



BDNA for Clinical Information Systems

August 2006

An Environment of Growth and Complexity

With advances in biomedical technology and improvements in our ability to store, share and transmit data over networks, the once disparate worlds of clinical engineering and information technology are converging into a new breed of health care technology: Clinical Information Systems (CIS). These systems support a variety of health care functions (from patient monitoring to imaging (X-Rays, MRIs) to operating rooms) and medical specialties (from Cardiology to Ophthalmology to Obstetrics/Gynecology).

As the number of these patient-critical systems grows, and an ever increasing portion of them become network-connected, the challenge to manage the complexity of the environment intensifies. In addition, regulatory and security requirements make it critical that CIS managers understand what is in their environment and how it is configured.

Take, for example, a large, national health care delivery organization:

- It is growing its base of hospitals by almost 30% through 2006
- It has over 250,000 clinical devices installed (compared to ~200,000 IT devices)
- The percentage of clinical devices connected to the network is expected to grow from 15% now to 60% in 2012 and 80% in 2015

As the managers of these environments grapple with the changing landscape, they face four distinct challenges:

- Operational and Asset Management Challenges
- Security Challenges
- Regulatory Risk Challenges
- Connectivity and Integration Challenges

Operational and Asset Management Challenges

Compared to IT departments, Clinical Systems Engineering departments typically have many fewer technical resources per asset dedicated to running and maintaining the systems. The assets are also increasingly remote: more clinical protocols are being pushed out of hospitals and clinics into patient homes in support of home care.

To facilitate regular maintenance procedures in this environment, it is critical to have an up-to-date inventory of all supported devices, including information on their configuration. Imagine a clinical systems provider issuing the recall of a specific clinical system model/version, but not knowing where that model/version is installed across your environment!

While several systems management solutions exist to support this challenge for IT systems, none are geared towards a biomedical/clinical environment. The current IT solutions may be able to identify, for example, some type of application running on a Windows 2000 operating system, but they will not be able to say that it is a Windows 2000 device running an MRI imaging application.

Enterprise IT departments of health care delivery organizations also have a stake in understanding the biomedical/clinical landscape. Because of regulatory, privacy and patient care concerns, these systems cannot be subject to enterprise IT guidelines, procedures and standards. In order to avoid applying such standard (and often automated) procedures to biomedical devices, IT departments must know what to avoid.

Security Challenges

Often, clinical systems are not subject to the same IT standards and procedures that traditional IT systems are subject to. Therefore these systems may become sources of security vulnerabilities. Because they had been very efficient in installing and keeping up-to-date anti-virus software on their workstations, one organization was surprised to find itself beset by a virus on its enterprise IT systems. It turned out the virus had entered the environment through a biomedical device, supplied and maintained by a vendor who was not subject to the same strict anti-virus policies as the organization. Being a network-connected clinical system, the virus spread from the biomedical device, over the network, infecting other vulnerable systems.

CIS environments are for the most part still new to “best practices” such as firewalls, properly partitioned networks, continuity of operations and disaster recovery procedures. As stated earlier CIS organizations are challenged by both a lack of resources and by limited visibility of the environment in which these practices need to be implemented.

Regulatory Risk Challenges

Exposure to regulatory risk is a factor driving many organizations, medical and otherwise, towards better control and management of their information systems assets. In addition to SOX compliance requirements, health care provider organizations must also contend with privacy regulations and medical malpractice risks.

A simple update or patch applied to a clinical system may shift the burden of regulatory responsibility. Take, for example, the case mentioned earlier of the vendor’s system introducing a virus onto the network attached biomedical device and subsequently onto the organization’s network. Even though the CIS manager was aware the biomedical device needed an anti-virus update, he was not allowed to apply the update himself. According to regulations, applying the update would shift the identification of the “manufacturer” of the device from the vendor to the customer. This would also shift the relevant regulatory burdens from vendor to customer. Having the information to triangulate device type, manufacturer/vendor and required updates can help the CIS manager from assuming unnecessary risk and in providing timely requirements to its vendor for device/system upkeep.

Another health care provider explained the need to automate error-free drug delivery. Most health care organizations have thousands of drug delivery systems (“pumps”) in use. These pumps need periodic safety protocols and formularies applied. To avoid human errors, many organizations are working towards automating the update of these safety protocols and formularies. As these updates are performed, errors are occasionally

generated. Currently the generated error codes are stored locally at the device, resulting in local remediation efforts and, again introducing inefficiency and potential for human error. As these drug delivery systems are increasingly networked, an ability to collect and manage these errors centrally would simplify health care organizations keeping current with drug delivery regulations.

