



White Paper: Enterprise Content Management
for Regulatory Compliance

*Best Practices Credit Unions Should Adapt
from the Healthcare Industry*

managing content through innovation

bluepointsolutions.com

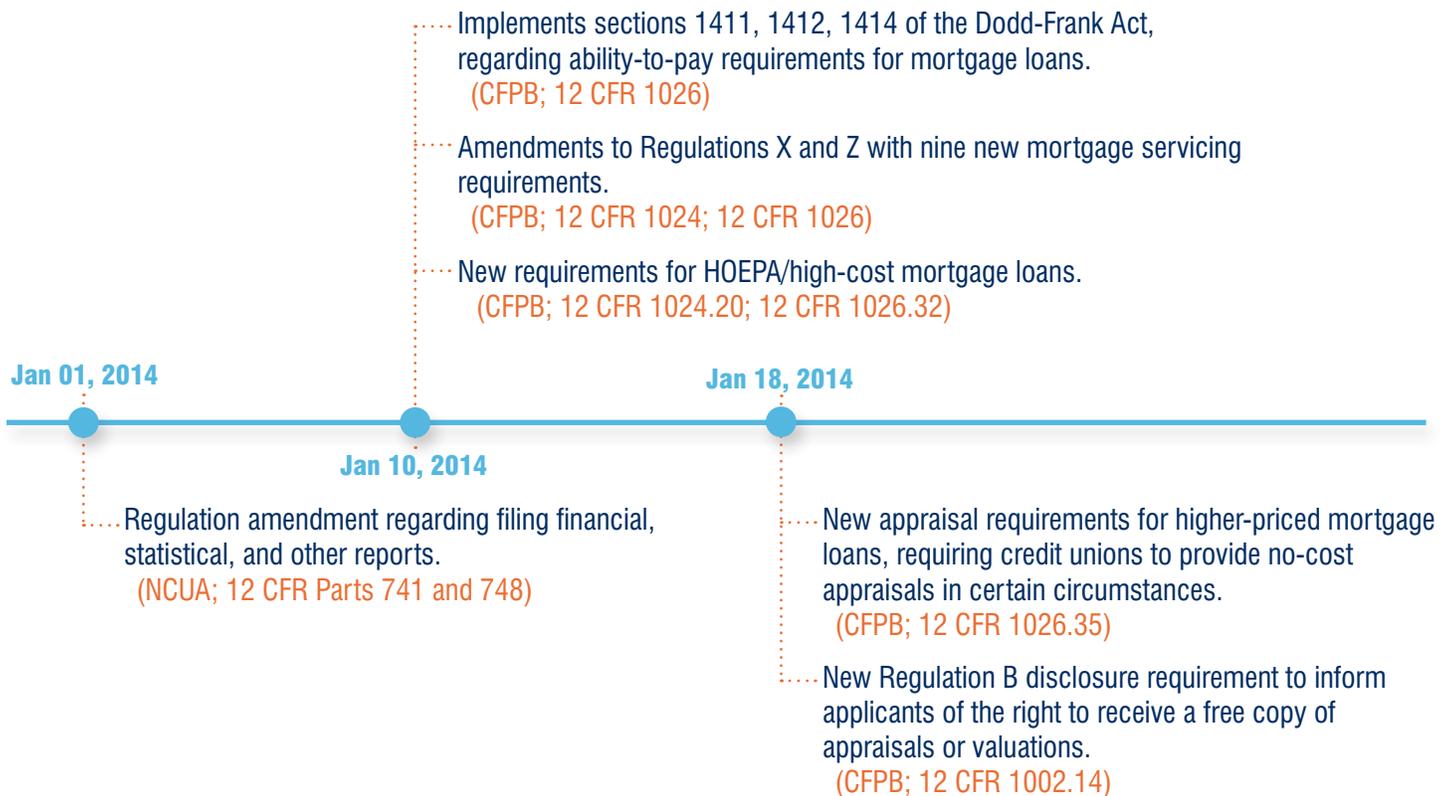
Enterprise Content Management for Regulatory Compliance:

Best Practices Credit Unions Should Adapt from the Healthcare Industry

I. Executive Summary

Credit unions now face a tidal wave of new compliance requirements that are steadily increasing the costs of managing and securing member information, and putting pressure on credit unions to find new solutions to keep these costs under control. Currently under-utilized by the majority of credit unions, an effective Enterprise Content Management (ECM) solution can be a tool for optimizing the management of critical member data, lowering the costs of managing that data, and finding new ways of extracting value from it, all while mitigating security and compliance risks. This paper presents key findings from examining similar challenges to the healthcare industry, which credit unions can learn from when responding to upcoming regulatory challenges.

