Healthcare Providers and Patient Data Security
Protecting Patient Data/Records
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOREWORD</td>
<td>1</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>2</td>
</tr>
<tr>
<td>TYPES OF DATA IN HEALTHCARE</td>
<td>3</td>
</tr>
<tr>
<td>COMMON CAUSES OF DATA BREACH</td>
<td>4</td>
</tr>
<tr>
<td>CONSEQUENCES OF DATA BREACH</td>
<td>6</td>
</tr>
<tr>
<td>RECOMMENDATIONS FOR DATA SECURITY COMPLIANCE</td>
<td>7</td>
</tr>
<tr>
<td>DATA SECURITY BEST PRACTICES</td>
<td>9</td>
</tr>
<tr>
<td>TRENDS IN THE FUTURE OF HEALTHCARE</td>
<td>10</td>
</tr>
<tr>
<td>HOW WINMAGIC SUPPORTS GREATER DATA SECURITY IN THE HEALTH SECTOR</td>
<td>11</td>
</tr>
<tr>
<td>CUSTOMER SUCCESS STORY: THE HOSPITAL FOR SICK CHILDREN (SICKKIDS)</td>
<td>12</td>
</tr>
<tr>
<td>CUSTOMER SUCCESS STORY: THE CHILDREN'S HOSPITAL</td>
<td>13</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>14</td>
</tr>
</tbody>
</table>
A 2012 independent study of 80 healthcare organizations, revealed a staggering amount of data security vulnerabilities. The study, the third of an annual series, revealed that the number of institutions that experienced a data breach has consistently increased. Furthermore, of those agencies, a significantly greater number reported experiencing multiple breaches (45 percent and 46 percent in 2012 and 2011, respectively, versus 29 percent in 2010). For healthcare agencies that participated in the study, the cost, or fiscal impact, of breaches (from 2010-2011) was substantial: $2.4 million, per institution (on average) and in a single data breach, 2,769 records were stolen (among study participants). Study participants estimated the average lifetime value of one lost patient (customer) at $111,810 – the potential total loss (should each patient compromised in a typical data breach be lost) could be in the hundreds of millions.

According to study participants, the consequences of data breaches for patients are no less concerning. Study participants estimated that of patients whose records were included in a data breach, 61 percent were at increased risk of financial identity theft, 59 percent were at increased risk of medical identity theft, and 70 percent were at greater risk of their personal health data being disclosed. Indicative of the universal concern about the state of data security among study participants, less than half felt their organizations were able to detect “all patient data loss or theft” and 67 percent didn’t feel their organizations had suitable controls or procedures in place to swiftly prevent and/or detect medical identity theft incidents.

This eBook will review data concerns specific to the healthcare sector; how data encryption addresses the unique data security challenges facing that sector; data security best practices, recommendations and trends for the health sector.
INTRODUCTION

In another age, a patient’s data was a paper document that lived in a very discrete group of files or folders somewhere behind the reception desk of a private practice or in the administrative offices of a hospital or clinic. Under these conditions, securing personal health information (PHI) was a relatively straightforward process – PHI was handled in areas only accessible by the appropriate personnel and kept safe behind lock and key. Hacking into it would require a highly concerted and conspicuous effort.

Today, healthcare providers work on a variety of systems: desktops, laptops, smartphones (or other mobile devices), tablets, and USB drives and routinely access PHI via those platforms. In fact, in the aforementioned study, 81 percent of participating organizations reported allowing employees and medical staff to use their personal laptops and mobile devices (a trend known as Bring Your Own Device - BYOD) to connect to provider networks or access company email, in spite of the fact that 54 percent do not believe these devices are secure (and with good reason, 65 percent of data breaches reported to Health and Human Services [HHS], between 2009 – 2011, occurred on laptops and mobile devices).

