Access and General Information Governance requirements of HIPAA and ARRA with an integrated platform solution.

With the proliferation of structured, unstructured and big data records, Healthcare organizations are struggling to balance IT and business priorities when it comes to retaining both patient and internal information records in compliance with HIPAA and HITECH. Get it wrong and data growth leads to crippling IT inefficiencies, skyrocketing costs and failures in compliance and record keeping.

Modern and adaptable strategies to the retention lifecycle of information that frees Healthcare providers from the complexities of retaining and accessing data for the long term, while radically lowering business risk are discussed in this white paper.
CONTENTS

Executive Summary ......................................................................................... 3
Risk in Healthcare Retention .......................................................................... 3
Traditional Approaches Create Cost Silos .................................................... 4
Journey to the Land of Strategic Information Retention ............................... 7
Building the Enterprise-wide Data Retention Platform ............................... 8
Simpana® Unified Platform Benefits ............................................................. 8
Since the American Recovery and Reinvestment Act (ARRA) in 2009, which brought about new Health Information Technology for Economic and Clinical Health (HITECH) privacy and security rules that apply to the HIPAA law, there has been a growing need for convergence in three specific areas of information management: economic and efficient data retention, legal search and discovery and organized long-term record keeping for HIPAA compliance. As a result, organizations are finally trying to implement an Information Lifecycle Management (ILM) or information governance strategy that directly addresses these areas. The solutions, unfortunately, typically are hindered by a lack of IT budget, violations in relation to poor HIPAA compliance controls, individual and legal access requirements to Protected Health Information (PHI) and developing industry and governmental standards for unstructured medical data record-keeping. The evolving nature of data retention for all forms of electronic information governed by HIPAA encourages an integrated approach from backup to archive that delivers true data life cycle management. In short, organizations are facing a “new dawn” in terms of the way traditional data retention is thought about in both on-premises and to-the-cloud applications, particularly in the current economic climate.

As information creators, owners and users, everyone is programmed to retain information. We rely on the applications and devices that we used to create the data to also store and retain it. When we are forced to delete data or given constraints on what we can save, human nature finds a way to hide it away in all manner of places. The result: records retention chaos with explosions in IT storage and data protection costs, increased risk from legal and regulatory failures as well as a lack of any formal and structured policies for record keeping across the enterprise.

**Risk in Healthcare Retention**

Not many of us can say we file what we receive, sift through and organize what we want to keep and then discard what we don’t. The reason is simple: Fear! Fear that we might inadvertently delete something we shouldn’t; fear that we or the organizations we work for might need something in the future that we cannot fully appreciate now; fear that when we apply rigor to the way we organize and have kept information that it will always be incomplete and inaccurate due to human error.

When we relate these challenges specifically to the Health Insurance Portability and Accountability Act (HIPAA), fear or the risk in healthcare records retention can reach new levels of anxiety. HIPAA itself, or more specifically 45 CFR Parts 160, 162, and 164, is focused on rules related to patient privacy, patient records security, electronic healthcare transactions, the identification of Protected Health Information (PHI) as well as what compliance means and how it is enforced. In relation to enforcement, the American Recovery and Reinvestment Act (ARRA) of 2009 brought new rigor to HIPAA in reference to PHI standards as well as the Health Information Technology for Economic and Clinical Health (HITECH) Act for expanded security and privacy.
In addition, and perhaps more importantly, there are increases in civil and criminal sanctions for non-compliance. The risks of million-dollar penalties and public embarrassment for data breaches and violations in PHI have never been more acute. As a result, it is imperative that effective control measures be implemented by organizations using solutions either on premises or in cloud/software as a service health solution provider.

**Traditional Approaches Create Cost Silos**

The reality for most healthcare providers is somewhat different. The lack of control and organization of records is a distinctive and individual human trait, which when compounded with the limited purging of information, causes data sprawl with the creation of many hundreds of separate silos of hoarded and duplicated information spread across the organization. The implication of this reality is quite dramatic as follows:

- The over-management of data resulting in unnecessary IT spend to manage duplicated content;
- Huge infrastructure considerations for storing types of “big data” medical records;
- Severely challenged healthcare record keeping for the organization of protected health information (PHI);
- The near-impossible access and discovery of information for legal discovery, compliance audits and responses to individual privacy access requests and internal exposure events;
- Constant enforcement through violation and penalties for mismanaged PHI.