UPCOMING COMPLIANCE REQUIREMENT TIMELINE



Enterprise Content Management (ECM) vs. Document Management

ECM systems are repositories of secure and searchable electronic documents and records that are captured and stored in any department of a company. More than just document imaging and management solutions that scan and store paper records, when deployed effectively, ECM systems' centralized security and search features mitigate compliance risks and increase employee productivity and operational efficiency.

Healthcare companies have successfully deployed ECM systems over the last ten years to manage risks associated with regulatory compliance, avoid millions of dollars of penalties, and streamline operations.

Many lessons can be learned by credit unions from the ways the healthcare industry uses ECM to address the following five regulatory challenges:

1. Information security risk
2. Paper documents reliance
3. Outsourced services risk
4. Siloed systems
5. Compliance costs



In the healthcare and credit union industries, information disclosure requirements and associated penalties have increased the impact of these challenges. Therefore, large volumes of data need to be identified, stored and indexed to meet compliance requirements. A secure and searchable centralized repository of electronic documents will help each industry achieve consistent, accurate and fast data retrieval, and risk mitigation, in addition to increasing productivity and improving service levels.

II. Overview of Regulations in Healthcare and Credit Unions

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 added teeth to The Health Insurance Portability and Accountability Act (HIPAA) of 1996 by significantly increasing the likelihood of penalties for privacy and

security violations.¹ Further, the US Office for Civil Rights (OCR), the body for enforcing healthcare regulations, upped the compliance ante by slapping on steep penalties for violations – from \$25,000 for each violation before HITECH to \$1.5 million thereafter – a 60-fold increase.

A secure and searchable centralized repository of electronic documents will help each industry achieve consistent, accurate and fast data retrieval, and risk mitigation, in addition to increasing productivity and improving service levels.

The OCR’s recent actions are teaching moments for the healthcare industry and point to the kind of information systems it needs to remain compliant. Here are three examples of lessons learned:

1. **WellPoint**, a healthcare insurance company, paid \$1.7 million for failing to secure protected electronic information of patients, and tracking the identity and rights of those gaining access to data.²
2. **CVS** and **Rite Aid** received penalties of \$3.5 million when paper records were stolen and misused by thieves.³
3. **Accretive Health** paid \$2.5 million, and was prohibited from doing business in Minnesota for four years, when a third party partner lost protected patient health information.⁴

RECENT HEALTHCARE COMPLIANCE PENALTIES

WellPoint	\$1,700,000
CVS & Rite Aid	\$3,500,000
Accretive Health	\$2,500,000

For these companies and the entire industry, the OCR now allows only ten days to produce HIPAA compliance audit documents.⁵ Thus the need for a single repository of all secured and easily retrievable electronic documents across all facilities and outsourcing partners of an enterprise is now an imperative.

The healthcare industry's recent past, hints at the credit union industry's future as it grapples with expansive new regulations for disclosures and underwriting of loans. These regulations were issued by the Consumer Financial Protection Bureau (CFPB) and are scheduled to go into effect in January 2014. The requirements associated with the new regulations have raised concerns in the industry, since credit unions now have to:

- Determine and document the ability-to-pay mortgages for primary residences based on eight criteria
- Comply with increased underwriting criteria for qualified mortgages and mandated rules for safe harbor treatment
- Disclose loss mitigation options and foreclosure protection for mortgage holders with delayed payments
- Display loan closing costs in standardized formats and show principal, interest, insurance, and servicing costs, including the impact of interest rates changes⁶

Given these new rules, documentation needs will explode at credit unions within a short time.

III. Challenges of Regulatory Compliance in the Healthcare Industry

Data breaches are pervasive and rising in the healthcare industry, even as enforcement has become more stringent, with the implementation of the HIPAA Omnibus⁷ rule in 2013 that extends liability to covered entities such as physicians' practices, business partners, and contractors in

healthcare facilities. The Poneman Institute Study of Patient Privacy and Data Security⁸ found that in 2012, 94 percent of healthcare organizations had at least one data breach and 45 percent experienced more than five incidents, compared to 29 percent in 2010. Studies like this highlight the five compliance challenges associated with the privacy and security regulations of HIPAA as follows:

1. **Information security risk:** Access to electronic patient records by unauthorized individuals was the largest reason for data breaches. HIMSS Analytics⁹ found that 56 percent of security breaches in 2012 were due to unauthorized access.

