

KEEPING THE PROMISE OF PRIVACY

Protecting Sensitive Data in Healthcare Organizations



A Frost & Sullivan White Paper

Sponsored by RSA, the Security
Division of EMC

TABLE OF CONTENTS

TABLE OF CONTENTS

Embracing the Digital Future in Healthcare – Are you Ready?	3
Benefits of e-Health	3
e-Health Initiatives Create Security Challenges	5
Provisioning of Patient Care	5
Consumer Awareness of the Importance of Privacy	6
Regulatory Compliance	6
Portability of Electronic Personal Health Data	8
The Growth of e-Health Initiatives	8
The Medical Information Lifecycle	9
Data Mismanagement	9
National Health Service (NHS), United Kingdom	10
Veterans Administration (VA), United States	10
Large Health Insurer, United States	10
Hacking and Fraud, Global	10
Advantages of a Strategic Approach to Securing Patient Data	10
Compliance	11
Containing Costs	11
Greater ROI on Security Investments	11
A Framework for an Information Risk Management Strategy	12
Discover and Classify	12
Define Policy	12
Enforce Controls	13
Report and Audit	13
Conclusions	13

EMBRACING THE DIGITAL FUTURE IN HEALTHCARE – ARE YOU READY?

The rapid evolution of technology has led to many innovations in providing patient care delivery. Concepts such as Electronic Health Records (EHR), Computerized Provider Order Entry (CPOE), and Telemedicine, are being implemented in healthcare organizations around the world. The end result of these transformations is that the majority of healthcare information is rapidly becoming digital. To reap the full benefit of this digital transformation, the business needs to be proactive and vigilant in mitigating the risks associated with protecting digital information. Digital health information will be created, transmitted, accessed, and stored across a complex IT infrastructure with a diverse set of clinical and non-clinical users and access points.

Without a well-defined strategy for managing the risk associated with this information throughout its lifecycle, healthcare organizations will struggle to derive full value from their technology investments. On the other hand, those organizations that implement an effective information risk management strategy as part of their digital transformation will see how the benefits of demonstrable security and privacy enhance their business.

This paper outlines briefly the types of transformations that are occurring, illustrates the challenges that digital health information is creating, and describes the core elements of a strategy to manage information risk to address these challenges.

BENEFITS OF E-HEALTH

The benefits of embracing the e-Health concept are enticing enough that efforts are being made in both developed and developing countries. The ability to connect departments and backend systems together creates an opportunity that ultimately improves efficiencies to levels that are impossible to achieve with paper documents, films, video tapes, DVDs, and non-consolidated computers or databases. These efficiencies include:

- **Improved patient care safety** – decreased time to diagnosis and treatment, continuity of care between physicians, enhanced prescription management between specialists, and more
- **Streamlined business processes** – rapid invoicing, credit card processing, insurance coverage approval, etc.
- **Physician productivity enhancement** – data availability to make better diagnosis and treatment decisions more rapidly, ability to make detailed patient notes without misplacing the paperwork, sufficient time savings to treat more patients
- **Improved patient care quality** – better outcomes for patients diagnosed with certain diseases, ability to view past patient data to enhance current treatment regimen, fewer incidents of misdiagnosis, reduced length of hospital stays and costs
- **Cost efficiencies** – reducing costs to the insurance provider, the patient, and the hospital

All of these efficiencies lead to higher satisfaction among the clients (patients) as well as the ability to reduce operational overhead and increase revenues by enhancing organizational productivity. However, these efficiencies highlight the need to protect information regardless of where it is located. A healthcare organization needs to evaluate where to invest, why to invest, and how security investments map to critical business needs and these new efficiencies.

A healthcare organization must deal with internal issues during the deployment of any of these platforms and applications. Changing to such systems requires a change in mindset among users, which include a wide variety of caregivers including physicians and nurses. Legislation helps force the issue but the healthcare providers must be able to quantify these efficiencies in a tangible Return on Investment (ROI) model that will help users see the benefits of such systems.