According to Experian, medical data theft increased by 50 percent last year. The current value of a healthcare record is approximately $50, more than a Social Security number or a credit card, making it a highly attractive "soft target." As the work of healthcare providers and third-party vendors becomes increasingly remote (an inevitable trend, according to insiders), data breaches can no longer be managed by merely securing the perimeter of a facility. It is perhaps for these reasons that many healthcare providers now view encryption as critical for any device that accesses their network.

Other data security challenges confronting healthcare providers include: vague U.S. federal regulations (i.e., recent upgrades to HIPAA and HI-TECH); inconsistent processes for full disk encryption on devices and insufficient implementation of automation of identity management; data leakage; and behavioral patterns that undermine data security.
COMMON FORMS OF PHI ACCESSED AND MANAGED BY HEALTHCARE PROVIDERS INCLUDE:

- Patient billing information
- Clinical trial and other research information
- Historical health records
- Employee information, including payroll data
- Administrative and scheduling information
- Accounting and financial information
- Email applications
- Productivity applications

A RECENT THREE-YEAR STUDY REVEALED THAT THE THREE FORMS OF DATA MOST SUSCEPTIBLE TO LOSS OR THEFT ARE:

- Patient billing information
- Employee records
- Non-patient records

THE SAME STUDY SHOWED THAT THE TYPES OF PATIENT DATA MOST OFTEN LOST OR STOLEN ARE:

- Medical files and billing and insurance records
- Payment details
- Prescription details
- Scheduling details
- Monthly statements
COMMON CAUSES OF DATA BREACH

In a nationwide roundtable (conducted in five sessions from 2011-2012), 100 healthcare providers discussed the challenge of managing information security in an environment that becomes more susceptible to data breach by the minute. Several common themes emerged: the rapid evolution of data security hazards, insufficient resources, inconsistent and/or inadequate data security practices, and the complexity of federal regulations surrounding data security, make keeping up with data security threats a full-time job – one that most providers have not provisioned for. Given the overwhelming majority of data breaches occur on laptops and mobile devices (65 percent based on HHS reports), this document will discuss that area of data security at length.

INSIDER NEGLIGENCE IS THE LEADING CAUSE OF DATA BREACHES

For the past two years, insider carelessness has topped the “top three” list of causes of data breaches in healthcare, followed by unintentional employee action, and third-party snafus, according to the three-year study and other industry sources. There are numerous examples of employee negligence-related data leakage, such as the case at Oregon Health & Science University (OHSU) which, in 2009, exposed the PHI of approximately 1,000 patients when an unencrypted laptop was stolen from an employee’s car. More recently at OHSU, the PHI of 14,000 patients were compromised when an unencrypted thumb drive an employee brought home without authorization was stolen. Even more infamous is the case of the 26.5 million veterans whose PHI (names, SSNs, date of birth, and other information) was breached when a laptop containing said data was stolen from a Veterans Administration (VA) employee’s home.
COMMON CAUSES OF DATA BREACH

2 ABSENCE OF BYOD POLICY AND/OR POLICY IMPLEMENTATION CREATES A “TARGET RICH” ENVIRONMENT

What unites these instances of data breach is the common practice of not encrypting the data of portable devices. Far from flukes, these examples are endemic of the sector. In a recent study of data security in healthcare, though the majority of providers had clearly defined procedures for securing BYOD, 46 percent admitted to not taking these precautions. In the nationwide healthcare provider roundtable, most participants acknowledged that while they believed policies should be in place to encrypt any device that accesses their networks, these policies were actually not enforced. More often than not, they lacked a formal BYOD policy altogether.

In Cisco’s 2013 report on BYOD, 59 percent of respondents who used smartphones to access PHI said they were not password protected, 53 percent accessed unsecured or foreign Wi-Fi networks, and 48 percent could not confirm if they disabled “discovery mode” on their Bluetooth devices and smartphones, which makes them extremely vulnerable to cyber-attack. In many organizations that participated in the two-year roundtable reported that it was not uncommon for doctors to email PHI to personal email addresses (even though this is a known HIPAA violation) which opens yet another portal for data breach, when that data is unencrypted.