Unauthorized access to electronic and paper patient records by unauthorized individuals are the two most common reasons for data breaches

2. **Paper documents reliance:** Unlawful access to paper records was found to be the second most common reason for a data breach, accounting for 34 percent of the cases in 2012, up from 32 percent in 2008 according to the same study.
3. **Outsourced services risk:** An analysis of breach statistics issued by the Department of Health and Human Services found that 57 percent of the incidents of lost data occurred at the premises of business partners.¹⁰
4. **Siloed systems:** Patient data frequently resides outside of databases, in applications such as spreadsheets or email, resulting in multiple, unconnected information silos. As a result, this data becomes hard to track and is frequently lost. Sixty-one percent of respondents to a survey by Commvault expressed concern about unstructured and independent patient health information.¹¹

5. **Compliance costs:** The HHS estimated the costs of compliance for 700,000 healthcare entities to be \$98 million, plus an additional \$113 million for business partners.¹² And these are considered gross underestimates in industry circles, where it is believed that they don't include the costs of audits and securing patient data flows to business associates.¹³

57 percent of the incidents of lost data occurred at the premises of business partners

IV. Challenges of Regulatory Compliance in the Credit Union Industry

Credit unions are just now beginning a cycle of new compliance activity. The CFPB, which regulates a wide swathe of financial services, especially mortgage loans, currently penalizes operational inaccuracies with monetary fines, and does not tolerate inconsistencies across systems and partners.¹⁴ A recent spike in monetary fines for errors in the administration of mortgage loans has had a chilling effect as the indicator of concern over these fines zoomed to 408 at the end of April 2013, compared to a baseline of 100 in January 2013, according to a survey by Wolters and Kluwer.¹⁵ While the CFPB acknowledges that credit unions did not have a sizable role in the housing crisis, the consumer protection rules written for mortgages apply equally to credit unions and banks, with monetary fines imposed for loan processing errors. In fact, one non-bank, Mortgage Master, recently was forced to pay \$425,000 for errors in over 21,000 mortgage loan applications.¹⁶

Like the healthcare industry, credit unions have the same five compliance challenges in addressing regulations as follows:

1. **Information security risk:** While CFPB does not have formal jurisdiction over information security, which has historically rested with the Federal Financial Institutions Examinations Council,¹⁷ it does require IT systems to have sound internal policies and procedures including information security.¹⁸ The compliance demands for information security will necessarily rise with storage of a much larger volume of sensitive personal and financial information of members, which result from the underwriting standards required.

The healthcare industry's recent past, hints at the credit union industry's future as it grapples with expansive new regulations for disclosures and underwriting of loans

2. **Paper documents reliance:** Compliance with disclosures laws, such as Good Faith Estimates of loan charges and underwriting standards to determine the ability-to-repay, will require maintenance of document trails, both electronic and paper. And the error-prone tracking of paper documents will increase compliance costs. Already, investors purchasing mortgages in the secondary market are realizing productivity decreases as a result of increasing paper documents received from originators. These investors report that 20 to 40 percent of lenders routinely submit incomplete or inaccurate files. As a result, investors were able to review only 50 purchases per month in 2012 compared to 139 in 2009, according to Access Mortgage.¹⁹

3. **Outsourced services risk:** CFPB will now hold credit unions liable when a violation of consumer protection regulations happens during loan processing at Credit Union Service Organizations

(CUSOs).²⁰ This mandate greatly expands the scope of monitoring of CUSOs by credit unions.

4. **Siloed systems:** The core banking systems of credit unions, their enterprise software, are falling short for compliance needs. The 2013 survey by Wolters and Kluwer found that 40 percent of the respondents in credit union and banking industries view lack of integration of technology systems as a barrier to managing compliance risk. Further, only 17 percent of credit unions have a single repository of electronic documents, while seven percent have multiple electronic systems, and 69 percent have hybrid paper and electronic systems.²¹
5. **Compliance costs:** Credit unions are already dealing with 120 regulatory changes from Federal agencies since 2008 and many more are yet to come. The compliance costs for smaller financial institutions are now conservatively estimated at five percent of operating costs.²²

40 percent of the respondents in credit union and banking industries view lack of integration of technology systems as a barrier to managing compliance risk

V. Best Practices in the Healthcare Industry

The credit union industry can learn from the recent experience of the healthcare industry by developing IT systems to prepare for a regulatory onslaught. The process that began with adopting electronic health records to reduce paper documents has increasingly migrated to more complete ECM systems in order to integrate all data types and keep track of document flows across an extended enterprise, including partners. Below are examples of ECM benefits for each of the five compliance challenges:

1. The Wythe (Virginia) County Community Hospital increases information security:

This hospital now has an ECM repository that securely isolates cardiology, radiology and lab results. Specialists can now only access permitted records. In this case, anonymous and unauthorized access to documentation is prevented by centralizing all documents in an ECM, categorizing them by type and access, and limiting access rights according to users roles.

