IRON MOUNTAIN®

TRANSITIONING FROM AN OPEN ENVIRONMENT TO A CLOSED ENVIRONMENT TASK FORCE REPORT

JULY 2015

LAW FIRM INFORMATION GOVERNANCE SYMPOSIUM JULY 2015

CONTENTS

BACKGROUND

Since 2012, the Law Firm Information Governance Symposium has served as a platform for the legal industry to collaborate on information governance (IG) best practices in the unique setting of law firms. The Symposium publications offer definitions, processes and best practices for law firm IG. In 2014, four task forces were assembled by the Symposium Steering Committee to work on specific, current law firm IG topics. This Transitioning from an Open Environment to a Closed Environment Task Force Report focuses on factors to consider and possible steps to take when contemplating increasing information security in the firm.

SYMPOSIUM STEERING COMMITTEE

BRIANNE AUL, CRM
Firmwide Records Senior Manager
Reed Smith, LLP

LEIGH ISAACS, IGP, CIP
Director, Records & Information Governance
White & Case LLP

RUDY MOLIERE
Firm Director Records and Information
Morgan, Lewis & Bockius LLP

STEVEN SHOCK
Lead Consultant / Interim Director, Network
Information Management Systems
eSentio Technologies

CHARLENE WACENSKE
Senior Manager FW Records
Morrison & Foerster LLP

TASK FORCE

BRIANNE AUL, CRM
Firmwide Records Senior Manager
Reed Smith LLP

BRYN BOWEN, CRM
Principal
Greenheart Consulting Partners

GALINA DATSKOVSKY
CEO
Vaporstream

BRIAN DONATO*
CIO
Vorys, Sater Seymour and Pease LLP

KATHRYN HUME
Independent Consultant

SHARON KECK
Director of Risk & Records Info. Management
Polsinelli PC

NORMA KNUDSON
Director of Facilities Management
and Compliance Support
Faegre Baker Daniels LLP

FRANK LASORSA
Director of Records and Compliance
Kelley Drye & Warren LLP

STEVEN SHOCK
Lead Consultant / Interim Director, Network
Information Management Systems
eSentio Technologies

BRETT WISE, CRM, IGP, CIP
Director of Records and Information Management
American Board of Pediatrics

***Task Force Leader**

SYMPOSIUM PARTICIPANTS

Iron Mountain would like to thank the following individuals for participating in the peer review sessions of the 2015 Symposium event and for sharing their perspectives and expertise during the creation of this task force report.

ANGELA AKPAPUNAM
Director of Document Lifecycle Services
WilmerHale

KAREN ALLEN
Manager, Information Governance Technologies
Morgan Lewis & Bockius LLP

DERICK ARTHUR
IG Operations Manager
Cooley LLP

BRIANNE AUL, CRM
Firmwide Records Sr. Manager
Reed Smith LLP

BRYN BOWEN, CRM
Principal
Greenheart Consulting Partners

BETH CHIAIESE, CRM, MLIS
Director, Professional Responsiblity & Compliance
Foley & Lardner LLP

SCOTT CHRISTENSEN
CIO at Large

TERRENCE COAN, CRM
Senior Director
HBR Consulting

JULIE COLGAN, IGP, CRM
Head of Information Governance Solutions
Nuix

GALINA DATSKOVSKY
CEO
Vaporstream

BRIAN DONATO
CIO
Vorys, Sater, Seymour and Pease LLP

BETH FAIRCLOTH
Director of Risk Management
Seyfarth Shaw LLP

STACEY FIORILLO
Director of Records Management
and Information Governance
eSentio Technologies

PATRICIA FITZPATRICK
Director of Information Governance & Compliance
Katten Muchin Rosenman LLP

JAMES FLYNN, CRM
Director of Records and Docket
Winston & Strawn LLP

GRANT JAMES, CRM
Senior Manager Information Governance
Troutman Sanders LLP

SHARON KECK
Director of Risk & Records Info. Management
Polsinelli, PC

CHARLES KENNEDY
Firm Director of Records and Docket
Jones Day

SAMANTHA LOFTON
Chief Risk and Information Governance Officer
Ice Miller LLP

FARON LYONS
Enterprise Account Executive
Alfresco Software

RUDY MOLIERE
Firm Director Records and Information
Morgan Lewis & Bockius LLP

DANA MOORE, IGP
Manager of Records and Information Compliance
Vedder Price PC

DERA NEVIN
Director, eDiscovery
Proskauer Rose LLP

RANDY OPPENBORN
Director, Information Governance
Foley & Lardner LLP

ALEXANDRA PROPHETE
KM Operations Manager
Cleary Gottlieb Steen & Hamilton LLP

DEB RIFENBARK, IGP, CRM
Director of Records and Compliance
Stinson Leonard Street LLP

