

Table of Contents

Executive Overview.....	1
Endpoint Data Protection Challenges Facing Healthcare Providers.....	2
Laws and Regulations	4
Healthcare Data Breaches.....	7
Protecting PHI on Endpoints The GuardianEdge Solutions.....	8
Best Practices in Action	14
Endpoint Data Trends in Healthcare.....	16
Conclusion.....	16

Executive Overview

While automation in healthcare has been limited relative to other industries, in recent years the use of information technology and the electronic exchange of sensitive patient data are increasing. Ample evidence exists to show that great forward strides in healthcare efficiency and quality can be realized through automation—especially when it is supported by a national health information technology infrastructure that allows for the secure electronic use and exchange of information. This approach to managing patient data will foster collaboration among physicians, staff, and patients, and is currently being developed with legislation and funding under the 2009 stimulus package (ARRA).

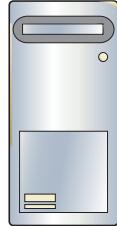
Among the many changes confronting all healthcare organizations today include:

- Larger geographically dispersed delivery of care
- Increasing use of specialists and sophisticated diagnostic and treatment technology
- A need for ready access to patient and disease data as well as automated decision support tools
- Increasingly mobile medical personnel who deliver patient care inside and outside of the hospital

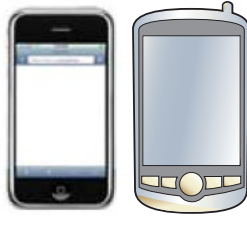
The result is a common requirement to access and secure patient data on a wide range of endpoints—laptops, personal computers, removable storage devices (USB keys, portable disk drives, SD cards, etc.), portable media (CDs/DVDs/ floppy), PDAs as well as iPhones and smartphones.



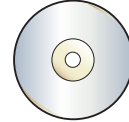
Laptops



Desktops



iPhones—Smartphones



Removable Media

Enterprise Endpoints—Personal and Protected Data at Risk

The foundation of this enhanced access to critical data must be a health information technology infrastructure that allows for a ubiquitous and secure exchange and use of information. Furthermore, it must protect the data in order to meet stringent federal and state security compliance requirements. This infrastructure also needs to support access to information and collaboration among mobile medical personnel as they perform duties throughout the expanded healthcare enterprise.

Similar to many other industries, healthcare is adopting an electronic transaction model. Common business drivers for this electronic model include improved patient care and delivery, processing of daily financial and medical transactions, compliance with regulatory issues and evidence-based care delivery, and communications among doctors, staff, patients, third-party providers and payers. The healthcare industry needs trusted and proven technology solutions that can help enable these business mandates.

Solutions for protecting data on endpoints in these environments must safeguard all private information and work within a maze of systems and priorities, while at the same time solving the operational issues of deployment, management, scalability, reporting, auditing, and enabling clinical capabilities for enhanced services. Key to the success of any implementation is close integration with this existing infrastructure, which enables the lowest possible costs of implementation, on-going management, and customization.

This white paper will discuss:

- The high priority currently being placed on healthcare information technology
- New federal and state mandates for the secure collection and exchange of electronic patient health information. Including those established as part of the stimulus package
- The application of endpoint data protection technology within healthcare providers
- Operational issues that surround managing the technology in these environments
- How GuardianEdge solves problems unique to healthcare providers

It will also explore key considerations such as the work flows inside departments (each of which operates as an island within its own organization and as part of the continuum for delivering quality patient care), the “collaborative” model of patient services, and how the combination of these unique work flows for each patient creates risk of exposure to protected health information (PHI) and other sensitive data. The paper also details how GuardianEdge technology can safeguard sensitive data while enabling organizations to provide quality patient care with a complete solution that seamlessly integrates with existing IT infrastructure for deployment, management, and on-going operation. Finally, it looks at the emerging use of mobile technology to give better access and patient care—a trend that is changing the landscape for protecting data on all endpoints devices.

An AARP study shows that healthcare sector losses are due mostly to physical theft of hardware and media (69%) and insider access (14%).

AARP Public Policy Institute – Into the Breach: Security Breaches and Identity Theft

Endpoint Data Protection Challenges Facing Healthcare Providers

Hospital IT environments operate with many unique locations, departments and specialist groups (physical therapists, MRI, radiology, AIDS testing, genetics testing, etc.) as well as close relationships with outside labs and subject experts. PHI lives within this web of relationships, organizations and specialists, where all the various players must collaborate and share information to effectively provide their highest priority—quality patient care. Furthermore, they all need easy, immediate, and secure access to this information.

Typically, this access is authorized on a limited “need-to-know” basis with each user having role-based access to a network and applications that transmit and store data. However, this “need-to-know” access policy must also be applied beyond the wide area network to protect data on endpoints. Many hospital applications that use PHI frequently require local access on an endpoint device. Departments also have a wide variety of specialized hardware and software for specific analysis and tasks. Many of these solutions require data-and computation-rich applications on endpoint devices and must have some of that data available locally for analysis and display, rather than stored in a backend system.

Complicating the problem are the work flows for patients and data tailored by physicians, insurers and local resources. Work flows vary by location and organization—and are often unique even within the same specialty. Staff operational work flows vary widely as well. In fact, there are as many work flows in hospitals as there are jobs, job titles, and roles in the departments.

The need for more mobility to improve quality of care and enhance productivity requires patient data to be present and secure on a local system or device—laptop, USB key, CD/DVD, etc. The clinical and business needs that require patient data to be more mobile enhance the risk of unauthorized access to data on endpoints.

Risk equated to a Post-It note

In the past, packaged medical apps came from a primary vendor and had strong password security built in. This meant there was little risk of data leaving an organization inappropriately, as it was all stored in a centralized system or in physical media files. There were few ways to extract information from these systems on endpoints except by using pencil and paper or printing it out. As a result of this low-risk environment security was taken so casually that, until just a few years ago, monitors were typically covered with Post-It notes where users had written the passwords for each major application.

Today, although most institutions use one top-tier vendor for billing, recordkeeping, insurance authorization and payments, they are not dependent on one strategic software vendor. Departments have specialized and tailored applications and information technology equipment to fit their specific requirements and needs. Many of the applications and technologies that previously existed primarily in an isolated state within each applicable department (nursing, lab, radiology, pharmacy, etc.) are now being connected to exchange information, collaborate, and create a complete view of the patient's care needs. This exchange of information among numerous applications—many of which may be from older legacy systems—creates a significant security challenge.