Integration and Connectivity Challenges

There are many factors driving the need for improved integration in clinical information systems.

- As more and more medical records are digitized and brought on-line, there are increasing demands for seamless sharing of patient data.
- An increasing number of clinical devices are being connected to enterprise networks.
- More mobile devices are being introduced in health care facilities to support functions such as patient care and monitoring.
- As clinical processes are pushed outside traditional health care centers to private homes and elder care centers, more clinical devices are also appearing in these environments.

Such trends point to the need for a professionally run and managed CIS network as well as improved inter-system integration. Current CIS resources are not adequate in numbers or skills to support the scale and complexity of these needs. This in turn heralds the need for convergence between CIS and enterprise IT, with common infrastructure and processes for supporting both the enterprise and clinical systems environments.

Key Components of Transformation to a Managed, Integrated CIS Environment

- Automated Discovery and Identification: Because visibility is a prerequisite for addressing all of the above challenges, it is critical to automate the process of discovering and accurately identifying what devices exist in the environment.
- Accurate, Timely, Periodic Inventory of Assets: Keeping the inventory of all assets fresh provides the ability to promptly and effectively target and address identified risks and operational issues.
- Proactive Analysis for Operational and Regulatory Risks: Building a periodic audit into the organization's business processes is critical. The audit should analyze the inventory for key operational events (software updates, patches, vendor support end dates, etc) and regulatory requirements (HIPAA, FDA reporting deadlines)
- Integrated IT and CIS Networks, with Built-in Security and Privacy Safeguards: The security, capacity and availability management discipline applied to IT networks needs to become standard practice for CIS networks. However, CIS networks need to be appropriately partitioned and secured to meet regulatory and patient care needs.
- Effective Tracking for Remediation or Improvement Initiatives: Because they provide critical patient care, it is critical that health care provider organizations follow through on their CIS remediation or improvement opportunities. Being able to

effectively and regularly track progress of these initiatives across the CIS environment allows the initiative owners to prioritize and target the remaining work, and evaluate value delivery to date.

How BDNA Can Enable the Transformation

BDNA Corporation provides content, applications and services to address many of these needs. Our current health care provider customers have already realized the benefits of BDNA's non-intrusive, comprehensive inventory capability, and are moving towards using both the inventory and reconciliation capabilities to track their IT and biomedical assets.

- **Biomedical “Fingerprints”**
BDNA has developed the capability to recognize or “fingerprint” several clinical information systems during its network scans. These “fingerprints” look for signature responses to BDNA queries, and allow the scanning application to identify with certainty the queried device as, for example, a specific imaging application or a particular patient monitoring product. We are working with our current clients to grow the set of such biomedical fingerprints.
- **On-demand discovery and inventory through *Inventory Consolidation***
BDNA's *Inventory Consolidation* application scans a customer-defined network space to discover, identify and catalog all network connected devices into an inventory, which can then be examined, sorted and filtered through the analytics/reporting user interface of the application. The discovery process is non-intrusive (in the sense that it leaves no agents on the devices it scans), has near-zero impact on network performance and produces very comprehensive and detailed data on connected assets and their attributes. Working in conjunction with biomedical fingerprints mentioned above, it can produce a list of clinical information systems, their platforms, locations, configurations, etc.
- **Reconciliation and tracking through *Asset Reconciliation***
BDNA's *Asset Reconciliation* application provides the capability to tally any two inventories/registers against each other to find matches and non-matches. Our clients have used them to reconcile BDNA discovered inventory against their asset registers, procurement lists, ERP lists, etc. The application can also be used to track changes in the environment across time, by reconciling inventories conducted at two (or more) different points in time.
- **Inventory Analysis and Value Identification from BDNA's Strategic Services**
With our experience implementing BDNA across multiple clients in many industry segments, BDNA's Strategic Services group has developed a proven methodology to derive the greatest value from using the BDNA solution. In addition to supporting our customers' projects to implement BDNA, the Strategic Services team provides custom analysis, conducts audits, identifies initiatives to manage risks and improve operations, and trains users in conducting their own analyses.



Summary

As Clinical Information Systems grow in number and complexity across health care provider organizations, there are growing needs to manage scale, complexity and risk. CIS organizations face many traditional IT challenges in managing their environment, but several challenges are unique. An effective tool to help identify, inventory and track the CIS infrastructure will be critical to managing complexity and risk. BDNA's suite of solutions and services are already providing this capability to health care providers. For additional information on BDNA solutions or services, contact: sales@bdnacorp.com