3 UNENCRYPTED MEDICAL DEVICES POSE SECURITY RISKS

In addition to BYOD, medical devices, such as wireless heart pumps, mammogram imaging and insulin pumps, which also contain PHI, are most often unsecured (69 percent according to a recent study).

4 INADEQUATE SECURITY DEFENSES ARE THE NORM

Among the participants of the three-year study, 63 percent did not feel they had sufficient resources, 66 percent did not feel their security budgets were sufficient, and 60 percent and 55 percent felt their technology and personnel were insufficient to manage security issues, respectively.
The architects of malicious viruses (and other data breach threats) are continuously developing new ways to outwit and outmaneuver an IT department’s best efforts to circumvent data breaches. For the majority of healthcare providers included in the aforementioned roundtable and three-year study, an ad-hoc cost-benefit analysis was often used to determine the budget for security solutions, because of a reigning belief that data breaches will not happen at their facility and that the risks do not outweigh the costs of implementing them. This view has become increasingly incongruent in lieu of a slew of high-profile and extremely costly data breaches at healthcare facilities and third-party organizations and the new alacrity with which federal regulators can and will persecute HIPAA and HITECH violators.

One prime example is that of the Chattanooga, TN-based healthcare insurer BCBST. A facility leased by BCBST was robbed and 57 unencrypted computer hard drives were stolen. The drives contained health plan identification numbers, SSNs, and diagnosis codes, as well as sensitive member demographic information. When the dust settled, the total cost of the BCBST data breach came to $23 million ($6 million for additional data encryption and close to $17 million for protection, investigation and member notification). The $1.5 million settlement paid to HHS was the first to occur as a result of a HITECH Breach Notification Rule enforcement action.

If this reaction sounds excessively punitive, due consideration must be given to the other potential consequence of healthcare data breaches, namely, that medical identity theft has resulted in inaccuracies in patient treatment (39 percent of organizations surveyed in the three-year study indicated that this had caused inaccuracies in a patient’s medical record and 26 percent reported it had affected the patient’s medical treatment). The worst-case scenario of medical identity theft is potentially fatal.

According to the three-year study and other industry sources, the cumulative economic impact of data breaches in the healthcare industry has reached $7 billion per year, monetary loss notwithstanding. The less-tangible long-term costs to healthcare providers – critically damaged reputations, fractured patient (customer) trust, and short- and long-term patient repercussions – make this “hot button” issue one that healthcare providers and third-party organizations must find more effective ways to address.
The United States’ Health Insurance Portability and Accountability Act (HIPAA) of 1996 is anchored by the twin goals of: 1) "Standardizing the electronic exchange of data between health care organizations, providers, and clearinghouses", and 2) "Protecting the security and confidentiality of protective health information.” To that end, a set of privacy standards has been disseminated by the Department of Health to ensure healthcare organizations, health plans, and providers (which "access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured PHI") adopt the guidelines of the Act and are held accountable to them. Those guidelines include stipulations about where healthcare data is stored and how it is protected from unauthorized access, in alignment with the overarching mandate of the Act that PHI remain secure at all times.

There are four principal goals of Canada’s Personal Health Information Protection Act of 2004 (PHIPA), of which the first two are: 1) to "protect the confidentiality” of PHI and 2) to protect “the privacy of individuals with respect to that information”.

**Encryption Supports HIPAA and PHIPA Compliance**

Section 64.312(a)(2)(iv) of HIPAA requires that applicable agencies implement "...a mechanism to encrypt and decrypt EPHI.” Furthermore, Sections 164.312(e)(1) and 164.312(e)(2) (ii) both of which address methodologies of protecting PHI from unauthorized access, can economically and efficiently be satisfied through data encryption.

Schedule A, Section 12 (1) of PHIPA (Ontario/Canada) states, "A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian’s custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.”