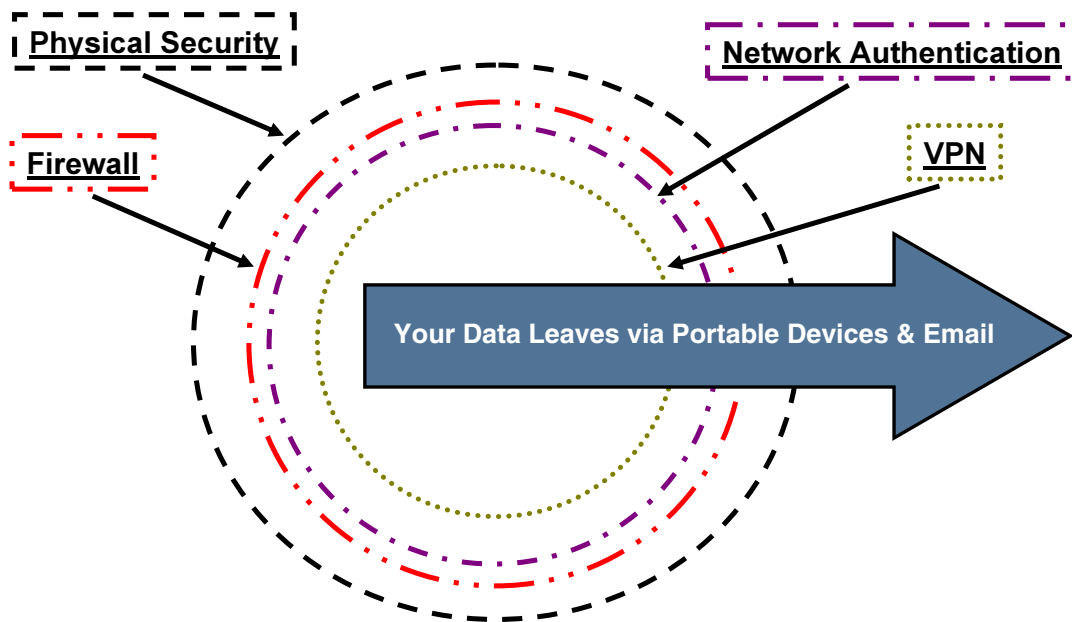
The healthcare organization's internal capabilities in addition to developing an ROI model need to be assessed before investing in e-Health platforms. As healthcare providers around the world undertake initiatives to embrace the digital future, there are serious issues that these organizations have to cope with during this industry-wide evolution, including:

- **Data volume** – computer use in the exam room, digital imaging modalities, test results, customized treatment plans, invoicing, etc., all put an enormous demand on storage growth.
- **Data access** – many healthcare organizations of all sizes have implemented technology that includes computers at nurses' stations, in every exam room, and in offices, in addition to mobile devices, remote workers, and patient portals, all with potential access to private medical records.
- **Data portability** – with the increase in technology usage and dependency many computer systems supporting electronic medical records in digital format are easier to access and distribute.
- **Interoperability** – connecting disparate databases and systems is important to capture older data and integrate past patient results.

Thus an obvious drawback to the digital future for the global healthcare industry is the difficulty in securing this highly sensitive and private information. In fact, the traditional concept of concentric circles of security (Figure 1) may not be sufficient in the case of hospitals and large teaching hospital systems due to widespread use of email as well as portable storage devices such as USB drives and microSD cards.

Access to these records through devices or portals increases the chances of highly sensitive data falling into the wrong hands. The next phase of e-Health is creating secure processes and controls that prevent any data theft while enhancing the experience of the patient.

Figure 1 – Traditional Concept of Concentric Circles of Security



Source: Frost & Sullivan

E-HEALTH INITIATIVES CREATE SECURITY CHALLENGES

Provisioning of Patient Care

The adoption of an electronic health record is an important component of e-health initiatives and an area where the highest security risk lies. The EHR is the front end that will be viewed by the user, but will in fact draw its information from many backend data sources. Frost & Sullivan research has found that in organizations without implemented EHR initiatives, the time from a patient's initial consultation to diagnosis and conclusion of the recommended treatment can be up to 40% longer than in an organization with a comprehensive EHR system. In the majority of cases, the longer time associated with patient diagnosis and treatment may lead to physician frustration and patient dissatisfaction. In a smaller number of more serious cases, the lag between consultation and treatment can lead to negative long-term health problems or even death, depending on the situation.

The importance of EHR in the current and future setup of hospitals increases the security risks. In 2007, the board of the e-Health Vulnerability Reporting Program assessed the security risks associated with EHRs in a 15-month study. The researchers evaluated current industry information security practices, benchmarked healthcare information security practices against other industries, and produced a set of recommendations for better protecting EHRs. The study included a survey of more than 850 provider

Frost & Sullivan

organizations and penetration testing of seven e-health systems, including five ambulatory EHR systems certified by the Certification Commission for Healthcare Information Technology, or CCHIT. The researchers concluded that EHRs were at risk and unless changes were made to current systems, patients would not trust these systems to protect their privacy. Whether this involves improving the certification process or creating better practices there definitely is a need to improve security. CIOs are also viewing security as a long-term threat. At the 2008 HIMSS Annual Leadership survey among CIO's security was found to be one of the larger issues.

