

HIPAA COMPLIANCE AND DOCUMENT MANAGEMENT

*How to create an agile, efficient
healthcare organization prepared
to execute operational changes
and absorb the financial impact
of HIPAA compliance*

By Ken Hansen

Channel Marketing Manager, CDIA+

Ricoh Americas Corporation

Table of Contents

1.0	Executive Summary
2.0	Why Does Document Management Matter?
3.0	The Impact of HIPAA on Document Management
4.0	Building an Agile Organization
5.0	Critical Success Factors
6.0	Conclusion

Executive Summary

The federal government enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to assure health insurance portability, reduce healthcare fraud and abuse, guarantee security and privacy of health information and enforce standards for health information. It covers all healthcare providers, payers and clearinghouses.

Document management will be only one component of any healthcare organization's overall HIPAA strategy. But it will be a critical one, especially as HIPAA becomes more prominent in the public consciousness, as well as the national media. Improving document management shows concerned consumers that your organization is working hard to protect their confidential health information and maximize the efficiency of healthcare transactions. Plus, streamlined document management can have a powerful ripple effect in any healthcare organization.

Administrative Simplification (Title II of HIPAA, Subtitle F) affects the patient records healthcare organizations print, copy, fax and email every day. It will require you to produce and/or manage large volumes of new documents — such as training manuals and patient education materials — on an ongoing basis. HIPAA will also require healthcare organizations to document their HIPAA strategy, implementation plan and outcomes.

Because organizational processes, policy assessment and procedure redesign represent the vast majority of compliance work, it will be far more important for healthcare organizations to establish a productive, efficient organization that shares information easily, enables smooth collaboration among workgroups and across departments, and interacts with business partners seamlessly than it will be to purchase new technology. This level of efficiency is impossible to achieve without a solid document management infrastructure.

Healthcare organizations need to address five critical factors to create a reliable, flexible document management infrastructure:

1. Choose the right partner.
2. Insist on exceptional documents.
3. Leverage digital technology.
4. Establish a reliable document management network.
5. Consolidate vendor relationships.

To find the best document management partner — one that will enable you to achieve these five critical success factors — you will need to initiate the search process now.

Why Does Document Management Matter?

It is crucial to start with the understanding that technologies and system architecture are only elements of HIPAA compliance. For purposes of HIPAA compliance, technological solutions will be necessary but not sufficient. Administrative, legal, and policy-level controls must be included too. The legal judgment of HIPAA compliance will be made at the level of the organization, not the level of any given policy, procedure, hardware, or software. ... The question for any vendor or consultant ... is not: "Is your solution compliant?" The real question is: "How would this proposal fit our own overall compliance strategy?"

— *"Thinking About HIPAA Compliance: The Role of Strategic Planning,"*
by John R. Christiansen, IT Health Care Strategist

Regular checkups. Hospital admissions. Emergency room visits. Prescription pickups. Insurance claims. Every day, patients interact with healthcare organizations to seek treatment, receive care and coordinate payment for service. All of these interactions depend on a smooth, uninterrupted flow of confidential healthcare information.

Until the digital age, the integrity of this information — and the efficiency with which it is exchanged — were not critical issues. Paper copies were locked up and access was severely limited. Today, information transfer is much more fluid. Providers, payers and clearinghouses exchange huge volumes of electronic documents, often via fax and email. Access to these documents is much less controlled. Confidentiality can be highly suspect. Backlogs are frequent and can have a detrimental effect on the quality of patient care.

As part of a broader healthcare reform strategy, the federal government enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA is a complex, multi-part act designed to achieve many different and often unrelated goals: assure health insurance portability, reduce healthcare fraud and abuse, guarantee security and privacy of health information and enforce standards for health information.

Today, many healthcare organizations are concerned with Title II of HIPAA, or "Preventing Healthcare Fraud and Abuse," which includes a section called "Administrative Simplification" (Subtitle F). Administrative Simplification calls for sweeping changes in four areas: the standardization of electronic health transactions; unique identifiers for providers, employers, health plans and patients; security of health information and electronic signature standards; and privacy and confidentiality.

