WHITE PAPER

proofpoint™

TOP 8 HEALTHCARE ARCHIVING AND E-DISCOVERY REQUIREMENTS

TABLE OF CONTENTS

OVERVIEW

Managing the growth of data in healthcare organizations is a major challenge that is driven by the growth of electronic data and an increase in litigation, driving costs and risk as organizations seek to control costs. IDC estimates that data will grow by 50x through 2020 and that unstructured data, including email and files, will account for 90% of this data.[1] Adding to this challenge is that 70% of an organization's data are duplicates and haven't been accessed over 90 days according to Gartner. Organizations face these challenges in an environment of increasing litigation and investigations that drive data risk and cost. In a survey of healthcare organizations by Fulbright & Jaworski, 100% of healthcare organizations indicated they predict litigation to continue at the same or increasing rates, while 96% of the same firms predicted the same for government and regulatory investigations.[2]

The increases in litigation and investigations place a premium on defensible e-discovery based on high performance, reliable, and repeatable search to perform time-sensitive response. These same requirements are required for other areas, including internal audits and HR investigations.

Leading healthcare organizations have responded to these challenges by moving from reactive litigation and investigative response to proactive reduction of data at risk through retention management and information governance, while expanding the data managed by the archive to cover SharePoint and file servers.

RECENT HEALTHCARE LITIGATION TRENDS[2]

100% of healthcare organizations predicted litigation would remain the same or increase

96% of healthcare organizations predicted government and regulatory investigation volume would increase

24% of healthcare organizations spend more than $10 million on litigation annually

64% of healthcare organizations had a dispute or investigation involving privacy and/or data protection issues

TOP 8 HEALTHCARE REQUIREMENTS

As the most secure cloud-based archive, Proofpoint Enterprise Archive provides the ideal e-discovery and search platform for healthcare organizations. With some of the largest healthcare organizations in the world as clients, Proofpoint understands the specific requirements for healthcare and can address the needs of managing larger volumes of data and varied sources of information.

This paper outlines the top requirements we've heard from our customers, and we present them here as a resource that healthcare organizations should consider when planning for their archiving and e-discovery solutions.

1. Effective and Defensible E-discovery

Healthcare is a highly litigious industry, and with organizations anticipating increasing or similar levels of litigation, it has become increasingly important to manage the risks and costs in a defensible manner. Proofpoint customers have indicated that reliable and defensible e-discovery is one of the most important archiving requirements, especially when coming from slow, unreliable systems that may deliver inconsistent results and may require over a week to deliver data.

Search Consistency

There are two major approaches to conducting preservation holds: identifying information by custodian and identifying information by query. In both cases, identification of the data is often conducted by performing a search.

Proofpoint customers have reported that some solutions have delivered inconsistent searches and may not identify all email that needs to be placed on hold, increasing the risk of spoliation.

In *3M Innovative Props. Co. v. Tomar Elecs.* (D. Minn Sept 18, 2006) the court imposed both sanctions and an adverse inference instruction after finding the defendant failed to conduct a reasonable search for responsive documents and implement a legal hold.

This is especially relevant for e-discovery as opposing counsel will often attack the e-discovery process. By moving to a system that has a robust and consistent search that produces identical results for the same queries, healthcare organizations can reduce their risk of under-preservation and the impression that their preservation system is not reliable.

"Most custodians cannot be 'trusted' to run effective searches because designing legally sufficient searches in the discovery or FOIA contexts is not part of their daily responsibilities."

U.S. District Judge Shira Scheindlin

Search Speed

Healthcare customers have also reported that searches become slow in their existing solutions as data volumes grow. One reason searches become slow is that many systems are not designed for large volume search, a complex task.

Similar to database systems which are split into OLTP systems for production use and data warehouses for archived data, the techniques used to search a production email server with recent data are much different than searching terabytes of historical data.

Additionally, some archives use simple search index partitioning techniques that reduce the technical complexity of scaling but also result in slow search response times that can take hours or days.

2. Elimination of PST Files and Backup Tape Restoration for E-discovery

In addition to slow and unreliable operations of messaging systems for e-discovery, healthcare organizations are also faced with the burdens of identification and collection of personal storage table (PST) files across their network and restoration of backup tapes for e-discovery. When email must be identified and collected from PST files across the network or in backup tape libraries, identification and collection can be costly, with organizations reporting collection and processing costs of $4,125 per GB.[3]

PST File Elimination

PST files are problematic for e-discovery because they contain email that is often the subject of holds but they are not easy to identify, collect, and preserve as they tend to exist locally on individual desktop and laptop computers. This is compounded by the fact that the approach of requiring custodians to identify and preserve email has come under fire due to recent scholarship and case law showing that custodians may not have the capability to perform this task. In *National Day Laborer Org. Network v. U.S. Immigration and Customs Enforcement, et. al.* (S.D.N.Y July 13, 2012), U.S. District Judge Shira A. Scheindlin wrote:

> "most custodians cannot be 'trusted' to run effective searches because designing legally sufficient searches in the discovery or FOIA contexts is not part of their daily responsibilities."