- 97% of healthcare CIO's are concerned about the security of data within their healthcare organization.
- 51% reported that internal security breach is a top security concern.
- 24% admitted to a security breach in the past six months.

Consumer Awareness of the Importance of Privacy

Businesses in all industries around the world have been the victims of data breaches that have negatively impacted both the organization as well as its customers. Over the past decade, media and law enforcement have successfully raised consumer awareness of the issue of data privacy in order to combat identity theft, fraudulent credit card charges, and more. Consumer awareness of the importance of data privacy has placed higher demands on healthcare providers due to the fact that unauthorized access to health-related data can have unique and far-reaching implications for patients.

A data breach at a hospital cannot only expose the credit card and bank account information of a patient, it can also provide a data thief with the information to seek medical care using the insurance of another person. Furthermore, medical identity theft can have a serious detrimental impact on the ability of the "victim" (i.e., patient) to obtain private health insurance in the future, and can place the life of a victim in danger as the medical history of two or more people are combined into a single health data record. Accessing the detailed medical history of a patient can also create issues from a provider standpoint as any change in these records could potentially lead to the death of the patient. This worst-case scenario can expose a hospital to civil lawsuits, negative publicity, and heightened regulatory oversight in countries with enforceable data privacy laws.

Regulatory Compliance

Healthcare providers in a variety of countries around the world have a legal obligation to protect the data privacy of the patients they serve. While these regulations have differing penalties for non-compliance, they demonstrate a growing global awareness of the importance of data privacy and protection for sensitive data such as EHRs and associated

financial payment records. Examples of global regulations that healthcare organizations must comply with include, but are not limited to:

European Union	Directive 2002/58/EC – The EU directive on privacy and electronic communications requires the 27 EU member states to harmonize national laws regarding data security to protect the confidentiality of communications.
United States	The Health Insurance Portability & Accountability Act – HIPAA requires the protection of healthcare data for individuals and has direct implications on information security, data retention, and eventual disposition. In addition, HIPAA compliance extends beyond healthcare providers to insurance companies and public sector agencies.
Canada	Personal Information Protection and Electronic Documents Act – PIPEDA regulates how private sector organizations collect, disclose, and use personal data in the course of business. This regulation was expanded in 2002 to specifically include the healthcare sector.
Australia	Privacy Act – This act established 11 privacy principles with principle 4 addressing the storage and security of personal information. The act requires businesses with access to personal information to implement measures that prevent loss, unauthorized access, modification, disclosure, or misuse of such information.
Japan	Japan Personal Information Privacy Act – JPIPA governs the distribution of personal data to protect individual rights and welfare while preserving the usefulness of personal information. JPIPA establishes policies for handling personal data, measures for protecting personal information, and obligations for businesses that handle personal data.
Global	Payment Card Industry (PCI) Data Security Standard – PCI DSS is a security standard that is supported by the credit card industry worldwide, which effectively makes it a self-imposed regulation. Via PCI DSS all organizations that transmit, store, or process credit card transactions are required to comply with the data security standard or risk fines and loss of the ability to process credit card payments.

These are acts that help govern healthcare data in a particular country based on legislation. There are also standards developed by the International Standards Organization (ISO) that can be attained by healthcare entities around the world and thus are harmonized across regions with differing content.

- **ISO 27799** is an information security standard developed by the International Organization for Standardization (ISO). Its title is *Health informatics – Information security management in health using ISO/IEC 27002*. The purpose of ISO 27799 is to provide guidance to health organizations and other holders of personal health information on how to protect such information via implementation of ISO/IEC 27002.
- ISO/IEC 27002 provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing, or maintaining Information Security Management Systems (ISMS).

Portability of Electronic Personal Health Data

Consolidated e-Health data is meant to be leveraged first and foremost by healthcare providers and administrators for diagnosis, treatment, invoicing, claims, etc. The challenge of having this type of data in electronic format is the increased potential for it to be accessed without authorization. The data could be inadvertently shared as a result of an email or an unattended computer station, or it could be intentionally stolen by hacking a portal that the patient or provider may access.