For example, primary vendors can't ensure that a vendor mix of applications that includes second-tier applications is secure, and some second-tier applications are legacy applications with little concept of security in their implementation. This combination of diverse data "islands" and centralized higher level applications makes protecting data on endpoints more difficult.

In short, patient data can reside in central repositories while also being used on endpoint devices throughout the organization. Therefore, the endpoint infrastructure must be secured, in addition to securing the primary applications. The endpoint risk includes not only laptops and PCs but also tools—such as USB keys, removable hard drives, CDs, DVDs and floppy disks—that make data more accessible for groups and individuals.

Given this highly complex environment, and the realities of funding IT projects in healthcare today where even money for critical projects is strictly limited, an IT organization for a healthcare provider requires a solution that solves the problem of protecting data on endpoints while also addressing critical operational issues—deployment, management, scalability, compliance, reporting, auditing, and user productivity—at the lowest possible total cost.

Until just a few years ago, monitors were typically covered with Post-It notes where users had written their passwords for each major application.

In an IT Compliance Committee report: Taking Action to Protect Sensitive Data that surveyed 201 organizations and found that of every 10 companies surveyed all experienced losses of sensitive data—one experienced two or less losses of sensitive data per year, seven experienced six losses, and two experienced twenty-two or more.

IT Policy Compliance Report

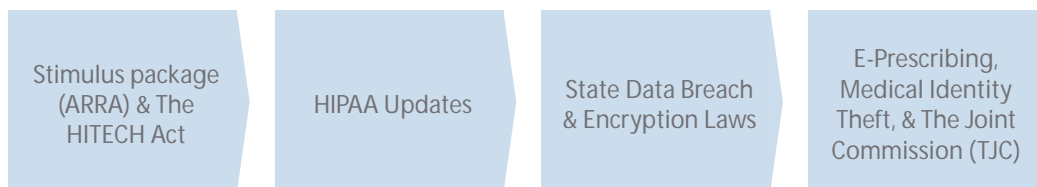
GuardianEdge addresses these challenges by providing a complete enterprise-class solution that delivers:

- Endpoint data loss protection via encryption for hard disks, portable media and devices, as well as smartphones
- Prevention of data leakage to portable media and devices by identifying data usage patterns while monitoring and controlling the flow of data
- Safeguards that protect PCs from the risks of malicious code on rogue devices and media
- WiFi connection security to protect core networks from the risks of bridging to unprotected external wireless networks

The GuardianEdge solution is standards-based, making it simple to deploy and cost-effective to implement, delivering strong centralized management coupled with low training and support costs.

Laws and Regulations

While the widespread adoption of measures such as electronic health records has the potential to improve the quality of healthcare in the U.S., these technological developments will be able to fulfill their promise only if Americans have confidence that their sensitive health information will not be disclosed inappropriately. As a direct result of this proliferation of electronic record-keeping, the last decade has seen the enactment of extensive federal and state legislation and regulation designed to protect sensitive personal information.



Legal and regulatory environment for healthcare insurance

Stimulus package (ARRA) and the HITECH Act

In January 2009, the stimulus package (the American Recovery and Reinvestment Act—ARRA) created the Health Information Technology for Economic and Clinical Health Act (HITECH Act). The HITECH Act is designed to improve quality of care by establishing a nationwide health information technology infrastructure that allows for the secure electronic use and exchange of protected health records by 2014.¹

The HITECH Act also amends parts of HIPAA and includes improved privacy and security provisions that require:

- Application of HIPAA security provisions and penalties to “business associates” of covered entities. (Previously, HIPAA required “satisfactory assurance” only.)
- Notification in the case of a breach and posting of such breaches on the Department of Health and Human Services (HHS) public website. (This includes covered entities, business associates, vendors, and 3rd party service providers.)
- Tiered increase in potential amount of civil monetary penalties. For example, a violation due to willful neglect can result in at least \$50K per violation up to a total of \$1.5M in a calendar year.
- Enforcement by State Attorneys General, in addition to the existing HHS Office of Civil Rights (OCR) enforcement powers.

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes the Security Rule as well as the Privacy Rule for Protected Health Information (PHI)—which defines PHI as any information about an individual’s health status, provision of healthcare, or payment of healthcare or that could be reasonably tied to an individual by a combination of patient name and address, birth date, or social security number. Both rules set standards and specifications for administrative safeguards, physical safeguards, and technical safeguards.

Administrative safeguards—formal practices to manage the selection and execution of security measures to protect data and the conduct of personnel in relation to the protection of data

Physical safeguards—physical measures, policies and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, as well as unauthorized intrusion

Technical safeguards—processes and technology to prevent unauthorized access to data that is transmitted over a communications network

In March 2006, HHS published its final HIPAA enforcement rule that established the initial civil monetary penalty authority for a HIPAA violation. This was expanded in January 2009 under the HITECH Act, as noted above.

In December 2006, HHS Centers for Medicare and Medicaid Services (CMS)ⁱⁱ published guidance to provide HIPAA covered entities with general information on the risks and possible mitigation strategies for remote use of and access to electronic protected health information (ePHI). This mandate ordered covered entities that handle ePHI to implement stronger authentication mechanisms for controlling access to the data.

State data breach and encryption laws

There are currently 45+ states that have passed data security laws that apply to companies that do business with residents of those States.ⁱⁱⁱ State laws require that businesses encrypt data in storage and in transit to avoid the data breach notification mandates.

Of the total 42,399 complaints received from 4/2003-2/2009, 11,992 were investigated.

7,992, or approximately 67%, of complaints investigated, obtained corrective action

US Department of Health & Human Services site 3/23/2009

For example, organizations that encrypt personal data are not required to notify the resident and can avoid the potential media exposure, reputation damage, civil and regulatory fines, and financial loss in the event a PC or other device with that information is lost or stolen. Encryption of protected mobile data (e.g., sensitive information on a smartphone, laptop, PDA, USB) is a significant, prudent measure for all organizations. In addition, if a device with encrypted data is lost or stolen, an enterprise-class endpoint data protection solution will provide auditable evidence that data on the device was encrypted.