This white paper examines the relationship between HIPAA and document management. We will look at the general impacts of Administrative Simplification on document management, specific concerns related to the final Privacy Rule and the proposed Security Standards, as well as the broader effects of ongoing HIPAA compliance in healthcare organizations. We will address how document management processes — such as the exchange of private patient records — will be affected by HIPAA. We will analyze secondary document-related impacts of HIPAA, such as a growing need to produce employee training materials. We will also show how healthcare organizations that streamline all document processes — not just those related to HIPAA — will be better prepared to make HIPAA-related changes quickly and more cost-effectively.

Document management will be only one component of any healthcare organization's overall HIPAA strategy. But it will be a critical one, especially as HIPAA becomes more prominent in the public consciousness, as well as the national media, for three reasons.

First, of the five HIPAA titles, Preventing Healthcare Fraud and Abuse is the easiest concept for those outside the healthcare industry to understand (unlike Title III, "Tax-Related Provisions" or Title V, "Revenue Offsets," for example). Second, Administrative Simplification is an area of HIPAA where components of the law are now becoming finalized (e.g., the Transaction Rule in 2000 and the Privacy Rule in 2001).

Third, and most important, privacy and security of confidential medical records are hot-button issues that resonate with healthcare consumers. The potential for fraud and abuse is easy to imagine, and the consequences of compromised data would be personally devastating to any individual. As media coverage of HIPAA gravitates toward the integrity of patient records, consumers will be looking to healthcare organizations like yours for reassurance. They will need to hear that you are taking a proactive approach to assessment and implementation. They will need to hear that your company values their privacy and that you are working hard to protect it — and them.

An airtight document management network is an excellent answer to some of the tough questions your customers will ask. In fact, we expect proof points like these — i.e., tangible evidence that your organization can protect confidential patient information — will be significant differentiators up to and after the final HIPAA deadline, as your competitors seek to leverage HIPAA requirements to create new business opportunities and expand market share.

The Impact of HIPAA on Document Management

Congress enacted HIPAA — also known as the Kennedy-Kassebaum Act — in 1996 to accomplish a broad array of healthcare reforms. Through HIPAA, the federal government aimed to "improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and healthcare delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, [and] to simplify the administration of health insurance."

Like any other piece of federal legislation, HIPAA is vast and complex, with far-reaching effects and a moving-target timeline. HIPAA compliance is required of all healthcare providers, payers and clearinghouses. Providers include hospitals, clinics, nursing homes, private practice physicians, dentists and suppliers. Payers include group health plans, health insurance insurers, health maintenance organizations (HMOs), Medicare and Medicaid, and government healthcare programs. Clearinghouses include billing service providers, repricing companies and value-added networks. In short, all healthcare organizations in the United States need to develop a HIPAA strategy.

Complicating this is the fact that HIPAA does not define compliance methods. The Health Care Financing Administration (HCFA) will not publish a compliance checklist, and has not specified how it will police HIPAA requirements. As a result, individual organizations must determine how to achieve technical and administrative compliance.

Given the situation, it would appear that role of document management in facilitating compliance with HIPAA is ostensibly small. However, as we will see, improving document management will be critical for facilitating compliance with Administrative Simplification as well as emerging HIPAA regulations. Moreover, streamlined document management can have a powerful ripple effect on productivity and profitability in any healthcare organization.

Let's start with the three basic points where HIPAA and document management intersect in healthcare organizations.

1. HIPAA affects the documents healthcare organizations print, copy, fax and email every day.

To date, two elements of Administrative Simplification have made the transition from proposal to final rule. (The first was the Transaction Rule, which relates to establishing a single national standard format for electronic health transactions.) After lengthy public debate, HHS issued its final regulations to prevent the abuse or unauthorized disclosure of private health records in late December, 2000. The final Privacy Rule took effect on April 14, 2001. Healthcare organizations have two years to comply with the rule. (Smaller health plans have three years.)