As mentioned earlier the traditional concept of concentric circles of security may be insufficient to protect personal health data. We live in a world where reporters pay hospital employees for information about famous patients, and gigabytes of information can be stored on portable devices as small as a fingernail, which can be easily overlooked during security searches. This coupled with the lack of security within healthcare organizations makes it a greater threat. The slightest negligence may give others the ability to view data they are not authorized for.

Although easing data portability between hospitals and physicians can be beneficial to both the patient as well as the hospital seeking to lower operational costs, the fact remains that one of the largest security threats to an organization are its own employees. Healthcare organizations require a security plan in place to protect data even after it has been placed on a portable storage device or attached to an email and taken outside of the organization. As stated earlier from the HIMSS survey, 97% of CIOs are worried about a security breach within their healthcare organization.

THE GROWTH OF E-HEALTH INITIATIVES

e-Health initiatives are being implemented around the world, making the trend towards complete electronic medical records a global rather than regional phenomenon. This has far-reaching implications for patients and healthcare providers alike because it provides an opportunity to share information with large healthcare organizational networks, ambulatory centers, imaging facilities, physician practices, and patients. The importance of these platforms becomes evident when a patient requires medical attention in a geographic area outside of their provider network. When the attending physician can immediately access the health history of a patient electronically without waiting for faxes, couriers, or express document shipments, this benefits both physicians and patients. In addition to reducing costs for healthcare providers, the ability to selectively send data on request to authorized providers in other regions or countries will at a minimum improve invoicing, patient satisfaction, and patient care, but more importantly it will contribute to saving lives, which is the goal for hospitals around the world.

The Medical Information Lifecycle

Unlike some industries where customer records have archive requirements of 10 years or less, the information lifecycle for medical records has vastly different requirements. In many parts of the world, medical records must be kept for the life of a patient, and in some countries, for one to two decades after death. With each year, the amount of data in an individual's health portfolio grows and can become more susceptible to potential misuse, accidental deletion, or accidental distribution due to the number of professionals that must access these files over the life of a patient. In today's environment of identity theft there can be issues with the ability of an unauthorized user accessing this data. After gaining access, unintentional distribution and data loss can affect the patient currently or the patient's family even after death.

Complicating matters further is the use of Continuity of Care Records (CCRs) within personal health record systems that provide a brief synopsis of recent visits to physicians and significant additional data about the patient. Since CCRs were developed for easy data transfer over a network connection, flash drive, or smart card in easy-to-read formats such as XML, PDF, or Microsoft Word format, copying and sending healthcare-related data from a protected network and storage archive may become a part of daily business operations for some hospitals. However, once the data has been removed from an environment protected by locked doors, firewalls, intrusion detection systems, network access controls, and secondary safeguards such as RFID tokens¹, EHR data can potentially be accessed and used for unauthorized purposes.

In many countries, the healthcare organization's responsibility for the protection of personal health-related data doesn't end when data has been copied and sent to an insurance company, or another healthcare provider. Healthcare organizations must have a plan to not only protect healthcare data and associated CCR data within the physical confines of the organization, but also when that data is copied and sent somewhere outside of the network.

DATA MISMANAGEMENT

As much as e-Health promises to advance patient care and the business operations of healthcare organizations, the fact remains that securing electronic data is a task that neither private enterprise nor government tends to do well on their own. This is no surprise since the core competency of hospitals is providing healthcare to patients rather than preparing for any number of possible ways that sensitive or private data can be lost.

1. Some hospitals such as Kaiser Permanente (www.kaiserpermanente.org) utilize RFID proximity badges in combination with passwords to access EHRs. When a sensor indicates that the user with the RFID badge has moved away from the computer, the system automatically shuts down access to the computer.

Examples of data mismanagement in both the public and private sectors are plentiful:

National Health Service (NHS), United Kingdom

In December of 2007, it was revealed that hundreds of thousands of files containing patient data had been lost by nine separate National Health Service trusts in the United Kingdom. Although in some instances the files were password protected, not all of them were encrypted. Nor did they have digital rights management safeguards in place to prevent data tampering.

Veterans Administration (VA), United States

Despite the wake up call in May 2006 for the Veterans Administration when a massive data breach compromised the personal data of up to 26.5 million veterans and included disability rankings, the VA has yet to find a way to secure veterans' medical data. This has been illustrated with the loss of data on up to 1 million physicians and patients from the VA Medical Center in Birmingham, Alabama. Also, in June of 2008 patient information was exposed in a security breach at Walter Reed Army Medical center in Washington, D.C.

Large Health Insurer, United States

A private healthcare provider revealed that information that included Social Security numbers, pharmacy, and medical data for up to 128,000 patients in several U.S. states was unprotected and exposed online for an undisclosed amount of time during 2007.