Schedule A, Section 13 (1), of PHIPA requires that “A health information custodian shall ensure that the records of personal health information that it has in its custody or under its control are retained, transferred and disposed of in a secure manner and in accordance with the prescribed requirements, if any.” Both of these mandates can be addressed by employing data encryption.
RECOMMENDATIONS FOR DATA SECURITY COMPLIANCE

HITECH ACT COMPLIANCE FOR CES AND BAS
The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 expanded the reach of HIPAA to “HIPAA covered entities [CEs] and their business associates [BAs] that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information…” Prior to HITECH, HIPAA only covered CEs, resulting in widespread data breaches of PHI among BAs. HITECH mandates data breach notification for any breach of PHI involving 500 or more records.

ENTITIES COVERED UNDER HITECH ACT COMPLIANCE REQUIREMENTS INCLUDE THE FOLLOWING:

- Contracted lab and radiology departments
- Third-party billing agencies
- Medical transcriptionists
- Hospital couriers
- Collection agencies
- Consultants
- Pharmacies with hospital contracts
- Off-site storage facilities

The specificity of HITECH, (i.e., breach notification of unsecured PHI that was not rendered “unreadable, unusable or indecipherable” to unauthorized individuals), form the Canines of the Act. While HITECH does not require data encryption, it makes data breaches of “unsecured PHI” an enforceable violation, thereby making preemptive measures of protecting PHI, such as data encryption, a less costly response. Under the provisions of HITECH, CEs and BAs must not only notify all affected individuals of any data breach (of 500 or more records), but must also notify Department of Health and Human Services (HHS), and, if the breach affects more than 500 people in a particular location, prominent media. Furthermore, these breaches are posted on HHS’ “Wall of Shame” for public review, further compounding the damaged credibility of the reporting entity.

By preemptively encrypting all PHI, organizations can avert the potentially devastating consequences of a HITECH enforcement action. To round out a CE’s data security program, insiders recommend taking a holistic approach to developing one that includes robust data protection, clearly defined and implementable identity and access management policies, and the appropriate technology to automate those policies, thus freeing up healthcare staff and third-party vendors to focus on quality member care and the administration of their facilities. In the subsequent section “Data Security Best Practices”, we’ll discuss a general framework for such a dynamic data security program.
The healthcare environment is a matrix of interrelated data that flows from patients/customers to physicians, diagnostic clinicians, lab techs, pharmacists, medical insurance billing specialists, in-home care providers, convalescent and/or rehab facilities, outpatient clinics, permanent and visiting nurses and various BAs. Synchronizing these interdependent institutions would be an impossible feat, but creating a data security program that safeguards data shared across them is more than doable with current data encryption technology.

DEVELOP A HOLISTIC SECURITY PROGRAM
To ensure the highest levels of data security continuity, healthcare providers can and must look beyond mere data security compliance and towards the best long-term data security strategy. Comprehensive strategies are centered on protecting data, not devices. Insiders recommend taking a granular approach to allowing data access and control (e.g., role-based identity management, and automated authentication). To retrofit an organization’s data security program and employ the strongest measures to safeguard PHI, insiders recommend the following:

1. Shift the paradigm from short-term cost-benefit analysis and the attendant reactive stance typical of healthcare providers on data security strategy, by reframing it as a business imperative which can and does impact revenue, by giving due investment to the human and technological resources necessary to create a greater data security fortress.

2. Define the BYOD privacy policy and implement vigorous access controls and disseminate to all CEs and BAs. (A recent Ponemon study found that a substantial percentage of BAs did not know that HITECH PHI standards applied to them.) The policy should address risks for BYOD usage, procedures to be followed, and reinforce employee adoption through education on how to avoid risky behaviors.

3. If your organization hasn’t already done so, consider having the IT privacy and security chief report directly to the board of directors.

4. Make privacy and security risk assessment an annual (or periodic) occurrence, to better gauge where the organization may be (or is) leaking data and what behaviors are contributing to that.