The IT cost of data retention is particularly impressive when you consider the number of copies of information created. The content types we create typically cycle through active applications and systems based on working data copies.
The trouble is the working copies indirectly result in many other passive clones, including backup and protected recovery copies, archived copies for scalability and regulated data copies for compliance retention. (Figure 1 above). The question then remains, particularly in reference to PHI, as to how data is actually secured, identified and retained as well as ultimately deleted in compliance with HIPAA and ARRA.

This is, of course, what we’ve always done. Organizations have traditionally bought best-of-breed solutions aligned to specific information types rather than thinking about the growth and retention problem holistically. Therefore, it’s no wonder that in response to global data growth patterns of 110% CAGR* or more, the default decision is “just add more storage,” which results in an exacerbation of already restricted IT spend. Big data, including medical image records, is the main contributor to this growth with a 55% CAGR*. Yet organizations still put stale or inactive data on expensive disk utilizing more than 47Pb* globally, and a contribution of more than 60%* of the overall storage growth compared to tape (45%*) and cloud (35%*). The inappropriate use of IT infrastructure and storage for managing relatively passive data is at the very heart of the economic retention challenge.

Envision a traditional data archive and typically you think of tactical reasons why data needs to be moved to ease pressure on stretched applications or to reduce the cost of data on file systems. While these are valid reasons, they typically are implemented with little thought for relevance, organization or future discovery. There is also the question of the meta data associated with the systems that create the content to be retained (e.g., the labeling of medical images). Where is that retained?

HIPAA 45 CFR rule 162.1000 encourages the encoding of records against specific schemas, including ICD-9 and ICD-10 as well as HCPCS. This meta data also needs to be retained with archive records to facilitate more accurate discovery in the future. Patient rights within 45 CFR 164.522 and 164.524 often require the identification and disclosure of PHI based on patient identifiers. Can archive solutions either capture this data or classify records once retained in a way that facilitates this consistent future discovery? Additionally, no one has a crystal ball to see how and which records need to be organized or classified in the future. This is why retention solutions need agility. Because storage or application pressures usually dictate immediate action, IT departments can rarely wait for healthcare providers to define their PHI retention strategy. Without direction, agile solutions or consolidate approaches, IT will move the data to ease pressure on production systems and often it goes into ill-conceived, soiled archives. Backup and data protection of these silos then adds to the problem as IT applies the same policies to archive protection as is done to backup of production data. The result? Lots and lots and lots of copies of the same data. Doesn’t this sound like the inspiration for the phrase “the blind leading the blind”?

*Enterprise Strategy Group Digital Archive Market Forecast 2010-2015

What we need is a revolution in strategic approaches to data retention that truly converges the way in which IT manages digital records and that aligns directly to the needs of healthcare operations.
When creating adaptable strategies for records retention we need to incorporate principles into our approach that address both the needs of the individual as well as the organization and enterprise. The definition of Information Lifecycle Management (ILM) as defined in the early 2000s by various IT and storage vendors offers a good initial perspective on how technology needs to manage retention by drawing out six core principles below (Figure 2).

1. **Conception**
   - Origin, Type e.g. Email, File, Document
2. **Proliferation**
   - Internal, External, Sent, Received
3. **Exploitation**
   - Accessibility, Filing, Search & Discovery
4. **Revision**
   - Version control, Audit
5. **Retention**
   - Protection, Location, Security
6. **Disposition**
   - Deletion, Purge

Of all these concepts, specifically in relation to HIPAA, the security rules of 45 CFR 164.306 often present the biggest challenge. Specifically, how to authenticate, encrypt and store records through their period of retention as well as safeguarding administrative and individual rights. Do you think that encryption and security officers naturally understand the complexity of managing encryption keys that change randomly per application and user? Multiple this by seven years or 84 months in an organization with four core medical applications and 1,000 patients and your security consideration will encompass in excess of 300,000 separate encryption keys that need to be mapped to patients and records. Still sleeping at night?

When considering the longer-term retention of information, you naturally start to think about its life cycle, and in turn how to manage data through change whether it's a three-, five-, seven-, 10-, 15-year or indefinite period of retention. It’s is only when you start thinking about the strategic life cycle of information requirements that you can begin to solidify a strategy around the need to intelligently move, deduplicate and apply retention to passive data typically at a granular level. While planning this, don’t forget to consider HIPAA compliance directives that can be applied both today and when future requirements dictate a degree of agility and change.
Journey to the Land of Strategic Information Retention

A great way of assessing where you are and what you need to do is to grade yourself on the motivation, approach and capabilities currently in place to retain information. Figure 3 highlights the different stages of archiving depending on how an organization views drivers around IT storage pressures, records compliance and governance as well as the expectations on information access and discovery.