According to the Privacy Rule, healthcare providers, payers and clearinghouses are prohibited from using or disclosing health information, except as authorized by the patient or specifically permitted by the regulation. Protection for health information starts when information becomes electronic, and stays with the information as long as it is in the hands of the provider, payer or clearinghouse. Information becomes electronic when it is sent electronically in a specified transaction (i.e. by fax or email), or when it is maintained in any computer system, from a desktop PC at a nurse's station to a full-scale data center in an insurance company. Paper versions of electronic information (i.e. prints, copies or received faxes) are also protected.

The Security Standards in Administrative Simplification are also of primary concern. Although the proposed rules have not been finalized, they will eventually mandate safeguards for the physical storage and maintenance, transmission and access to all individual health information that exists in an electronic format. These standards apply to all transactions adopted under HIPAA, as well as all individual health information that is maintained or transmitted.

The information covered in the final Privacy Rule and the proposed Security Standards is critical to the profitability of any healthcare organization; it includes the documents — such as patient records — that fuel the processes that providers, payers and clearinghouses use to authorize treatment, deliver treatment to patients, and administrate payment for these services.

This leads us to three important and interrelated conclusions. First, the volume of HIPAA-affected documents is astronomical, even for a small, single-physician practice. Second, changing the way these documents are managed will require extreme diligence and a concerted, organized, long-term effort. Third, changing the way documents are handled will require cooperation among providers, payers and clearinghouses.

2. HIPAA will require healthcare organizations to produce and/or manage large volumes of new documents on an ongoing basis.

Healthcare organizations already deal in high-volume paperwork and electronic files. Working toward compliance with HIPAA guidelines for Administrative Simplification adds whole new categories of documents to this already crowded environment. This affects you two ways: you will need to produce new kinds of documents quickly and cost-effectively; and you will need to receive them from external sources, distribute them, archive them and manage them. Examples of potential document overflow are abundant:

- **Training materials.** Changing one traditional workflow process in a large organization — let alone multiple overlapping procedures — requires comprehensive training and education on a wide variety of topics. To support your HIPAA-related training efforts, you will need to produce separate training packets, overhead and electronic presentations, copies of critical standards and procedures, and many other materials for each area of concern. The following is a small sample of training topics related to just two aspects of HIPAA (privacy and security):

- Awareness training for all personnel (including management)
- Periodic security reminders
- Virus protection
- Monitoring log in success/failure and reporting discrepancies
- Password management

- **Patient education.** HIPAA requires healthcare organizations to create a set of fair information practices designed to inform patients about how their information is used and disclosed, as well as ensure patients have access to information about them. Once these practices are in place, you will need to communicate these points to patients in a clear, concise and easy-to-read format. You will also need to update patients about new developments or updates to your policies.

- **Internal communications.** To raise awareness of the widespread implications of HIPAA for the entire healthcare enterprise, many organizations will need to provide continuous updates to employees at all levels about HIPAA-related progress, news, changes in legislation, timelines and other factors. These documents may take the form of posters, newsletters, booklets or simple reports.

- **Marketing communications.** To emphasize HIPAA-related results to customers and business partners, some healthcare organizations will need to produce short runs of high-quality, full-color marketing communications, including brochures, leaflets and handouts. These documents may be informal, such as leave-behind sheets for a town hall meeting, or formal, such as sales tools or press kits.

- **Standards documents.** As part of the Transaction Rule, HIPAA requires providers, payers and clearinghouses to follow six standard code sets for electronic document interchange (EDI). All of these standards are accompanied by voluminous documentation, and all are updated regularly. New standards will need to be rolled out to multiple points in your organization. As standards change, the updates will need to be tracked, monitored and deployed. The code sets are: American National

Standards Institute (ANSI) X12N; National Council for Prescription Drug Programs (NCPDP); International Classification of Diseases, 9th Edition, Clinical Modification (ICD-9-CM); HCFA Common Procedural Coding System (HCPCS); Current Procedural Terminology (CPT); and Current Dental Terminology (CDT).

- **Hardware and software documentation.** Although the majority of HIPAA-related changes will involve process improvement, new technology will be required — especially to meet the security and privacy standards for encryption. Each new solution adds its own small library of documents. Portions of these instruction manuals and operator guides will most likely need to be incorporated into training and education packets.