Alternatively, loss or theft of a device with unencrypted nonpublic personal customer data automatically results in a data breach that requires the organization to notify customers across most states. Nevada and Massachusetts have also passed specific laws that mandate data encryption—it is no longer a choice in these states. Other states are also considering similar encryption mandates.

In Nevada — “A business in the state shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission.”

In Massachusetts — “Any business that stores personal information about a resident in the Commonwealth shall encrypt all transmitted records with personal information across public networks and all data transmitted wirelessly. They must also encrypt all personal information stored on laptops or other portable devices.”

Typical consequences incurred by the affected organization include the following, with an average total cost of \$202 per record:

- Remediation costs (credit monitoring services, special programs, etc.)
- Customer service costs to answer customer questions about the breach (phones, mail, email)
- Notification costs (written, email, press, etc.)
- Legal liability when an ID theft occurs
- Damage to image and trust
- Stock price impact
- Staff costs (legal council, executive management time, etc.)

e-Prescribing, Medical Identity Theft, & The Joint Commission (TJC)

Other significant events are also raising the bar on how well hospitals, clinicians, and other covered entities protect the security and confidentiality of patient health information and the increasingly connected healthcare networks.

For example:

- HHS is pushing for adoption of e-prescribing. Effective in 2009, doctors will receive a “bonus” on Medicare payments for e-prescribing. After 2013, the bonus payments will be phased out and doctors will be penalized with lower reimbursement rates for not e-prescribing. Ensuring that each healthcare provider has a safe and secure technology infrastructure and a HIPAA

The total average costs of a data breach grew to \$202 per record compromised, an increase of 2.5 percent since 2007 (\$197 per record) and 11 percent compared to 2006 (\$182 per record).

Breaches are costly events for an organization; the average total cost per reporting company was more than \$6.6 million per breach (up from \$6.3 million in 2007 and \$4.7 million in 2006) and ranged from \$613,000 to almost \$32 million.

Ponemon 2008 Annual Study: Cost of a Data Breach

compliant information security program is key to the success of this e-prescribing initiative.

- *Medical Identity Theft.* Medical identity theft is an emerging issue that raises concerns for consumers, healthcare providers, health plans, and others. In January 2009, the Office of the National Coordinator for Health Information Technology published its "Medical Identity Theft Final Report."^{IV} This report found that the potential consequences of medical identity theft include the loss of accuracy of medical records, expenses to individuals whose identities are stolen, widespread expenses to the healthcare system, and compromised patient care if inaccurate health records are relied on at the point of care. The report includes recommendations of policy and technical approaches to address issues of prevention, detection, and remediation of medical identity theft.
- *The Joint Commission January 2009 Deadline.*^V In July 2008, The Joint Commission issued updated accreditation standards that go into effect in January 2009. This will require healthcare organizations to become aware of the new standards and comply. Information security, privacy, and technology risk management are key among these updated standards. Hospitals must meet the challenge of enabling compliance with these newly enhanced standards. If they do not, they risk the loss of reimbursements from Medicare for such services and increased liability of insurance costs.

As the national awareness and cost of sensitive patient and employee data breaches continues to rise, government agencies take a more active role in the security of sensitive data. Additionally, as the use of technology to exchange information grows, healthcare organizations must also ensure they are enabling prudent security practices at all endpoints. The burden of change rests on the organizations themselves, who must abide by these technology risk management and information security standards for the use and dissemination of healthcare information—or face strict penalties for noncompliance or loss of accreditation.

The steady stream of privacy breaches threatens to undermine the health-care industry's effort to adopt electronic medical records. That push is meant to make medical care both safer and more convenient for patients, but a major barrier to health-care digitization has been anxiety about preserving the security of such sensitive data.

Are Your Medical Records at Risk?
Wall Street Journal Online, 4/29/2008
Sarah Rubenstein

Healthcare Data Breaches

In spite of these laws, rules and expanded government and accreditation initiatives to secure nonpublic personal information, almost every company has experienced a data breach or theft of corporate desktops and laptops. A recent AARP study reveals that healthcare sector losses are due mostly to physical theft of hardware and media (69%) and insider access (14%). This data shows that the healthcare sector would benefit both from controlling access to information through endpoints and encrypting the information resident on the endpoints. Examples of recent healthcare data breach losses include:

December 12, 2008 Oregon Health and Science University. 890 patients were notified that a stolen laptop may contain their health records.

January 9, 2009 NHS Central Lancashire Primary Care Trust. A healthcare worker lost a USB memory stick containing the records of 6360 prisoners.

February 3, 2009 Baystate Medical Center (Pediatrics Division), Massachusetts. Several stolen laptops expose an unknown number of patient details.

February 9, 2009 Parkland Health & Hospital System, Texas. A stolen laptop exposes names, birthdates and SSN for 9300 patients

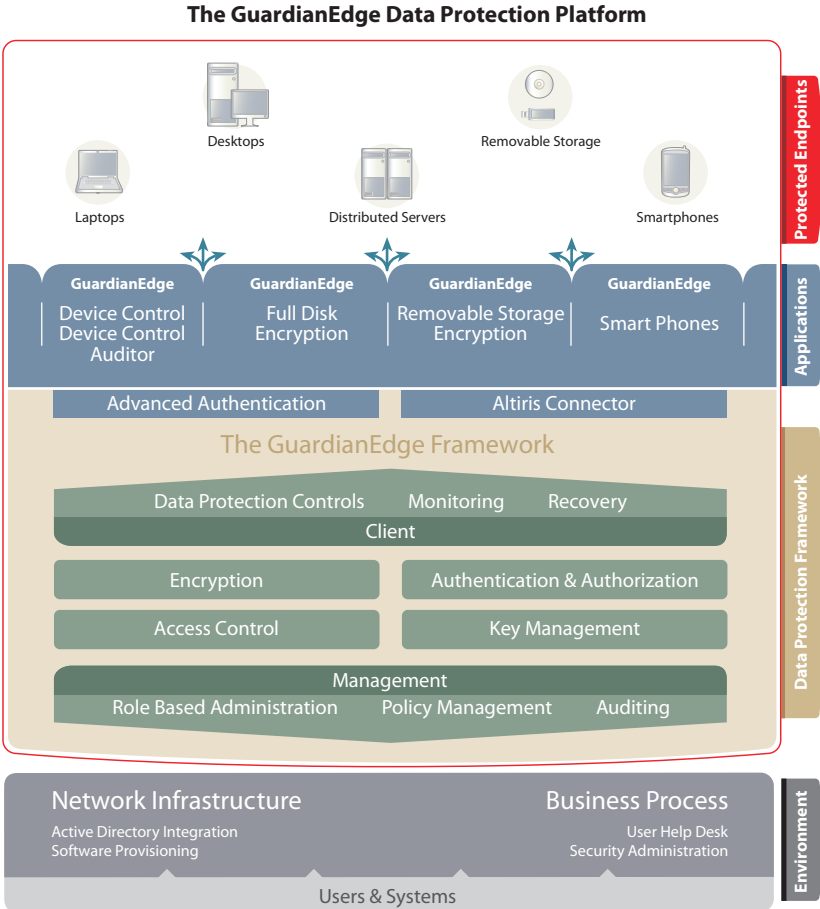
February 18, 2009 Kaiser Permanente, California. Records of 29,500 Northern California employees found on a confiscated computer