STEVEN SHOCK
Lead Consultant / Interim Director
Network Information Management Systems
eSentio Technologies

SCOTT TAYLOR
Manager of Records, Conflicts
& New Business Intake
Smith, Gambrell & Russell LLP

CHARLENE WACENSKE
Senior Manager Firm Wide Records
Morrison & Foerster LLP

JOHAN WIDJAJA
Assistant Director Records & Information
Morgan Lewis & Bockius LLP

JOEL WUESTHOFF
Senior Director
Robert Half Legal

EXECUTIVE SUMMARY

This task force report was created to help law firms make an informed decision when considering how best to transition their firms to a higher level of information security to both protect firm data as well as client-supplied information.

This report will detail potential factors motivating firms to contemplate moving to a closed environment as well as key issues to contemplate before undertaking such a transition. The report will then propose potential solutions to consider including practice guidance and emerging technologies that can automate some or all of the security regime. Finally, this report explores best practices for changing organizational culture to ensure a seamless adoption across the firm, including how to communicate these changes and how to audit for compliance going forward. The primary scope of this report focuses on data within the firm's document management system (DMS), though it will address collaboration sites, file shares and externally hosted applications as well.

INTRODUCTION

Information security within the legal industry has been subject to intense scrutiny for several years, arguably, more than it has ever been in the past. The message has come through various channels consistently (client audits, the HIPAA Omnibus rule, The New York Times, and the FBI to name a few): law firms must continue to improve client data security. Typically, how a firm elects to do this largely depends upon three factors: demographics (including the firm's client base and practice scope), direct instruction by clients through outside counsel guidelines (OCGs) and the responses of others in the industry.

Historically, law firms have fostered an environment of knowledge sharing and collaboration to efficiently service their clients. To support this objective, many firms by default have configured their document management systems and other data repositories as open (further defined below) with ethical walls or other security measures applied on specific matters or documents as required. Over the past few years, more stringent regulatory and client security requirements have prompted many of these same firms to re-evaluate this open structure. These firms are now considering restricting data access to only those individuals within a given practice area or those working specifically on a given matter. In fact, some firms have already taken steps to modify their default security to a more secure limited access or closed capability (also defined below).

This closed approach is not without its own unique set of challenges. For example, will modifying the existing open structure create knowledge management inefficiencies for attorneys who often need to respond urgently to client requests? How will firms, especially those subject to fee arrangements based upon similar work being performed across a set of matters, ensure the necessary individuals have access to the documents they need? What training and policies should a firm consider implementing to proactively curtail workarounds which circumvent the new security structure? Lastly, and a critical IG challenge, what options do firms have available when determining who will be responsible for monitoring/modifying the required security throughout the matter lifecycle?

DEFINING OPEN AND CLOSED SYSTEMS

For purposes of this report, the Task Force utilized the following definitions for open and closed systems:

- **An open system refers to the absence of access controls by default. Generally, any user of the system can search for and access a document by default.**
- **A closed system refers to a system whereby a solution restricting access to information exists, and by default subgroups of documents are restricted and can only be searched and accessed by restricted groups of users. Which groups can view which documents may depend upon the practice group, the client, the type of document, the content of the document or other metadata.**

As is usually the case with many IG initiatives, the process of transitioning from an open environment to a closed environment will impact almost every individual within the law firm, from the administrative departments who implement the changes to the secretaries and timekeepers who need access to the information on a daily basis. For firms that assign the responsibility of security administration to the latter group of individuals, the impact may even be greater. The content of this report may be relevant to many parties within the law firm, but at a minimum will be essential for those individuals and departments responsible for:

- Information governance
- Information technology applications and infrastructure
- Information security
- Privacy
- Knowledge management
- Records management
- Risk management/compliance/general counsel
- Practice management

OPPORTUNITIES AND BUSINESS DRIVERS

Recent industry and regulatory forces affecting law firm clients are now requiring law firms to take a hard look at their internal information governance policies in order to remain competitive and in compliance with client demands. Names like Sony®, Target®, The Home Depot®, JPMorgan Chase & Co.® and Neiman Marcus® have made headlines as examples of large, sophisticated retail and financial services organizations that fell victim to information security breaches. These examples of large data breaches have transformed the consumer perceptions of those organizations' brands and reputations and increased the pressure on law firms to tighten their approach to security.