Next, consider where important “digital” assets live. How are they managed and ultimately how you can converge the way you keep them? This requires a paradigm shift in thinking. For example, the true cost of passive data archiving is not in the way data is retained in an archive but how it is also protected. One terabyte (1TB) of archive data can easily lead to 10TBs or more of protected archive—and the data hasn’t even changed. Active data in live applications and systems is also protected and already being copied for different scenarios. Neither is delivering a consolidated life cycle approach to retention.

The answer: touch data once, store it once and manage it once

So what’s the answer to this dilemma? Bring on a single, intelligent platform. A solution that unifies the way data is processed for backup and archive into a truly modern and single-touch approach for converged and agile data life cycle management. This platform incorporates deduplication throughout the life cycle with automated rules that drive organization, retention and disposition through a virtualized approach to retaining, authenticating and encrypting records regardless of source or storage. Unification through this progressive and intelligent approach is the elixir to unlimited enterprise-wide search that can provide seamless access to information for multiple roles in an organization while easing the legal burden of discovery and preservation. What’s more, all this capability is delivered bottom-up to an organization rather than top down.
Building the Enterprise-Wide Data Retention Platform

CommVault® Simpana® software is such a unified platform that delivers on the message of “oneness.” Simpana software provides one place to keep data without duplication across the enterprise, from protection to destruction. The benefits of such an approach can transform any organization. From the top, CIOs can reduce long-term costs and risks associated with retaining information and in turn provide improved business access. IT managers can directly reduce IT spend throughout the life cycle of data management with improved operational efficiency and flexibility in storage management today and in the future. Healthcare operations can get their systems working efficiently with reduced licensing and capped growth whether virtually or physically managed. Patients also benefit from improved privacy access to individual PHI across the provider, as well as better employee collaboration and sharing of passive content across the enterprise. Corporate legal teams can finally, through a single mouse click, preserve legal content to reduce litigation risks and costs as well as gain insight into evidence early in the discovery process. HIPAA records/compliance teams can conform more easily and holistically to industry regulation with improved records organization, synchronized retention and disposition with ease of supervision, monitoring and auditing.

Simpana® Software Unified Platform Benefits

Simpana software solves information governance and retention life cycle management across all types of capture data. With Simpana software’s unified approach, data is cost-efficiently managed across data protection, data reduction, records retention and search strategies while maintaining high-speed performance in the face of increasing data volumes.

Through its single platform, Simpana® software can intelligently manage data and information across heterogeneous applications, virtual servers, operating systems and infrastructure from a single console. It revolutionizes the problem of both retaining and protecting all types of enterprise information – from the data center to the edge and to the cloud - with a single platform.
Simpana software is designed to efficiently capture, move, retain, find and recover data from any storage tier, including disk, tape and cloud. Simpana software provides:

- Policy-based life cycle management enables data records to be retained across tiers of storage, tape and cloud environments. Storage savings improve server performance, lower capacity management overhead and can reduce or eliminate the need to buy more disk as data ages.

- Fast, scalable, object-based virtual content store preserves end-user and application views of data records while managing the original objects in the data management platform.

- Simpana OnePass backup and archive provides content preserved views of data while taking advantage of storage management features with no additional movement over normal backup to minimize server, network and production systems impact.

- Robust and common content archive interface that integrates a wide range of heterogeneous data sources using both HTTP and REST based protocols. This provides the flexibility to integrate with third-party healthcare applications for declaration based retention and storage management.

- Embedded and media independent, FIPS-1,-2 certified encryption for the secure long term management of data records from capture to rest, using a choice of 5 different ciphers from 128bit to 256bit.

- Powerful architecture provides flexible options to address the diverse, “big data” scalability requirements of vertical markets including PACS and patient records in healthcare, together with other large data types including digital video and audio as well as high-volume transactions and images.

- Full Content Indexing (CI) option enables all data to be searched and retrieved in context. All copies of indexed data (protection, migration and archive data) are combined into a single, searchable archive. Result sets can be viewed and refined before the retrieval process for maximum efficiency. Data can be automatically classified, tagged and retained based on the needs of your business.

- Modern Data Protection provides seamless integration with backup and recovery operations. A single pool of data with a common interface to centrally set and manage policies and schedules simplifies data management operations. Policy and job management is consolidated while reporting and alerting is improved for administrative.

To learn how to simplify the growing complexities of healthcare data management with CommVault Simpana software, please visit commvault.com/healthcare.

For more information on Simpana Information Governance solutions please see commvault.com/compliance.
Resources