In addition to e-discovery challenges, PST files also provide challenges for backup, storage, and retention management.

Elimination of PST files by using an email archive as a solution for PST file proliferation is recognized by Gartner as a best practice.[4]

Backup Tape Elimination for E-discovery

Accessing backup tapes for e-discovery is problematic due to the time it takes to load and process tapes and the fact the information may be spread across many tapes. Indexing technology now exists to reduce the number of tapes processed, but this is still expensive. In Moore v. Gilead Sciences (N.D. Ca Nov. 16, 2011) the defendant estimated indexing of tapes would cost $360,000 for a single custodian. Archives are a faster and less expensive way to access the same data for e-discovery.

3. Defensible Disposition via Information Governance

As the amount of information grows, so does the amount of information that is outdated and no longer accessed, increasing the risk and burden of the legal and IT departments to respond to external and internal data requests. Magistrate Judge Andrew Peck says that information governance to defensibly dispose of data will become the top e-discovery trend.[5]

Volume of ROT (Redundant, Obsolete or Trivial) Data

The reason information governance is getting more attention is that organizations have realized that up to 70% of their data may be ROT (redundant, obsolete or trivial) and that up to 99% of data on backup takes may be useless.[5] While traditional collection and processing costs are substantial at $4,125 per GB, review costs are even higher at $22,480 per GB.[3] When 70% of data being reviewed for e-discovery can be defensibly disposed of beforehand, the cost and operations savings can be substantial.

Defensible Disposition Within Organizations

In a recent survey of 430 information governance professionals, 96.1% indicated they believe defensible disposition is necessary to manage growing amounts of information, with 65.8% of respondents having some form of defensible disposition program under way.[6]

HEALTHCARE CLOUD USAGE[8,9]

88% of healthcare organizations that use the cloud reported average cost savings of 20% per year.

29% of healthcare IT budget is predicted for cloud services in four years.

51% of healthcare organizations listed security as a concern for moving to the cloud.

36% of healthcare organizations listed performance as a concern when considering the cloud.

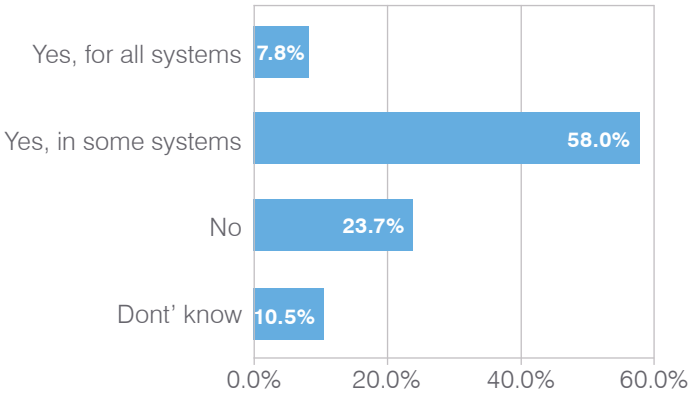

Figure 1. Defensible Disposition In Practice[4]

4. Power and Control in the Cloud

Many healthcare organizations face tightening budget constraints and prefer to deploy a greater proportion of their IT resources for patient-care applications. As an alternative to spending more resources and person-hours maintaining an on-premise archive, organizations are turning to the cloud for a high-performance solution that provides predictable costs while reducing operational and staffing costs. In a recent survey, 89% of healthcare organizations were considering moving to the cloud.

Benefits of The Cloud for Healthcare

Healthcare organizations have indicated benefits in four areas.

	Benefit
Cost	88% of healthcare organizations that reported utilizing cloud computing have reduced costs by an average of 20% per year.
Capital	Over 50% of healthcare organizations that have implemented cloud reported reduced initial capital outlays, indicating lower risk.
Accessibility	49% of healthcare organizations reported "anywhere access" via web and mobile devices was a benefit.
IT Requirements	About 50% of healthcare organizations realized significant savings from consolidating IT infrastructure and reducing IT energy and power requirements.