Along with data breaches, major industries have also faced significant regulatory changes. In December of 2014, Benjamin Lawsky, superintendent of New York's Department of Financial Services, announced increased regulatory efforts to assess the information security protocols across the financial industry with special focus on the security of third-party vendors like law firms.[1] The previous year, the HIPAA Omnibus Rule rocked the legal industry by requiring compliance from (and holding liable) any third-party business associate (including law firms) that provides services to a HIPAA-regulated entity which involves the transfer of protected health information (PHI).

Law firms are not immune from the general societal phobia and concern regarding the safety of digital information, especially as they house their clients' most sensitive company data (e.g., trade secrets, intellectual property and information about impending mergers and acquisitions), and personal information (e.g., medical records and the content of personal wills). Given that one unfortunate incident can completely transform a brand identity, it's not surprising that senior management's core motivation to devote time, money and energy to information security is to protect the firm's reputation. The mere statistical likelihood of a breach, reinforced by the industry's increased attention to the importance of security, is prompting firms to revisit their information security practices and invest heavily in tools designed to either prevent security breaches or to detect them when they occur.

Many of today's security professionals have conceded that a breach will inevitably occur, particularly since hackers (like physical viruses) mutate and learn more quickly than their prey can adopt new defense mechanisms. The majority of law firm risk management and security professionals have therefore shifted their view of what constitutes a strong defense by developing and implementing practices that mitigate the impact of a breach should one occur. Fortunately, one age-old technique that goes a long way in containing the impact of a breach is that of using access controls, be they role-based (where access to information is restricted based upon job function), mandatory (where users need specific credentials to access classified information) or minimum necessary (where access to information is restricted to those who explicitly require access to do their work). The open versus closed debate is effectively a deliberation on which access control model is appropriate for law firms now that the risks of a breach potentially exceed the benefits traditionally accorded to the efficiency and productivity inherent in an open system.

In practice, it is often client or regulatory requirements that ultimately drive law firms to consider shifting from an open system to a closed system. The past few years have seen an increase in the responsibilities of regulated entities to manage information security and operational risk in both their own environments, and those of third-party business partners. The regulatory changes impacting law firm clients are transitively impacting law firms via the vehicle of outside counsel guidelines, requests for proposals (RFPs), information security questionnaires or contracts

like business associate agreements (BAAs). Through these methods, clients often mandate that their information be only accessible to those attorneys and staff working on the matter in question. Some clients require this protection on all highly sensitive information; others require minimum necessary protection on personal sensitive information like medical records, social security numbers or other identifiers.

Some firms have clients and practices that expose them to national security scrutiny as part of the International Traffic in Arms Regulations (ITAR).[2] These regulations dictate that information and material pertaining to defense and military-related technologies (items listed on the U.S. Munitions List) may only be shared with US persons unless authorization from the Department of State is received, or special exemption is used. In law firms with open by default systems, meeting these regulations may pose particular challenges; however the consequences of non-compliance are potentially severe.

Despite the growing pressure placed on law firms, old habits die hard. While implementing a minimum necessary information access model may theoretically be the best information governance technique to contain the impact of a breach, it often meets resistance in practice. Attorneys remain confident that their ingrained duty to protect client confidentiality, as required by the Model Rules for Professional Responsibility, will suffice to meet today's risk and that restricted access controls would hamper their ability to work competently. Most auditors would not agree, in part because many of the users of these systems are not attorneys. This conflict is one of many issues to consider when examining whether, and how, to close a system.

CONSIDERATIONS WHEN CLOSING A SYSTEM

Many factors must be taken into account when a firm considers changing the overall security of its environment. How well the change manager can identify the appropriate interest areas and decision makers within the firm and to what extent they need to be involved in strategy, planning and execution will ultimately determine how effective such a change will be. In firms that are larger and more geographically spread out and/or more practice-diverse, this task can become increasingly challenging for the change manager to address.