5. To address ownership concerns among BYOD users, institute BYOD policy that all PHI must be encrypted on those devices. A good encryption solution can provide both full and partial disk encryption.

6. Implement sufficient controlled access (e.g., to facilitate fluidity for practitioners working via mobile devices, controls can allow them to access data without being able to pull it off the system).

7. An organization’s HIPAA- (or PHIPA-centric) policy needs clearly defined consequences for each type of infraction, if guidelines are to be optimally adopted (regardless of an individual staff member’s value).

8. Have a BA agreement on file with any cloud application provider you use to disseminate PHI.

9. Once the data security strategy has been defined, organizations need to create a framework for sustaining it (e.g., a routine briefing by the IT manager of the CEO [or board] on critical current data security issues would help them stay abreast of those issues and support more informed and relevant data security strategy).
TRENDS IN THE FUTURE OF HEALTHCARE

In the two-year roundtable, panelists identified sharing information across multisite facilities, via Health Information Exchanges (HIE), open access, and wireless technology, and Accountable Care Organization as looming threats to healthcare PHI security. Of those present and future concerns, securing data over mobile devices was “top of mind” and encryption was universally expressed as a major concern. BYOD usage was seen as an emerging trend and, among the majority of providers, a potential source of future cost-savings. Though seldom done, panelists concurred that they will be obligated to conduct routine risk assessments, in future.

The trend of mobility and BYOD shows no signs of abating and is considered a major threat to PHI security. A recent Ponemon study underscored the importance of not merely securing data stored on mobile devices, but also protecting data simply accessed by mobile devices (such as smartphones and tablets). Current estimates of healthcare organizations that allow BYOD to access their networks range from 81 percent to 89 percent, signaling the significant presence they have in the data landscape and the need for addressing mobile data security via policy and practice in healthcare institutions and third-parties. In the subsequent section we’ll discuss solutions to securing PHI accessed at-rest and by mobile devices.
HOW WINMAGIC SUPPORTS GREATER DATA SECURITY IN THE HEALTH SECTOR

A key element of the allure of mobile and BYOD usage in healthcare is accessibility. The tug-of-war between having continuous access to PHI via mobile or BYOD (for clinicians) and restricting that access (to ensure greater data security) has been at the crux of the industry-wide trend of substandard protection of PHI on those platforms. For optimal PHI security, experts recommend that data is encrypted on both at-rest and mobile devices. That encryption needs to be translucent enough to operate behind-the-scenes, integrate across platforms seamlessly, and offer no disruption to the user-experience, in order to bridge the IT – clinician divide.

WINMAGIC’S SECUREDDOC PROVIDES:

- Protection of patient data and personal information on laptops, desktops, tablets, mobile devices, and associated removable media including USB thumb drives and CD/DVDs.
- Auditable compliance with legislated security requirements for personal health information including the Health Insurance Portability and Accountability Act (HIPAA) [USA], the Personal Health Information Protection Act (PHIPA) [Ontario/Canada], and similar legislation worldwide.
- Continuity of access to critical computers and data storage devices in the event of forgotten passwords or other mishaps to authorized users.
- Prevention of data leakage to unencrypted removable media (CD/DVD/USB).
- Avoidance of breach notification costs and the associated negative publicity caused by a data breach.
- Support for shared computer assets containing PHI by multiple authorized users in varying roles.

Additionally, SecureDoc meets FIPS 140-2 requirements, a key component of the HITECH Act, and provides encryption processes for data at rest consistent with National Institute of Standards and Technology (NIST) guidelines.
CUSTOMER SUCCESS STORY:
THE HOSPITAL FOR SICK CHILDREN (SICKKIDS)

**Challenge:** Protecting confidential patient data on the laptops of an increasingly mobile user community across multiple locations.