Protecting PHI on Endpoints – The GuardianEdge Solution

Leading organizations and healthcare providers are finding that the best way to eliminate the loss or leakage of PHI data on endpoints is to be proactive. In other words, to avoid incurring the costs of medical identity theft or other type of breach, and comply with a decade of laws and regulations organizations need act before a device is lost or stolen. This means ensuring that data on high-risk mobile devices such as laptops is protected against unauthorized access.

Physicians in hospitals and clinical campus environments will continue to need mobile access to patient information—either wirelessly or by logging into the nearest PC. Alternatively, a lab technician's access must be limited to lab results, preventing inappropriate access to fully detailed patient records. Similarly, DVDs sent from radiology to the patient's primary physician must be protected so that PHI is not compromised if the physical media is lost in transit or stolen.

Proactive best practices for securing endpoints in this diverse environment include a mix of endpoint device encryption and other endpoint access control technologies, role-based policies and procedures, training, auditing (who has accessed which application and what data is where) and, most of all, diligence.



TCO and deployment costs are key considerations

Not only must successful protection ensure the safety of data, be transparent to end users, and preserve existing work flows in, as well as between, a healthcare organization's myriad "islands"; it must also take into account the fact that budgets and resources are constrained as never before. The result is that protection must be implemented not "at-all-costs" but within the reality of existing budget and support resources. A low TCO then is critically important, and is driven by the capability to solve the operational issues that surround endpoint data protection by making maximum use of existing infrastructure, training and resources.

- Direct integration to existing directory services and management interfaces, for instance, immediately removes the need to implement a costly parallel group, user, authentication and administrative management set, and minimizes the training requirements and "ramp" required for IT staff to come up-to-speed.
- Policy control and deployment should be integrated with existing mechanisms already in use, as this prevents the need to implement a new set of servers to support the solution, and training for staff in how to create, use and audit policy implementation.
- And the solution must also work within the framework of your existing system management tools—software and update deployments should continue with existing or minimally changed work flows.

This approach results in maximum leverage of your existing investments. Costs for initial deployment are low, since no parallel infrastructure is required and on-going management does not require the creation of a new IT management team to sustain protection.

The GuardianEdge Data Protection Platform

A The GuardianEdge Data Protection Platform is based on an enterprise-ready, standards-based architecture that protects sensitive data while providing simple, flexible implementation and low TCO along with a complete set of endpoint data protection controls.

Standards-based—A standards-based architecture is a key enabler for a successful project at the lowest possible implementation and on-going management cost. Elements of a standards-based architecture include:

- *User and Administrative management*—GuardianEdge user and administrative management leverage existing directory services (Active Directory and eDirectory) to make real-time use of existing groups, organizational units, administrative roles, machines and users with little or no synchronization lag and without the need to rebuild and administer a parallel management set.
- *Policy creation and deployment*—Similarly, policy creation and deployment occur using existing policy mechanisms (Microsoft GPOs and similar mechanisms) to avoid the need to create an entirely new policy infrastructure.
- *Communications*—Communications use the protocols and transport layers already optimized for in enterprises—HTTP(S), XML and SOAP are key enabling protocols. This allows data protection solutions to easily work within existing network structures

Medical data breaches on the rise

Despite privacy regulations, data breaches are not only becoming more common within the medical community, hospitals and medical centers are slow to report the breaches to patients

SCmagazine.com
May, 2008

- *Management Interfaces*—Management interfaces use familiar Active Directory based metaphors and tools that your IT team is already trained on, and accustomed to, make it simple and easy for staff to get up-to-speed and allow fast implementation.
- *Databases*—Storage and reporting of data collected to monitor the state of your implementation and provide auditable proof of protection status are available via existing or familiar databases that your organization already knows how to support and manage – Microsoft SQL Server.
- *Software installation*—Client and server software installation leverage your existing software delivery and reporting mechanisms with MSI and EXE file formats available

Enterprise-ready—To achieve enterprise readiness, a solution must be scalable, support high availability, integrate with existing infrastructure and with existing IT and business processes while supporting a transparent user experience.

- *Standards-based implementations support enterprise readiness*—Implementations like GuardianEdge's that are standards-based inherently support this with scalability, availability and infrastructure integration already built into the underlying existing architecture; Databases implemented for high availability are used to support the implementation. Network architectures and transports already include high availability communications capability. And so on.
- *Integration with existing IT and business processes*—Just as important is integration with your existing IT and business processes. GuardianEdge Data Protection Platform products support existing patch, update and configuration management with little or no process change, and support existing management tools and consoles such as Altiris, Active Directory and eDirectory. The result is a solution that can be implemented quickly, and supported with your existing personnel.
- *Transparent end-user experience*—Lastly, achieving enterprise readiness requires an end-user experience that causes minimal disruptions in business workflows and minimal help desk calls. The GuardianEdge Data Protection Platform achieves this with solutions designed and matured for a transparent user experience.