Law firms are often resistant to change, however certain drivers may make the change easier for the firm to implement. When the need for security is driven by clients' OCGs, the firm might better overcome the institutional inertia against change, assuming the firm is agreeable to the guidelines listed within. It may also be easier for the firm to implement such a change for a particular practice, such as a practice group that requests only members of their team have access to their client matters. Or perhaps certain clients, like banks, for instance, require that access to their information is restricted to a pre-defined working group. When the driver is a regulatory requirement, compliance with the law typically trumps any resistance to secure the impacted data. For example, there are an increasing number of firms concerned with the exposure of personally identifiable information (PII) and PHI within their environment, including where that information is and who needs to be restricted from accessing it.

The scope of locking down an entire environment can be broad as well. It can include locking down access to certain information for internal users and external long-term contractors. It can encompass the entire firm or only specific departments and practice groups. It can be limited to internal systems or be extended to the flow of information outside firm walls. In the following section, the assumed scope is anyone with access to internal systems, but the section will touch on other possibilities as well.

MANAGING INSTITUTIONAL KNOWLEDGE AND LEGAL PREDEDENTS IN A LOCKED-DOWN ENVIRONMENT

Many firms have historically fostered an open environment allowing most users almost unlimited search access to firm-proprietary knowledge and precedent material. In many situations, the environment is structured to align with the firm's knowledge management (KM) initiatives. As such, attempts to limit open access need to account for a number of factors in order to maintain acceptable, productive access to precedent and general knowledge, including:

- **The challenge of creating scrubbed (in a closed system) versus non-scrubbed (in an open system) knowledge and precedent material.**
- **Effective information data mining beyond legal precedents, such as creating budget models from similar matters, and the ability to leverage work on prior matters as business development opportunities for the firm.**
- **Transitioning to a concerted KM effort[3] (including engineering correlations, how to structure information redaction as part of the precedent process, how to build in a precedent generator in work product development and how to identify appropriate KM work product, such as winning briefs, groundbreaking legal work, successful deal documents and documents associated with managing a matter under budget).**

THE LOGISTICS OF APPLYING SECURITY

Another key consideration for a firm moving to a closed environment is how to best create an efficient mechanism to either add or remove access to information associated with clients, matters and/or groups of clients and matters. It is useful to think about this process using three approaches: centralized, distributed and mixed.

Centralized approach: In the centralized approach (during matter intake), the firm restricts access to the matter to need-to-know parties only. If additional users ultimately need to be added to the matter, a designated team can be contacted to add them accordingly. To be successful, those charged with making access control decisions should understand why a particular workspace is restricted, and who has the authority to grant (or deny) access. They should have a documented change management process to follow and be equipped with an understanding of how to escalate certain situations (e.g., if there is an ethical wall involved, consult the GC's office).

While this approach allows robust control over matter security, it can be very difficult for attorneys to add people on the fly. If the process isn't efficient, people may not follow it. For example, if the need arises for someone (currently not approved) to review a given document, if not quickly addressed, the attorneys are likely to simply check out and send the document to the individual, thus completely circumventing security. Therefore, ease of use should be taken into consideration when deciding on a given approach.

Distributed or user-dependent security approach: In this approach, the firm relies upon the attorneys and the matter team to decide when and how to secure the document. This approach involves both the training of staff and the deployment of tools that will help staff secure the information accordingly – both in the DMS and when transmitting it to other locations. Such tools might include secure email, encryption software, etc. Should a firm elect this approach, it is critical to include an audit trail of actions performed by individuals within the firm.

Mixed approach: In this approach, the matter is secured from its inception, as in the centralized approach. Attorneys on the team are given the ability to grant appropriate access to both internal and external parties when needed. For the best results, software tools to enable encryption and persistent security should be deployed as well. This approach should also include an audit trail of the ad-hoc users added by the attorney. It should allow for compliance monitoring, and ideally, it should be used beyond the DMS.

For all of the above approaches, the firm must also determine which documents are in scope for being secured. For example, a firm may choose to secure only documents containing PHI or PII, or documents containing a client's confidential information. This approach reduces the number of documents impacted, since the majority of documents in the DMS are typically not sensitive beyond the normal expectation of client service standards. The feasibility of this approach will depend on the firm's client base, and the effectiveness of the technology and/or process employed to implement such a targeted lock down.