Figure 2. Cloud Benefits for Healthcare[8]

Control and Security are the Top Cloud Concern

Healthcare organizations have indicated that security, performance, and integration are the greatest concerns with moving to the cloud.[8]

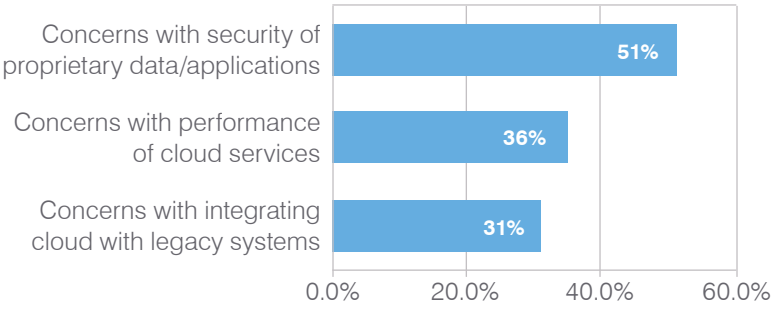

Figure 3. Top Healthcare Concerns for Using the Cloud[9]

5. Funding Strategic IT Initiatives with E-discovery Cost Savings

Healthcare organizations must often face increasing IT requirements in the context of flat or declining IT budgets. At the same time there are increasing requirements to implement patient care systems such as electronic medical records (EMRs).

Some strategic IT initiatives such as EMRs can cost tens to hundreds of millions of dollars to implement and, in this context, it becomes even more important to find cost savings in terms of both hard dollar savings and soft operational benefits that can free up staff from working on non-strategic tasks.

Archiving provides a number of significant hard and soft benefits that can be used to fund strategic IT initiatives including the following that can reach hundreds of thousands to millions of dollars in savings.

Hard Cost Savings	Soft Cost Savings
Reduced Legal Fees • Collection Reduction for PSTs • Collection Reduction for Servers • Collection Reduction for Desktops and Laptops • Backup Tape Restoration • Email Retention and Information Governance **Reduced Storage Costs** • Storage Reduction for Archiving • Storage Reduction for Stubbing • Storage Reduction via Retention **Reduced Operations Costs** • Reduced Backup Times and Media Costs • Lower Risk Insurance Costs • Energy Cost Savings	**Search Benefits** • End User Productivity Gains • Early Case Assessment • Investigative Search • Defensible Disposition **IT Benefits** • Stability • Data Loss • Mailbox Quota Elimination • Mailbox Recovery Efficiency • Email Systems Upgrades • Archive Systems Upgrades **Risk Reduction Benefits** • Defensible Legal Holds • Administrative Legal Hodls • Active Legal Holds • Regulatory Compliance • Fraud Reduction

HEALTHCARE MOBILE USAGE

93% of healthcare organizations said mobile apps were very important and a must-have, or made a significant contribution.[13]

62.7% of healthcare organizations using mobile and wireless devices have said they have seen an increase in productivity.[13]

67% of healthcare organizations have reported increased employee satisfaction by enabling mobile and wireless solutions.[13]

Over 33% of healthcare organizations have seen improvements in patient outcomes that they can attribute directly to wireless initiatives.[13]

Figure 4. ROI Benefits from Cloud Archiving and e-Discovery[10]

6. End-User Search and Access: Mobile and Web

At the same time healthcare organizations must handle the increasing burden for e-discovery and the deployment of EMR systems, doctors and staff becoming more mobile with the introduction of smart phones and adding the requirement to access more data from a variety of devices.

With traditional systems, providing timely email response itself could be a challenge as greater e-discovery and regulatory burdens place increasing load on the systems, thereby reducing the ability to access data for end-users.

Mobile Adoption in Healthcare

Mobile adoption in healthcare is significant with 89% of physicians and 84% of non-physician clinicians using wireless data applications according to the HIMSS Mobile Survey.[10] Of these users, 88% were able to access data from an approved on-site network while 77% were allowed to access data from approved public network.[9] Aligning with the adoption of the cloud, 56% of healthcare IT directors, administrators, and managers indicated that mobile access to apps is driving a faster move to the cloud.[12]

Improved Productivity, Satisfaction, and Results with Mobile Access

The adoption of mobile and wireless technologies within healthcare is having a dramatic impact according to healthcare practitioners, with improvements in employee productivity (63%), employee satisfaction (67%) and patient outcomes (33+%).[13]

Figure 5. Healthcare Productivity Inpace of Wireless[11]

Given these adoption rates and outcomes, enabling mobile access to email data via native applications for iOS, Android, and Blackberry should be considered.

7. Compliance with Regulatory Retention Requirements

Healthcare organizations operate under a number of regulations and rules that have regulatory retention requirements including HIPAA, Medicare, Sarbanes Oxley, and others, each with varying retention, deletion, and access requirements.

HIPAA Retention Requirements for Health Records

There are often questions about whether HIPAA mandates retention of email. HIPAA has retention rules for HIPAA policies, PHI disclosures, and health records (which come in many file types) but no specific retention rules for email as a file type. Generally organizations have taken three approaches to retaining email with respect to health records to meet HIPAA compliance.