Hacking and Fraud, Global

An organization that works closely with healthcare organizations has recorded an 85% increase in the number of attempted attacks directed specifically at the healthcare sector. Attempts to breach data at healthcare providers increased from 11,146 per healthcare client per day in early 2007 to an average of 20,630 per day by the end of January 2008. This trend illustrates the intent of criminals to obtain patient information for fraudulent purposes. It also brings to light the uncomfortable fact that not all hacking attempts are prevented, as security researchers² proved in May of 2008 when healthcare information for patients from across the United States, Europe, and the Indian sub-continent were found on a server connected to the Internet.

ADVANTAGES OF A STRATEGIC APPROACH TO SECURING PATIENT DATA

When numerous organizations in both the private sector and the government have a difficult time securing patient data, it is worth taking a step back to view the problem

2. Researchers at the security firm Finjan reported this information on May 6, 2008.
<<http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP>>

from a higher level in order to get a better picture of the task at hand and ensure that critical areas aren't ignored. Areas to consider include, but are not necessarily limited to:

Compliance

When considering the issue of compliance, it should be remembered that governance and regulatory compliance frequently dovetail with each other and are not mutually exclusive. Thus, it becomes important to consider what compliance really means for the organization and what effect non-compliance with internal policies could mean for a hospital or healthcare organization. Frequently, employees in an organization view certain policies as an annoyance rather than something that was created as a safeguard to protect against potential outside liability. Keeping employees focused on the reasons for internal policies and external regulations helps keep the entire organization more secure and ensures increased support for enhanced information security measures as they are introduced. Adoption of these systems also plays a part in the compliance issues. These policies need to be tested over various scenarios before widespread adoption. Compliance is one of the biggest reasons for internal security breaches.

Containing Costs

Cost containment is the goal of any business, and the healthcare industry is no exception. The cost of implementing all the platforms that would define e-Health systems can be daunting for some, but the ability to better serve patients, improve business processes, reduce overhead costs, and enhance productivity can't be ignored. However, in order to achieve those objectives, a comprehensive information security plan should be in place that protects against some of the most common security issues such as:

- Lost or stolen laptops, USB drives, back-up tapes, CDs, or Smart Cards.
- Accidental distribution of patient data via email systems.
- Unsecured computers in exam rooms or work stations.
- Unauthorized access through breaching online portals.
- Stealing patient information and using it to access personal health data.

If these basic issues cannot be adequately planned for, implementation of these platforms should be postponed until a security plan has been established. Without a comprehensive security strategy to deal with these most basic security weaknesses, these systems can subject an organization to outside liability in excess of the cost benefits promised by the solution.

Greater ROI on Security Investments

Security spending is typically seen as a cost center within most organizations — hospitals and other healthcare organizations are no exception. Historically many organizations have found that security investments have brought little noticeable monetary rewards and

in some cases were more of a nuisance than a solution. As a result, upper management is often hesitant to spend any more money on security than is necessary.

However, compliance, cost containment, and improved quality of care are tremendously beneficial to healthcare organizations and are especially important to executives. The key is to educate executive-level personnel on the correlation between making strategic security investments and generating a greater ROI. Comparing even just the hard costs of a well-known data breach against the cost of implementing a solution before the incident occurred can be very eye opening.

A FRAMEWORK FOR AN INFORMATION RISK MANAGEMENT STRATEGY

One of the main challenges with making strategic security investments is that it is difficult for most organizations to know where to begin. Frost & Sullivan believes that there are four key areas that organizations must consider to create a customized Information Risk Management Strategy.

Discover and Classify

In order to protect all sources of sensitive data, the organization must first discover and classify that sensitive data. Sensitive data does not only consist of patient data, but also includes sensitive staff and business data. The organization must also consider all the possible places where sensitive data may reside. This could include databases, laptops, PDAs, email, and proprietary billing and diagnostic systems.

There are technology solutions designed specifically to help organizations discover and classify data for the purposes of securing it. Using these solutions, especially if the vendor has experience in the healthcare vertical, can greatly improve the speed and accuracy of this process.

Define Policy

Once the data is discovered and classified, the organization must determine its policies for handling and protecting the data. Protection has to be applied around three key areas: data, people, and infrastructure.

- **Data** — The data itself needs to be protected. This means that the data should be confidential, have integrity, and be accessible only to the people who have the access and authorization to view and change the data.
- **People** — Mistakes will be made. Laptops and CDs will be stolen and lost. Passwords will be compromised.
- **Infrastructure** — The data needs to be protected in transit.