The Hospital for Sick Children (SickKids) is Canada’s most research-intensive hospital and the largest children’s centre. To ensure total PHI-security on multiple platforms, Sick Kids conducted a rigorous Proof of Concept evaluation of three of the top providers of data encryption solutions. Crucial to success was the ability to protect data on Windows and Mac laptops, integrate with existing security applications, unencrypt data, provide data recovery capabilities, support security policy protocols, offer client management and monitoring capabilities, auditing and reporting capabilities and preboot authentication functionality. Only SecureDoc met all of SickKids’ data security requirements.

Pilot testing of 25 laptops used by physicians, administrators and researchers, amply demonstrated that SecureDoc integrated with SickKids’ complex environment, enabled administrators to centrally manage laptops as well as removable media from a single central console, and did not interfere with patient care.
CUSTOMER SUCCESS STORY:
THE CHILDREN’S HOSPITAL

Challenge: Protecting confidential patient data on the laptops of an increasingly mobile user community across multiple locations.

One of the top children’s hospitals in the United States, The Children’s Hospital, in Denver, Colorado, has over 1,000 pediatric specialists and more than 3,500 full-time employees devoted to caring for kids of all ages. To retain the trust the hospital has built in its more than 100 years in existence, the hospital needed a way to ensure that PHI shared by its medical staff which serve on the main campus, campus, two emergency locations, three community-based after-hours care sites, nine specialty care centers, and more than 400 outreach clinics, on laptops would remain secure at all times.

The Children’s Hospital realized that the most effective way to protect PHI was by deploying full-disk encryption. “We looked at both whole-disk and file encryption, and found that while whole-disk encryption ensured that no data on a laptop could be accessed by any means,” explained Andrew Labbo, Privacy and Data Security Officer and Information Security Manager at The Children’s Hospital.

“We with file encryption we could not be certain that all data was protected and would still have to undergo the painful process of notifying all patients in the event of a lost or stolen laptop. Whole-disk encryption also met all HIPAA (Health Insurance Portability and Accountability Act) requirements that call for a mechanism to be put in place to protect data at rest on laptops.”

After two months of extensive testing of five different solutions, The Children’s Hospital chose Winmagic’s SecureDoc. “It had the flexibility to integrate with our existing technologies while its versatile installation options meant that busy medical staff would not be disrupted during the installation of the encryption.” Another month of piloting SecureDoc confirmed they had made the right choice, “The support staff confirmed that we could fully integrate the encryption software with existing technologies,” noted Labbo. “We also confirmed that there would be no disruption associated with adding the encryption layer as users could continue to use their computers while it installed in the background.”
CONCLUSION

Study after study reveals that a significant percentage of healthcare providers (despite recent data breaches) remain entrenched in outmoded privacy practices and lack control over third parties’ use of PHI they provide, making them doubly vulnerable to compliance regulation violations. Ramping up data security measures (especially of mobile and BYOD) are top priorities. Internal strategies toward this end include: training internal staff, restricting user access, and revising contracts with BAs (and BA subcontractors) to properly ensure an organization’s data security aligns with federal guidelines.

By circumventing unauthorized data access via user sign-on (and password protection) and encryption, which offer a much broader degree of data security than the firewall of a decade earlier, organizations can minimize the risk of data breaches, regardless of their size. Extending data security programs beyond a provider’s own organization to its BAs and their subcontractors and enforcing individual accountability for, and staff awareness of, the repercussions of data breaches (especially due to negligence or unintentional acts) are viewed as critical components of long-term data breach reduction.

WinMagic provides the world’s most secure, manageable and easy-to-use data encryption solutions. With a full complement of professional and customer services, WinMagic supports over five million SecureDoc users in approximately 84 countries. We can protect you too.

For more information on SecureDoc Enterprise Server contact sales@winmagic.com or visit our website to access a number of valuable resources:

PRODUCT PAGE
http://www.winmagic.com/products

WHITE PAPERS
http://www.winmagic.com/resource-centre/white-papers