Retention Policy	Description
Email with PHI is part of patient's health record	Some organizations classify email containing PHI as part of the patient's electronic health record (EHR) in which case it needs to be retained for the same period of time stipulated for all of the patient's health record. These regulations are often stipulated by state and type of provider.
Email with PHI is not a record but under a general email retention policy	Some organizations do not consider email, whether it has PHI or not, to be part of a patient's electronic health record but retain email for a certain period of time before deletion using a general email retention policy.
Email with PHI are not records and there is no general email retention policy	Some organizations do not consider email in any form to be part of a patient's electronic health record and also have no retention policies set for email in general.

Figure 6. Email Retention Practices for HIPAA

HIPAA Retention Requirements for PHI Disclosures

For PHI disclosures, HIPAA stipulates organizations must retain PHI disclosure information for six years prior to an individual's request. This data may be retained using a variety of means that ensure the data is retained and accessible.

8. Single Vendor Solution

Healthcare organizations must deal with information in many formats and meet many requirements, including, but not limited to, archiving, e-discovery, information governance, retention management, defensible disposition, and regulatory compliance. In addition to managing this information, healthcare IT organizations require DLP to prevent unauthorized PHI disclosures and email protection solutions to protect themselves from outside threats such as spam, viruses and a new generation targeted attacks.

Selecting a single vendor is important to many healthcare organizations, but it becomes even more important to evaluate the vendor when doing so. Some requirements organizations have found valuable are described below.

Retention Policy	Description
Working Product with Realistic Validation	At a minimum, the product must work as advertised. While some products work well in demo and proof of concept situations, the reality of operating under real workloads is quite a bit different. An easy way to evaluate vendors is by examining their guarantees. For example, with a cloud deployment, does the vendor have uptime and search response time guarantees? In addition to the guarantees, it is important to evaluate whether the guarantees are realistic. For example, some organizations boast unrealistic 100% uptime guarantees that they have understandably failed, raising the question of how seriously the vendor intended to stand behind their guarantee in the first place.
Innovation	Requirements change and evolve so the vendor must have the breadth and depth to innovate in critical areas of importance to address key market needs such as by allowing customers to maintain control of their data in the cloud, by addressing a changing environment such as enabling defensible disposition of information and by preventing targeted attacks.
Customer Satisfaction	Finally, a high customer satisfaction rate is important for customers. Due to the growing amount of data under management, many customers will stay with vendors even if the service provided is not meeting their expectations. It is important to ensure that the vendor is providing services to both generate renewals and customer satisfaction.

Figure 7. Single Vendor Requirements

ABOUT PROOFPOINT ENTERPRISE ARCHIVE

Proofpoint Enterprise Archive is the leading cloud archiving and e-discovery solution with a unique set of patented technology backed by unique, industry-leading SLAs and covering a wide set of data required by healthcare organizations. Healthcare organizations of all sizes have recognized this and turned to Proofpoint for industry leading capabilities and performance. Proofpoint's core capabilities include:

- **Leading Technology:** Proofpoint's cloud archive is protected using Proofpoint's patented DoubleBlind™ Key Architecture, ensuring the customer, not the cloud provider, stays in control of the data when it's placed in the cloud.
- **Leading Guarantees:** Backed by the industry's only search performance guarantee, organizations can have the confidence that their data is protected, and they can respond to legal requirements confidently and defensibly.
- **Leading Data Coverage:**
  - Microsoft Exchange on-premises
  - Microsoft Office 365
  - Personal Storage Tables (PST) files
  - Microsoft SharePoint
  - Windows, Linux, and Unix file servers
  - Social Media including Facebook, LinkedIn, Twitter
  - Instant messaging systems
  - Bloomberg

Proofpoint continues to innovate both technology and business processes to provide the best services. Contact us today to learn how we can help solve your information security and governance challenges.

[1] IDC. *The Digital Universe*. 2011
[2] Fullbright & Jaworski, *9th Annual Litigation Trends Survey Report*. 2013.
[3] RAND Institute for Civil Justice. *Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery*, 2012.
[4] Gartner Inc. *Best Practices for Using Email Archiving to Eliminate PST and Mailbox Quota Headaches*. Sept. 21, 2012.
[5] LXBN TV. Information Governance Will Replace Predictive Coding as Top Trend in E-discovery – Andrew Peck, January 30, 2013.
[6] Index Engines. *Defensible Deletion & Tape Remediation*. February 25, 2013.
[7] eDJ Group. *"Defensible Deletion" Series Topic Overview.* 2012.
[8] CDW. *The CDW 2011 Cloud Computing Tracking Poll*. 2011.
[9] CDW. *CDW's 2013 State of the Cloud Report*. 2013.
[10] Proofpoint, Inc. *ROI Benefits of Archiving and e-discovery*. 2013.
[11] HIMSS. *HIMSS Mobile Survey.* December 2011.
[12] CDW. *CDW's 2013 State of The Cloud Report.* 2013.
[13] NetMotion Wireless. *2011 Survey: Wireless Trends in Healthcare*. 2012.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.