated in policy developments around deploying national broadband. While this is useful, the national development of a health-sector response suggests building regional points-of-presence¹⁵ where other services, such as education, are also aggregated. This, in turn, suggests architecting for more than health services; it suggests providing partitioned capacity for other services, which may, from a health sector perspective, reduce costs of infrastructure development and increase political support.

The foundations for health connectivity include the following:

- Requiring connection to all providers
- Providing access and gateways for patients
- Recognizing that an area-based health strategy is more desirable than simply focusing on the transfer of acute- and emergency-care information
- Understanding the patient's journey through the system, and his or her information requirements
- Connecting and communicating to promote team-based clinical problem solving and, thus, changing work practices

Endnotes

1. Information technology in health tends to be a catchall phrase and includes almost anything electronic that displays or transports information. This paper focuses primarily on the transportation of information and the provision of applications in a connected environment, in which connectivity is the defining factor.
2. A Cisco concept about how planned connectivity can positively impact health outcomes.
3. Malaysian public health ICT activities are one example.
4. The Indian Government plans to install online and video-based kiosks in 100,000 villages, providing agriculture purchase services, education, and health support services.
5. "e-Government Strategy", page 6, Australian Government Information Management Office, March 2006.
6. "National Strategy for e-Health," page 2, Ministry of Health and Social Affairs; "New Zealand Health Information Strategy," page 34, Ministry of Health, August 2005; "eHealth Is Worth It" study, European Commission, September 2006.
7. "The RAND Study of Potential Costs and Benefits of Electronic Medical Record System," Richard Hillestad, Ph.D., RAND Corporation, September 21, 2005.
8. Public Services Summit @ Nobel Week, December 2006. Teledermatology pilots in Norway observed a 40 percent decline in face-to-face specialist consultations. In New Zealand, chronic-care telehealth services achieved a 60 percent decline in hospital admissions.
9. New Zealand District Health Board, May 2006.
10. New Zealand District Health Board, Counties Manukau.
11. "Symantec Internet Security Threat Report," Symantec Corp., January 2006. According to the report, there were 6,110 "denial-of-service" attacks per day from January 1 to June 30, 2006. And, Web application vulnerabilities made up 69 percent of all vulnerabilities.

12. User-needs assessments are required both to evaluate the current network capability in a region or across a state and to understand the dynamic between vertical and horizontal capability. Cisco has significant experience in this arena.
13. Multiprotocol Label Switching VPN model. A VPN is a private communications network often used by several companies or organizations to communicate confidentially over a publicly accessible network. VPN message traffic can be carried over a public networking infrastructure (e.g., the Internet) on top of standard protocols, or over a service provider's private network with a defined service-level agreement between the VPN customer and the VPN service provider.
14. A Medical-Grade Network is an optimized network architecture for the healthcare industry based on best practices for real-time collaboration, availability, security, and flexibility. This type of network optimizes interactions between processes, applications, and technical architecture components.
15. Points-of-presence (PoP) are geographically dispersed access points for subscriber connection, consisting of Layer 1, Layer 2, or IP access transport services sourced from commercial telecommunications carriers, and providing firewall, encryption, IP VPN termination, and other services.

More Information

The Cisco Internet Business Solutions Group (IBSG), the global strategic consulting arm of Cisco, helps Global Fortune 500 companies and public organizations transform the way they do business—first by designing innovative business processes, and then by integrating advanced technologies into visionary roadmaps that improve customer experience and revenue growth.

For further information about IBSG, visit <http://www.cisco.com/go/ibsg>



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.