A complete set of solutions—The platform supports an array of applications, including hard disk encryption, media protection as well as iPhone and smartphone protection. These products, and their shared management platform, help to ensure that:

- Sensitive data remains inaccessible on lost or stolen devices
- Information does not inadvertently leak from an organization
- Risks from portable devices, media and WiFi network connections are reduced or eliminated

"Acquiring 3000 tablets increased our risk dramatically. Our comfort zone is having GuardianEdge"

Director Of Information Security at Select Medical
Brian Rusignuolo

This unified approach lowers the cost of ownership by eliminating redundancy and ensures that misalignment of policies and their administration do not create hidden exposures.

GuardianEdge Hard Disk Encryption—Protects data on desktop and laptop PCs from physical loss or theft with strong encryption—providing a “safe harbor” from data breach risks and disclosures whenever a laptop, PC or hard drive is lost, stolen or even simply retired. It delivers a complete solution that includes pre-boot authentication, single sign-on integration and transparent user operation.

GuardianEdge Device Control Auditor—Allows easy assessment of an organization's exposure to data loss and data leakage on removable devices.

GuardianEdge Media Protection

- Prevents data leakage from PCs with port, device and file type controls that keep data from leaving protected platforms inappropriately
- Shields data on USB flash drives, CD/DVDs, copiers, MP3 players, and other removable storage from physical loss or theft with strong encryption
- Reduces the risks to PCs from portable devices, storage and media with protection from auto-executing code (e.g., AutoRun worms) and hardware keyloggers
- Protects organizations from the risk of exposure to network attacks using bridging from wireless networks

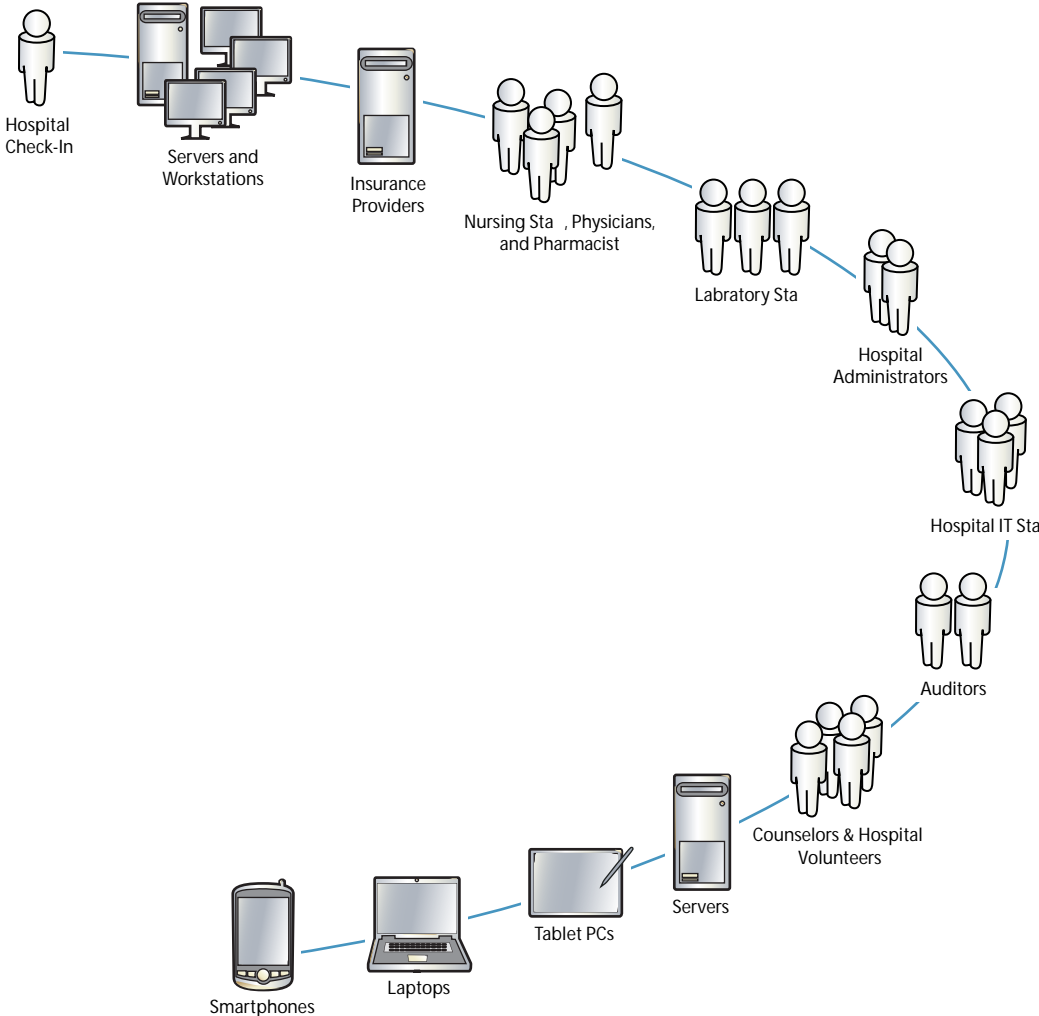
GuardianEdge Smartphone Protection—Provides a complete solution for protecting data on Windows Mobile smartphones and Apple iPhones with file and folder encryption to protection against loss or theft and device configuration, security and access controls.

GuardianEdge Advanced Authentication—Enables deployment of strong multi-factor pre-boot authentication for enhanced protection of data encrypted with GuardianEdge Hard Disk and additional access security with GuardianEdge Removable Storage Encryption

GuardianEdge Altiris Connector—Integrates the GuardianEdge Data Protection Platform directly with the Altiris Notification Server™ Console, allowing IT administrators to improve security by streamlining the deployment and monitoring of GuardianEdge Hard Disk Encryption and GuardianEdge Media Protection through the same familiar management console they already use for asset management, configuration management, patch and update control and more

A Day in the Life of Patient Data at a Healthcare Provider

As an example how GuardianEdge addresses the complexity of real-world healthcare environments, we'll follow the course of a patient's data—from the time they come into an emergency room for treatment of a fractured leg all the way through discharge—concentrating on the potential exposures of their data on endpoints that result from each step in the process.