CHANGE MANAGEMENT/COMMUNICATION CONSIDERATIONS

Given the potential reluctance for attorneys and staff to adapt to the new security structure, it's critical for a firm to use proper change management methodology when implementing such a change within its environment. At minimum, the firm should consider the following questions:

- **Who are the influencers within the user community? How can they help the firm promote the new security protocols?**
- **What will the future state of the firm be once the default access has been modified?**
- **Why is it important that the security be modified? What are the firm's objectives?**
- **How does the firm promote that leadership supports this change?**

There are a number of cultural considerations that a firm will need to ponder when identifying the most successful approach to introducing the new security structure to its users. Some key factors to consider are the firm's organizational structure, size, practice group composition and geography. For example, a firm with a centralized organizational structure may want to ensure the change communication comes from the global leadership team, while a firm with a decentralized organizational structure may benefit from the communication being disseminated by the team leaders within various offices and practice groups.

Once the firm has identified who will disseminate the message, they will then need to focus on how the message can be sent. Meeting individually, or in groups, may offer users the chance to proactively raise concerns or pose questions they may not otherwise ask until the new security has been implemented. Firms may also want to utilize emails, newsletters, their intranet or social media to communicate and reinforce the benefits behind the new security structure.

A firm has multiple options available when determining their change management plan. Regardless of the path they choose, it is critical that consistent communication be part of the process. In the planning/strategy phase, communication should be focused on ensuring that leadership and stakeholders understand and support the proposed security structure. In the testing phase, communication should be focused on instruction to, and feedback from the pilot group. In the implementation phase, communication will need to be carefully planned, staged and timed in line with the project plan. By ensuring that communication remains two-way throughout the key project phases, the firm will exponentially increase its chances of successful user adoption.

TRAINING CONSIDERATIONS

When transitioning to a more restricted information access environment, developing an evolutionary training program and setting up a robust support platform are critical to user adoption, understanding and compliance with the new policy. First, a firm should identify and understand the constituency of its users, as well as their interests and needs, before developing targeted training programs. For maximum effectiveness, a firm should consider structuring training in discrete, easily consumable, contextual packets that will not take a lot of time and can be reinforced periodically to confirm compliance. Creating context for training is especially important, and a firm should locate areas of common interest first. They may review practice group regulations, OCGs or other client requirements that contain specific instructions that must be followed. For example, if part of the policy is to restrict information related to clients and matters for a particular practice area, then training for members of that practice area should be designed with those requirements in mind.

It is imperative that a firm's training materials focus on the specific user audience being trained, and that it encompass all types of users including current users, new hires, departing individuals and users who may not actually be employees (e.g., contractors and outsourced staff). Table 1 serves as an example of how a firm may divide its audience.

POSSIBLE AUDIENCE SEGMENTS FOR TRAINING

AUDIENCE TYPE	EXAMPLES
Billing Timekeepers	Attorneys, paralegals, other paraprofessionals, litigation support staff
Non-Billing Timekeepers	LAA/secretaries, project managers, resource secretaries, document services, records management, office services
Key Stakeholders in the Securing Process	Ethical/legal compliance, General Counsel's office, conflicts attorneys and staff, knowledge management, new business intake team, docket, accounting, ancillary services (marketing, etc.)
IT Staff	Infrastructure, applications development, help desk (training and updated guidelines for them is crucial), DBAs, desktop support, etc.
Third-party	IT vendors, consultants, electronic discovery firms

TABLE 1

Tailored, reinforced training may also assist firms during attorney departures. Most firms have a process for handling departing attorneys, however attorneys may not be educated on the process until they have decided to leave the firm. In an open system, the departing attorney is able (although probably not authorized) to take whatever documents they can find in the DMS. In a closed system, security changes may be necessary to allow the appropriate access to documents during an attorney departure. Ensuring that all attorneys are educated and reminded of the firm's departure process may prevent a situation like the following: In a recent breach experienced by a major multimedia conglomerate, investigators found multiple files containing sensitive salary information for a major audit/accounting firm. Those files should have never left the audit firm to begin with, and they should have never been loaded onto the conglomerate's servers. While this breach did not occur at a law firm, it reinforces the importance of proactive, consistent education regarding the firm's departure process so that data is transferred in accordance with established firm policy.