3. HIPAA will require healthcare organizations to document their HIPAA strategy, implementation plan and outcomes.

Step one toward HIPAA compliance for all providers, payers and clearinghouses is a thorough risk assessment, followed by the creation of a detailed action plan, implementation and administration of the plan, and an ongoing audit.

This is a vast undertaking that, again, will require your organization to produce a wide variety of new documents. You will most likely need to perform separate assessments for your business, transactions and security. Each assessment must include policy, procedure and practice evaluations. You must document these measures up to and beyond specific deadlines, and audits will cover policy and procedure — a new twist for the healthcare industry.

You must also consider the documentation necessary to design HIPAA efforts that are consistent with your core competencies and broader strategic initiatives. Doing this work now will reduce the risk of delays, which can lead to the implementation of expensive, non-strategic investments. Of course, understanding the full scope of your efforts will also allow more cost-effective planning and allocation of internal resources.

The point here is similar to number two above — you are opening up a new realm of documents. But the emphasis is different, and crucial. Training materials and communications will be important to your success. However, well-documented policies, procedures and change implementation plans will be vital to your profitability, productivity and competitive livelihood should you be faced with an audit.

Building an Agile Organization

It is clear that HIPAA is an enterprise-wide issue — not an information technology issue. There are legal, regulatory, process, security and technology aspects to each proposed rule that must be carefully evaluated before any healthcare organization can begin its implementation plan. Although facilitating compliance will involve some technology purchases, it will mainly involve changing the way your organization works. Not just how you handle documents — how you handle every component of operations.

In fact, recent research indicates that organizational processes, policy assessment and procedure redesign will represent up to 80% of the work your organization does to comply with HIPAA standards.

Which leads to the following conclusion: In the long run, it will be far more important for healthcare organizations to establish a productive, efficient organization that shares information easily, enables smooth collaboration among workgroups and across departments, and interacts with business partners seamlessly than it will be to purchase new technology.

The reasoning here is straightforward: The vast majority of your journey towards HIPAA compliance will involve planning and implementing changes — in policy, procedure and practice — across your organization. An agile, efficient organization is much better equipped to make these kinds of sweeping changes.

Agile healthcare organizations communicate underlying strategic thinking to their constituencies more effectively. They address issues and generate consensus more rapidly. They can create and distribute supporting documents without relying on outsourcing.

What's more, agile organizations become proficient at eliminating bottlenecks and crossed lines of communication, both of which hinder operational productivity and hurt the organization's ability to change and improve itself.

Most important, agile organizations can identify areas for improvement, determine how to make these improvements and actually change the process — without compromising productivity, budgets or the quality of their work, whether patient care (providers) or information delivery (payers, clearinghouses).

Keep in mind, this level of operational efficiency is impossible to achieve without a solid document management infrastructure. This is why document management will play such a vital role in your organization's transition to HIPAA compliance.

Consider, for example, costs. Facilitating HIPAA compliance will have a major impact on cost. Significant financial resources will be required at the outset, and on an ongoing basis. If your organization has fast, flexible and efficient document management you will be able to cut costs several ways. You will be able to produce most of your documents in-house, which eliminates the cost (and security risks) of using third-party vendors. You will be able to spend less to produce each document if you switch to digital systems in a networked architecture. You will spend less to maintain these systems, which are

Section 4.0

measurably more reliable than analog devices and traditional host printers. By reducing costs on an enterprise-wide scale, you can prepare your organization to absorb a portion of the financial impact of HIPAA. That means faster recovery and stronger ROI.

Consider also productivity. Agile organizations that manage documents effectively are by nature more productive. They can do more work and process more transactions in less time. By increasing productivity throughout your enterprise, you can prepare your business to roll out HIPAA-related changes quickly.

Exceptional document management also improves data security. Confidentiality is threatened not only by the risk of improper access to electronically stored information, but also the risk of interception during electronic transmission of the information. In other words, protected healthcare information needs to be monitored at multiple points in your document workflow, as well as multiple points in the document lifecycle. If workflow and document lifecycles are streamlined, it will be easier for your organization to ensure the privacy of sensitive documents no matter where they are.