The core banking systems of credit unions, their enterprise software, are falling short for compliance needs

2. Baptist Health of South Florida moves from paper to electronic documents:²³

Baptist was so bursting with paper documents that it decided to purchase expensive offsite storage in Miami-Dade County, resulting in exorbitant fees for retrieving documents. After it installed an ECM system, completely manual processes are now automated, and all documents, clinical and business, are digital. This example shows that a healthcare facility using nothing but paper can successfully migrate to an all-electronic integrated content management system.

3. Sharp Healthcare of San Diego reduces business partner risk:²⁴

This California hospital needed to integrate its electronic health records across multiple facilities and third-party physician groups, and has connected its ECM system to an outside entity using ECM software from another vendor. Now patients can securely access their documents sourced from a third party system. Thus, integration of diverse systems across multiple healthcare facilities and partners now meets regulatory concerns.

4. Sharp Mary Birch Hospital aggregates their systems and records:²⁵ At this entity, doctors still receive faxes about changes to the medical records of patients, but now their ECM system is able to import these faxes to update electronic health records. Thus, ECM's integration of unstructured and structured documents helps doctors gain a complete profile of a patient.

5. Mental Health Center of Denver (MHCD) lowers cost of compliance: MHCD reported a rate of return of 1315 percent by deploying ECM.²⁶ This example shows that the implementation of ECM proves to deliver very high return on investment when reduced compliance penalties and increased efficiencies are considered. And unexpected returns are often gained, such as recouping of doctors' lost time when reviewing the complete online histories of medicines prescribed to patients.

Credit unions are already dealing with 120 regulatory changes from Federal agencies since 2008 and many more are yet to come

VI. Conclusions: Lessons for Credit Unions

ECM deployment at credit unions leads to consistent, accurate, and fast retrieval of documents required for audits. They also deliver higher data integrity from security applied at the point of record collection and retrieval, including access by outsourcing providers. But, in addition to compliance and security, ECM provides an opportunity to streamline and automate processes to gain efficiencies. With ECM, staff at credit unions can be relieved of the tedium of locating, retrieving, and searching documents, and giving them more time to understand and

serve member needs. With strong ECM systems, the reputation of companies is more likely to be protected when data loss is minimized with content access control.

Compliance costs for smaller financial institutions are now conservatively estimated at five percent of operating costs

When selecting an ECM system, it is important to choose a solution that addresses the five challenges outlined above. Product features and associated benefits that help credit unions match the achievements in the healthcare industry and provide operational efficiencies are as follows:

1. **Policy-managed security:** to create right-of-way for each user of the repository and not leave the entire pool open for anyone to access
2. **Digitization of documents:** to eliminate document loss and pilferage common with paper records
3. **Open standards:** to ensure integration across ECM systems
4. **Centralized repository:** to aggregate all documents, structured and unstructured, in one place for secure and rapid retrieval required for compliance audits
5. **Comprehensive:** to meet current compliance with fewer resources, gain organizational efficiencies and streamlined operations, and improve customer service for current and prospective members

By keeping these five criteria in mind when searching for and implementing an ECM system, credit unions can surely realize all the benefits healthcare companies are now achieving, without experiencing as much pain as those companies have over the last ten years.