Step	GuardianEdge Protection
<p>Department: Admitting</p> <p>Action: Patient data collection, insurance verification, primary physician notification, interface with first responders information</p> <p>Risk: local data stored on admitting room PCs and laptops</p>	<p>Hard Disk Encryption protects data in the event of physical loss or theft of a device</p> <p>Media Protection ensures that only approved devices can connect and that only approved file types can move from those systems and makes certain that any data leaving the platform is safe if the device or media is misplaced or stolen</p>
<p>Department: Emergency</p> <p>Action: Assess, order imaging and blood work, treatment, orders e-Prescription from tablet computer, may need to notify external surgical personnel (activate wireless emergency phone network), interface with Primary Care group phone system</p> <p>Risk: Exposure of PHI</p>	<p>Hard Disk Encryption protects from physical loss or theft of the devices.</p> <p>GuardianEdge Media Protection ensures that only approved devices can connect and that only approved file types can move from those systems</p>
<p>Department: Radiology</p> <p>Action: Imaging of fracture, accesses patient's previous imaging exposure data; writes DVDs for consulting physicians and primary physician, interfaces with primary physician office electronic medical record</p> <p>Risk: PHI</p>	<p>Removable Storage Encryption uses a shared group encryption key is within the medical group that allows consulting and primary care physician to seamlessly access data on DVDs and other portable storage devices. Patient image and personal data are encrypted for protection from loss or theft of the media, but all parties can use the data without changes to their existing workflow.</p>
<p>Department: Consulting physicians</p> <p>Action: Review Imaging on a PDA, laptop, or courier delivered DVD of the fractured leg</p> <p>Risk: Exposed PHI (name, DOB)</p>	<p>GuardianEdge Media Protection makes certain that any data leaving the platform is safe if the device or media is misplaced or stolen</p>
<p>Department: Nursing units</p> <p>Action: Physicians nurses, transport, lab, therapy, physician assistants with different level access to the electronic medical record</p> <p>Risk: Inappropriately exposed PHI</p>	<p>Data Protection Platform supports multiple logins to single systems</p> <p>GuardianEdge Media Protection ensures that only approved devices can connect and that only approved file types can move from those systems</p>
<p>Department: Pharmacy</p> <p>Action: Reviews allowed portions of medical and pharmacy history for contra-indicators, fill prescription</p> <p>Risk: Exposure of PHI</p>	<p>Hard Disk Encryption protects against risks associated with physical loss or theft of the devices</p>
<p>Department: Discharge</p> <p>Action: Out-processing. Final information sent to billing department, patient's medical record sent to inpatient rehabilitation facility, health insurers, and primary care provider</p> <p>Risk: Exposed PHI (name, DOB)</p>	<p>Hard Disk Encryption protects against risks associated with physical loss or theft of the devices</p> <p>GuardianEdge Media Protection ensures that only approved portable devices can connect, that only approved file types can move from those systems and makes certain that any data leaving the platform is safe if the device or media is misplaced or stolen</p>
<p>Department: Outpatient therapy</p> <p>Action: Visiting therapist and visiting nurse work with patient (update progress) record time and patient progress for billing and for primary care follow up</p> <p>Risk: Exposure of PHI through device theft</p>	<p>Hard Disk Encryption protects against risks associated with physical loss or theft of a device</p>

Best Practices in Action

Achieving best practice status in compliance is not easy. Success requires planning and dedicated resources, staff, and management and technology. Let's take a look at two institutions that are best of breed. Each has a multifaceted solution that includes GuardianEdge technology.

Southwest Washington Medical Center

The Southwest Washington Medical Center is a mid-size, 450-bed hospital serving Southwest Washington near Portland, Oregon. The center has 100 physicians as part of its 3,200-member staff and supports an additional 400 physicians and works with 200 partners in the area. Southwest is one of only 40 hospitals to have won Top 100 Hospital® status six or more times in the last 14 years. This level of achievement carries over into its best practices in information protection and compliance.

Christopher Paidhrin is the HIPAA & IT Security Officer, ACS Healthcare Solutions at Southwest Washington Medical Center and has responsibility for PHI data. He believes that Southwest Washington Medical Center is the custodian of the patient's information and needs to control access to the data. Over the last few years he has led efforts to secure and protect information and endpoints by helping create a strategy based on analysis of risk, requirements and cost, and then implementing policy and procedures for training employees, implementing a mix of technology, and carrying out monitoring and auditing.

Southwest Washington Medical Center built policies and procedures to address federal and state regulations, analyzed its own workflow, and purchased identity and access management software. These workflow policy and procedures go as far as tightly controlling what goes into patient charts, who puts it in, and where it goes.

Employee education is a key part of their data protection strategy. On the day we interviewed Paidhrin, he was giving new hires required IT data protection training. Southwest Washington Medical Center also requires mandatory annual training updates for all employees.

Southwest Washington Medical Center implemented Active Directory single sign-on for its employees and extended it to cover approximately 3200 employees at 200 partners that include another 400 physicians in the local area. The hospital has a secure VPN linking to its 200 partners.

The Active Directory implementation gives the hospital physical control of data and RBAL (role based) control over 200 applications. Physicians, attending physicians, and other non-physician employees have specific access levels defined for patient information. The audit captured every login, program and screen access, file, and record access over the last five years.

In accordance with HIPPA regulations, Southwest Washington Medical Center has had a BAA (Business Associate Agreement) in place with its partners for the last five years. This agreement ensures that partners protect PHI according to Southwest's policies. Southwest Washington Medical Center audits partners every 90 days.

In 2008, Medical and Healthcare organizations were responsible for 14.8% of breaches and loss of 7,311,833 records

Identity Theft Resource Center, 2008 Stats report

Southwest Washington Medical Center has 50-60 visiting nurses, each with a laptop. All the laptops have GuardianEdge full disk encryption protection installed. To further reduce the risks, laptops are only loaded with the PHI needed for the patients that nurses will be visiting that day. Changes and updates are automatically synchronized with the main system when they return. The laptops are then updated to have only the information needed for the next day's visits.

The executive laptops are also protected by GuardianEdge software, even though they typically do not contain PHI. Southwest Washington Medical Center has had 4-5 laptops stolen in the last few years. All were encrypted and the data was protected.

Today, all USB ports and removable media on Southwest Washington Medical Center desktops and laptops are disabled. To streamline patient care, Southwest Medical is considering additional access to PHI data for physicians and staff by allowing use of these removable storage devices (USB keys, CDs and DVDs, etc.) and is considering GuardianEdge Media Protection to enable protected device connections and provide encryption to protect the data that will be allowed to move to those devices.