Section 5.0

Critical Success Factors

As healthcare organizations move toward full implementation of HIPAA strategy, some will succeed and others will fail outright. Some will succeed, but overspend. Others will succeed, but achieve compliance too late. When it comes to document management, there is a wide range of variables that will determine where your organization falls on this spectrum. We have identified five critical issues that will play the largest part in determining your short- and long-term success in terms of document management.

1. Choose the right partner.

Every step toward compliance should come from your enterprise-wide HIPAA strategic plan. It is important to choose a document management partner that can help you with risk assessment, workflow analysis and security monitoring. You need a partner that understands networks, encryption and data security in addition to document creation, distribution and retention, and combines this expertise with a strong background in healthcare. You should also choose a partner that understands the full scope of HIPAA, and can easily tell you exactly how a given document management solution meshes with your overall strategy. What's more, your partner should understand the meaning of long-term support. The entire HIPAA compliance process will be a methodical arrangement that continues to evolve as new information is revealed, standards are updated, and your organization's priorities change over the next several years. It will be critical to choose a document management partner that is experienced in this type of long-term customer engagement.

2. Insist on exceptional documents.

Compare these two hypothetical situations:

Scenario 1: A 100-bed hospital is conducting its first training session with nurses about new processes for document encryption. The training leader distributes information packets to the attendees. Packets are obviously copied from a black-and-white original. The analog image quality is grainy. Some of the text is smeared and difficult to read. In fact, captions on charts and graphs are illegible. Pages are only copied on one side and stapled by hand. During the presentation, many documents lose their staples.

Scenario 2: A 50-person department in a large insurance company is meeting to kick off the first in a series of HIPAA compliance programs. The program leader distributes the information packets. These materials combine crisp text with full-color graphics. Each “copy” looks exactly like a printed original. The color makes key messages more memorable. The entire piece fits neatly into three-ring binders, complete with cover and insert sheets.

Which message would you rather send? The quality of the documents you produce — especially those that reach key employees — will speak volumes about your organization’s level of commitment to achieving HIPAA compliance.

3. Leverage digital technology.

In-house digital document management systems allow you to produce more kinds of documents in less time, with a lower total cost of ownership than older analog devices. Image quality is exceptional. Speeds run as high as 100 pages per minute or more. They typically offer special features that protect sensitive documents from unauthorized usage. They are often multifunctional, and can do the job of up to four separate systems (printer, host printer, fax, copier), which saves valuable floor space and cuts your costs. And unlike analog systems, digital systems can be connected to your network.

4. Establish a reliable document management network.

Standalone systems for document management are appropriate for smaller installations. But most healthcare organizations stand to gain a number of important benefits by moving document management to a network. In a networked environment, end-users can access a wider range of capabilities (copy, print, fax, host print) right from a desktop PC interface. In a networked environment, you can balance workloads across multiple departments instead of overloading a single system. Plus, you have built-in redundancy that allows you to take systems down and perform maintenance without compromising productivity.

5. Consolidate vendor relationships.

Effective document management involves hardware, software, installation, training, supplies inventory, network configuration, service and maintenance, and ongoing assessment of productivity for a wide range of technologies. Plus, HIPAA assessments require you to include vendor performance. By working with fewer vendors — or ideally, one vendor — you can simplify each of these activities. You will have only one number to call, and one familiar team to look to for issue resolution. Plus, HIPAA involves a great deal of standardization, as we have seen. It is difficult to standardize anything when you are negotiating with a different vendor for each component of your document management workflow.

Conclusion

Developing and managing flexible, enterprise-wide document management solutions requires careful planning, adequate internal resources and an informed, capable partner. To find the best partner — one that will enable you to achieve the five critical success factors — you will need to start the search process now. As you evaluate potential partners, your top priority should be strategic fit. Candidates should have a clear, straightforward approach to improving productivity, reducing operating costs and streamlining document processes. They should be able to articulate how their solutions interconnect with your overall strategy for HIPAA compliance. They should also have case studies and other proof points that demonstrate their competency in document management, as well as their expertise and experience in healthcare.