1. "As HIPAA Regulations Get Teeth, Healthcare Firms Feel the Bite," by Paul E. Proctor, Wes Rishel, October 2012, Gartner - <http://www.informationweek.com/whitepaper/healthcare/policy/as-hipaa-regulations-get-teeth-healthcare-firms-f-wp1381414778>
2. "Ready or not: HIPAA gets tougher," by Erin McCann, Healthcare IT News, 15th August 2013 - <http://www.healthcareitnews.com/news/ready-or-not-hipaa-gets-tougher>
3. "HIPAA violators get few penalties for trashing your privacy," by Bob Segall, wthr.com - <http://www.wthr.com/story/20153005/few-penalties-issued-for-trashing-your-health-care-privacy>
4. "HIPAA Final Rule: Preparing for New Business Associate Obligations and Liability Risks," by Reece Hirsch, Morgan Lewis, June 2013 - http://www.morganlewis.com/pubs/AIS_Webinar_NewProvisions_12feb13.pdf
5. "Unprepared entities risk being hit with hefty financial penalties," by Michelle DeBarge and Jody Erdfarb, Connecticut Law Tribune, Vol. 38, No. 20, 14th May 2012 - <http://www.wiggin.com/13712>
6. "CFPB Finalizes "Know Before You Owe" Mortgage Forms, November 20th 2013 - <http://www.consumerfinance.gov/newsroom/cfpb-finalizes-know-before-you-owe-mortgage-forms>
7. "What You Need to Know about the HIPAA Omnibus Rule," by Todd A. Rodriguez, Esq, AAOS - <http://www.aaos.org/news/aaosnow/jul13/managing4.asp>
8. "Third Annual Benchmark Study on Patient Privacy and Data Security," Ponemon Institute, December 2012 - http://www2.idexperts.com/assets/uploads/ponemon2012/Third_Annual_Study_on_Patient_Privacy_FINAL.pdf
9. "2012 HIMSS Analytics Report: Security of Patient Data," Kroll Advisory Solutions - http://www.krollcybersecurity.com/media/Kroll-HIMSS_2012_-_Security_of_Patient_Data_040912.pdf
10. "Breach Report 2012, Protected Health Information," Redspin, February, 2013 - <http://www.slideshare.net/RedspinInc/redspin-phi-breach-report-2012>
11. "Managing the Exponential Leap in Healthcare Data Growth: Achieving Compliance and Operational Efficiency," Commvault - webdocs.comvault.com/assets/2013-healthcare-it-survey-summary-whitepaper.pdf#!
12. "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act," January 2103 - <https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the>
13. "The HIPAA Conundrum in the Era of Mobile Health and Communications," by Jason Wang, MD and Delphine J Huang, Journal of American Medical Association, September 2013 - <http://jama.jamanetwork.com/article.aspx?articleID=1732507>
14. "Compliance Hot Topics," by Robin D Hoag, Doeren Mayhew, March 2013 - <http://www.slideshare.net/trmooreandco/credit-union-compliance-hot-topics>
15. "Regulatory and Risk Management Indicator," Wolters Kluwer, June 2013 - <https://www.cuinsight.com/press-release/regulatory-and-risk-management-concerns-climbing-for-banks-and-credit-unions>
16. "CFPB Takes Action Against Nonbank and Bank for Inaccurate Mortgage Loan Reporting," October 2013, <http://www.consumerfinance.gov/newsroom/cfpb-takes-action-against-nonbank-and-bank-for-inaccurate-mortgage-loan-reporting/>
17. "CFPB: What is New Regulator's Role?" by Tracy Kitten, CU Info Security, July 17th 2013
18. "Implementing the CFPB-required Compliance Management System (Part 2)", <http://www.complianceguru.com/2013/02/implementing-the-cfpb-required-compliance-management-system-part-2/>
19. "The Hidden Costs of Compliance," <http://www.elliemae.com/pdf/em-whitepaper-compliance.pdf>
20. "Third-Party Compliance Traps for CUSOs, Vendors and Credit Unions," by Michelle A Samaad, CU TIMES, September 27, 2013 - <http://www.cutimes.com/2013/09/27/third-party-compliance-traps-for-cusos-vendors-and>
21. "The State of Enterprise Content Management in Credit Unions," Bluepoint Solutions, 2013 - http://www.bluepointsolutions.com/stateofecm_2013/
22. "Financial Industry wrestles with compliance costs," Mainebiz, 1st April 2013 - <http://www.mainebiz.biz/article/20130401/CURRENTEDITION/303289999>
23. "How ECM implementation reduces medical record storage footprint," by Don Fluckinger - <http://searchhealthit.techtarget.com/tip/How-ECM-implementation-reduces-medical-record-storage-footprint>
24. "Comparing standalone ECM software to EHR vendor offerings," by Don Fluckinger - <http://searchhealthit.techtarget.com/tip/Comparing-standalone-ECM-software-to-EHR-vendor-offerings>
25. "Integrating IT for next-gen EMRs," by Jared Blankenship, Health Management Technology, March 2013 - <http://www.healthmgtech.com/articles/201303/integrating-it-for-next-gen-emrs.php>
26. "MHCD turns paper into treatment rooms - and income," by Dennis Grantham, Behavioral Healthcare, 2nd July 2013 - <http://www.behavioral.net/article/mhcd-turns-paper-treatment-rooms-and-income>