Select Medical

Brian Rusignuolo is the director of information security at Select Medical Corporation, a leading provider of specialty healthcare. From Select Medical's headquarters in Mechanicsburg PA, he oversees security for 91 hospitals, over 1000 rehab clinics, and 21,000 employees in 30 states. Select Medical also regularly adds new lines of business and facilities.

Rusignuolo's compliance strategy is to save Select Medical's staff from thinking about anything other than caring for the patients. This means technologies, policies, and procedures must work transparently. His strategy complies with HIPAA and makes business sense for Select Medical. "I can make things really secure but then the business can't operate: patient care has to move forward," states Rusignuolo. At the same time, he sees that HIPAA compliance is somewhat interpretative and can be viewed as "formalized common sense" of the things they should have been done anyway. Data breach legislation modeled on California's SB1386—with its breach notification and costs—has made endpoint data protection a real priority.

Like Southwest Washington Medical Center, Select Medical has developed policy and procedure, mandatory staff training programs, BAAs with partners, and has implemented Active Directory and role-based access. The fact that the 91 hospitals and 1000 rehab clinics in 30 states are managed from the Mechanicsburg site makes his security environment challenging. This mandates that the network can be managed, new software rolled out, and RBAL controlled from the headquarters location.

Select Medical has 21 independent hospitals and 70 *hospitals in a hospital* (HIH) where it occupies a few floors of another hospital. HIH co-habiting normally employs a model that keeps everything segmented from the host hospital: Select Medical's network, data lines, etc. Some of the HIH use patient services—radiology, labs, etc.—that are shared with the host hospital through endpoints hardwired to the "host" hospital network. Data sharing between the HIH and the host is starting to take off—as, for example, with Ohio Health in Ohio through private networks (VPN tunnel).

Hospitals underrate malicious intent in data breaches

... However, hospitals generally underestimate the malicious intent and the financial damage involved in data breaches and are unaware they're being targeted by perpetrators wishing to commit identity theft or medical fraud.

AMEDNEWS.com
American Medical Association
May, 2008

Select Medical was conducting a small pilot in a clinical setting involving 100 mobile devices. Then Select Medical acquired an outpatient division last year. Suddenly they had a new line of business with over 3000 therapists using wireless tablets to document the therapy and link up with Mechanicsburg for billing and record updates. The implementation had to be brought into HIPAA compliance quickly.

Vendor evaluation, pilot, selection and deployment of GuardianEdge Hard Disk Encryption software on tablets and desktop endpoints (10,000 total) took less than three months. They have had a couple of the GuardianEdge protected laptops stolen since then. However, since the information was protected and auditable, Select Medical was required to report the theft under the legislation's auditing requirements but was exempt from the notification sections of the rules.

Select Medical's staff uses smartphones for phone conversation and emails but not to make clinical decisions today. They are secondary devices and are not main devices. Still these devices represent a concern because the emails do sometimes contain private information (although attachments are encrypted). Typically, these devices contain no clinical information. Nonetheless, Select Medical plans to do a benefit vs. risk vs. cost analysis as they continue to look at smartphones as a potential applications platform.

Vendor evaluation, pilot, selection and deployment of GuardianEdge Hard Disk Encryption software on tablets and desktop endpoints (10,000 total) took less than three months. They have had a couple of the GuardianEdge protected laptops stolen since then. However, since the information is protected and auditable, Select Medical was required to report the theft under the legislation's auditing requirements, but was exempt from the notification sections of the rules.

Select Medical's staff uses smartphones for phone conversation and emails but not to make clinical decisions today. They are secondary devices and are not main devices. Still they represent a concern because the emails do sometimes contain private information (although attachments are encrypted). Typically, these devices contain no clinical information. Nonetheless, Select Medical plans to do a benefit vs. risk vs. cost analysis as they continue to look at smartphones as a potential applications platform.

Law requires health data breach notifications

The recently enacted economic stimulus law includes new requirements for how companies must notify people of breaches to their protected health information. Some experts say the rules could lead to federal breach notification requirements for other types of data.

*Federal Computer Week
February 27, 2009*

Endpoint Data Trends in Healthcare

Several key application trends are emerging that promise to reduce healthcare cost, improve access and enable quality patient care. Deployment of devices with these applications will drive future needs for enhanced data protection within hospitals, physician's offices, outpatient clinics, and mobile endpoints. These include automating the medical records in physicians' offices, hospitals, and at every point in the continuum of care, integrating the use of more mobile devices in patient care, leveraging and managing cellular partnerships and an opportunity to differentiate themselves in the patient care arena.

The future of hospitals, clinics, and physician offices depends largely on empowering all aspects of healthcare in real time, from any device and any location where: referrals, authorizations, and insurance claims are transmitted and processed electronically; prescriptions are written and renewed online; or providers and patients are discussing treatment plans. Hospitals, providers, clinics and physicians' offices, health insurers and Centers for Medicare & Medicaid Services (CMS) are demanding a more integrated and collaborative model of care. Secure endpoint technology is key to the success of this collaborative and connected healthcare infrastructure.

Small Practice EMR

Today only 28 percent of physicians have access to electronic medical records (EMR), mostly in the 7,500 hospitals and 16,000 large group practices. Automating the EMR within smaller practice groups will improve patient care and reduce costs. Securing the endpoints and complying with federal and state statutes for the two-thirds of the physicians in the 140,000 small practices (groups of eight or less), will mean either expanding the affiliated hospitals PHI protection umbrella or deployment of appropriate PHI protection policy and technology for the records housed in the small businesses.

The GuardianEdge solution can be extended to cover the offices as remote Windows networks managed by the host hospital's IT infrastructure.

More Mobility

More smartphones and laptops are going to be tied into hospital and clinical IT infrastructures. Today, only a small percentage of physicians are using smartphones for anything beyond communication. Increasingly, however, they will use these mobile devices to access the patient records, digital images and lab results remotely and use them to electronically write and send prescriptions to pharmacies. Increased use of EMR in smaller practices will force physicians to have remote access to the data including PHI, because they tend to operate a 24/7 business cycle.