For each of these key areas, the healthcare organization should define not only the policy for accessing the data, but the appropriate response to unauthorized access or transmission of data.

Enforce Controls

After policy has been defined and executive management has approved, then the organization will establish a control framework based on policy, risk, and location of the data. The organization will then implement appropriate controls (e.g., encryption and key management controls, access controls, reporting and audit controls, etc.) to ensure that the policies (data and access control) are enforced. In order to be effective, these controls must have both a technology and human resource aspect. This means that the technology must be in place to prevent access and change to data by unauthorized personnel, and that disciplinary action is also available within the organization to implement against offenders.

There are technology solutions to address each of the three policy areas defined above. Solutions designed to enforce policy include: data loss protection, encryption, key management, and one-time password tokens. The combination of well-defined policies, technology solutions, and consequences for non-compliance can allow the healthcare organization to realize the benefits of strategic initiatives knowing that the risk has been addressed.

Report and Audit

Finally, no security strategy would be complete without a reporting and auditing component in place. A healthcare organization is in a constant state of flux — doctors, patients, staff, and technology change all the time. The only way to ensure that policy is being enforced and that new risks are not being overlooked is to have a consistent reporting and auditing platform.

Manual reporting and auditing is unrealistic for most healthcare organizations given the size and complexity involved. The best technology solution to address reporting and auditing is a Security Information and Event Management (SIEM) solution. SIEM solutions monitor events as they transpire on the entire network, correlating events from all devices on the network. SIEM solutions are constantly on the lookout for breaches in policy and can provide early warning when a breach of policy occurs.

CONCLUSIONS

e-Health initiatives are beginning to drive healthcare organizations to implement new and sophisticated information systems to enable improved patient care, lower costs, and accelerate revenues. However, as these systems are implemented and patient data moves from locked offices and filing cabinets to an electronic format, crucial security issues arise

that must be addressed by the healthcare industry. Data breaches and lost patient data enable criminals to sell private information to newspapers, use a patient's credit cards, assume a patient's medical identity, and potentially endanger a patient's life as multiple people seek treatment under the same health record.

With patient health and personal information at risk, Frost & Sullivan believes it makes sense to consult with security experts such as RSA in order to better map out potential threats and devise strategies to close them. Important next steps to improve the security of personalized health data in hospitals include reviewing the current security scenario, talking to industry experts, and prioritizing areas where data security could be compromised. Every healthcare organization should consider their own internal IT capabilities and match them with external risk management expertise as they choose to implement any e-Health platform. These scenarios need to be studied in detail and need to align with the best practices that Frost & Sullivan have identified:

- Discover and Classify
- Define Policy
- Enforce Controls
- Report and Audit

The e-Health initiative is well on its way and currently there is a need for better security controls that limit the ability for this data to fall into the wrong hands. Hospitals and healthcare groups need to plan ahead and consult with the right security experts to ensure the safest and best path toward attaining efficient e-Health systems.

CONTACT US

Palo Alto

New York

San Antonio

Toronto

Buenos Aires

Sao Paulo

London

Oxford

Frankfurt

Paris

Israel

Beijing

Chennai

Kuala Lumpur

Mumbai

Shanghai

Singapore

Sydney

Tokyo

Silicon Valley
2400 Geng Road, Suite 201
Palo Alto, CA 94303
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SW1W 0DH, UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost
myfrost@frost.com
<http://www.frost.com>

ABOUT FROST & SULLIVAN

Based in Palo Alto, California, Frost & Sullivan is a global leader in strategic growth consulting. This white paper is part of Frost & Sullivan's ongoing strategic research into the Information Technology industries. Frost & Sullivan regularly publishes strategic analyses of the major markets for products that encompass storage, management, and security of data. Frost & Sullivan also provides custom growth consulting to a variety of national and international companies.

The information presented in this publication is based on research and interviews conducted solely by Frost & Sullivan and therefore is subject to fluctuation. Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or end users.

This publication may not be downloaded, displayed, printed, or reproduced other than for non-commercial individual reference or private use within your organization, and thereafter it may not be recopied, reproduced or otherwise redistributed. All copyright and other proprietary notices must be retained. No license to publish, communicate, modify, commercialize or alter this document is granted. For reproduction or use of this publication beyond this limited license, permission must be sought from the publisher.

For information regarding permission, write:

Frost & Sullivan
2400 Geng Rd., Suite 201
Palo Alto, CA 94303-3331, USA