Tablets and mobile devices increase the exposure as they move off-site. Rich clinical healthcare applications that have access to full patient data within the local network of a hospital will move to remote access and mobile devices. The nature of the mobile platform and the bandwidth of the remote connection will mandate that some PHI data is persistent on the mobile devices. These devices will be protected using GuardianEdge technology.

ePrescribing

ePrescribing is defined as entering a prescription for a medication into a data entry system (PC, PDA, tablet, or smartphone) and thereby generating the prescription electronically, rather than handwriting it on a paper form. As highlighted earlier in this paper, HHS is pushing for adoption of eprescribing. Doctors will now receive a "bonus" on Medicare payments for e-prescribing. After 2013, the bonus payments will be phased out and doctors will be penalized with lower reimbursement rates for not e-prescribing. Ensuring that each healthcare provider has safe and secure desktops, laptops, connected PDAs and smartphones technology and a HIPAA-compliant information security program is key to the success of this e-prescribing initiative.

These devices will contain PHI and will need to be protected with GuardianEdge technology.

M2M

Machine to machine (M2M) remote monitoring with wearable patient data collection devices is expected to grow in an effort to improve the coordination of care for chronic conditions. As the nation's population ages, the number of chronically ill Medicare beneficiaries is expected to grow dramatically, with serious implications for access, quality, and Medicare spending. With 15 percent of Medicare patients representing 75 to 80 percent of Medicare costs, CMS has initiated since 2003 demonstration projects to make the case for effective disease management model of care. Remote medical monitoring of chronic conditions (diabetics, chronic heart failure, etc.) by electronic devices is already happening (e.g., former Vice President Cheney's pacemaker has a radio in it so it can be monitored in real time).

The last 2 -3 days of a hospital stay following treatment are for monitoring and recovery. Beds run \$5,000 to \$7,000 per day. Third party payors and CMS, primarily responsible for the payment of care over the age of 65, are adopting the use of monitoring devices to reduce the cost of care of the elderly, disabled and chronically ill patient populations. CMS is rapidly increasing the use of M2M technology, as many countries are finding it more cost-effective to help patients manage their disease more effectively in their home. Additionally, as patients are kept home, the use of hospital services is reduced dramatically, as a result of a reduction in repeated hospitalizations. This increased homebased care will rely on mobile devices with data collected and forwarded to nurses, and primary care providers who can then manage their patients in real-time, avoiding the need of more costly services in the hospital setting. Many of these devices may contain PHI and will need to be secured.

Protecting these devices will require variations of GuardianEdge Smartphone Protection technology.

Conclusion

Protection of data on endpoints is a real priority for healthcare providers, but must exist within an environment where the first priority is patient care, and where that care—and patient data that it requires—is becoming increasingly mobile. Hospitals and other providers have grown a complex web of systems and applications that can leave PHI exposed on laptops, desktops, iPhones, smartphones, removable media and removable storage. At the same time, the pressures on resources and budgets have never been greater, resulting in the absolute requirement that solutions be implemented at the lowest possible TCO, and make maximum use of existing resources.

No vendor offers a better solution to these problems for healthcare providers than GuardianEdge.

A complete standards-based, enterprise-class implementation—To achieve a low TCO, GuardianEdge applications are implemented to support industry standard infrastructure, integrate with existing IT and business processes and provide a transparent user experience. The result is successful projects, fast rollouts, low deployment costs and low management costs.

A complete set of endpoint data protection controls—Including hard disk encryption, media protection (encryption and additional security controls) as well as iPhone and smartphone protection ensures that:

- Sensitive data remains inaccessible on lost or stolen devices
- Information does not inadvertently leak from an organization
- Risks from portable devices, media and WiFi network connections are reduced or eliminated

A track record of successful volume deployments—With over 1500 customers in healthcare, insurance, government, aerospace, manufacturing and finance as well as implementations of over 300,000 endpoints, GuardianEdge has clear and compelling evidence of deploy-ability and maintainability.

For healthcare providers, GuardianEdge offers a simple choice—a proven, easy-to-implement and low-cost solution to protecting PHI data on their laptops, desktops, smartphones, and portable media.

ABOUT GUARDIANEDGE

GuardianEdge is the leading provider of endpoint data protection for the enterprise. More than two million users around the world depend on GuardianEdge solutions to safeguard sensitive and proprietary information and ensure compliance with regulations for maintaining consumer privacy and to enable secure enterprise mobility. The company's endpoint data protection solutions have been deployed by leading organizations, including Lockheed Martin Corporation, Deutsche Bank AG and Humana Inc., as well as numerous agencies in the U.S. departments of Veteran Affairs, Defense, State and Education.

i On April 27, 2004, Presidential Executive Order 13335 called for the development and nationwide implementation of an interoperable health information technology infrastructure to improve quality and efficiency of health care and outlined a plan for most Americans to have electronic health records by 2014. This Executive Order established the Office of the National Coordinator for Health Information Technology under the Department of Health and Human Services.

ii CMS is authorized to investigate complaints of and make enforcement decisions for non-compliance related to the HIPAA security regulations. Enforcement of the HIPAA Privacy Rule is under the authority of the Office for Civil Rights (OCR). When privacy issues occur in the context of potential security violations, CMS and OCR collaborate to enforce the HIPAA rules.

iii In some states such as California, these laws include medical information and health insurance information. In some of the other States, the law actually states that a HIPAA covered entity is excluded. In other States, compliance with a more stringent law such as HIPAA can create compliance by default. The handling of medical records varies among States.

iv A copy of the Medical Identity Theft Final Report is available at <http://www.hhs.gov/healthit/documents/MedIdTheftReport011509.pdf>

v The Joint Commission evaluates the quality and safety of care for more than 15,000 health care organizations. To maintain and earn accreditation, organizations must have an extensive on-site review by a team of Joint Commission health care professionals, at least once every three years. The purpose of the review is to evaluate the organization's performance in areas that affect care. Accreditation may then be awarded based on how well the organizations met Joint Commission standards.

Corporate Headquarters
475 Brannan St., Suite 400
San Francisco, California
94107-5421
t. +1.800.440.0419
t. +1.415.683.2200
f. +1.415.683.2349

www.GuardianEdge.com

GuardianEdge is a trademark of GuardianEdge Technologies Inc.
All other products and services mentioned are the trademarks of their respective companies.