TECHNOLOGIAL CONSIDERATIONS: OPTIMISTIC VS. PESSIMISTIC DMS[4]

Firms should examine several technological considerations when locking down their environment. First, a firm must choose how to deploy its DMS. In an optimistic deployment, all matters and documents are open unless otherwise secured. Users are essentially trusted to only access that information which they legitimately need. Conversely, in a pessimistic deployment all matters and documents are secured and only opened to those who require access. Users are essentially not trusted to access only the information they legitimately need. Most firms originally deployed their DMS systems in an optimistic manner, consequently if they desire a different approach, it may take quite a bit of planning to change both the technology and the mentality of its users. Such deployment changes must be carefully planned and discussed with the IT and practice management functions.

THOUGHTS ON OTHER SYSTEMS

Because sensitive information doesn't live solely in the DMS, firms should consider other technologies to further secure their documents and environment. Examples include:

Data Loss Prevention (DLP): DLP software generally controls data-in-motion. For example, the firm might set a policy that stops any document with personally identifiable information from being emailed. DLP software can also alert administrators that a potential violation is taking place, without actually preventing an action. This kind of software is generally complimentary to DMS security.

Encryption: Documents may also need to be encrypted when shared with outside parties, and sometimes even within the firm. External (e.g., client) documents of a highly sensitive nature that might contain, for example, HIPAA-protected data may need to be encrypted when shared so that only authorized parties can access them. Further, documents containing sensitive internal information (e.g., partner compensation) may likewise need to be encrypted – even in the DMS. Encryption comes in many flavors: it can involve key exchange or can be policy-based and transparent to the end user.

AUTHORIZED EXTERNAL USER CONSIDERATIONS

In a law firm environment, the term *authorized external user* mainly applies to a client or third-party granted access to a firm's collaboration site (e.g., a deal room or litigation discovery room which are not systems of record). In some cases, if the firm is using contractors, they could be given access to the DMS on a limited basis to only work on the matter for which they were contracted. In general, access by non-employees to the firm's DMS (and other information repositories of record) should always be restricted.

POTENTIAL SOLUTIONS

Whether information security be applied only to the DMS, or extended to other repositories like Microsoft® SharePoint or file shares, firms can consider three basic approaches to securing documents:

» 1. Maintain an open DMS, and secure documents as appropriate.

» 2. Maintain a closed DMS, and share documents as appropriate.

» 3. Employ a hybrid approach, closing some matters, and leaving others open.

These approaches can be mixed to manage required document security changes.

» Approach 1: Open by Default DMS – Securing Documents as Appropriate

As most have an open DMS, permitting individual authors to apply document security is often the path of least resistance. Following this approach, documents are public to all DMS (or SharePoint or file share) users at the time of their creation. Applying higher-level security to a designated document requires that authors take additional steps to make the document private, and then provide access to appropriate individuals. During the course of a matter, various users will transition to/from the team that may need access to the document; as such, the legal team working on the matter must update document security accordingly. Most DMS systems enable users to apply this type of security to entire folders and matters, easing the burden of applying the same security settings to multiple documents.

There are several potential drawbacks to this approach. First, it can be very difficult to verify that security is being appropriately applied across the system. Second, the task of applying security can be very burdensome on the end users. Third, this approach does not scale well when different users require different access levels to multiple matters for the same client. In practice, this approach is rarely reliable, and likely would not pass client audit scrutiny.

» Approach 2: Closed by Default DMS – Sharing Documents as Appropriate

At the other end of the spectrum, firms can set all documents private to the author by default. If other users need access, the author (or delegate) must explicitly grant access rights. This approach complies with client requirements that only those working on their matters access their documents.

As with the open approach, there are practical drawbacks. First, firms must manage competing client demands to deliver work product both efficiently and securely. As access restrictions hamper knowledge management and reuse, firms must find alternative means to ensure productivity and consistent quality. Second, this approach can burden the document author (or delegate) given the time spent to adjust the security as matter teams evolve. Finally, since many matter and client documents don't require such tight security, attorneys on less sensitive matters will likely resist what they consider to be unnecessary administrative requirements.

» **Approach 3:** The Hybrid Approach

To balance the previously mentioned setbacks, firms can consider a hybrid approach. Here, central information governance and risk management teams leave certain documents public to internal attorneys and staff, but automatically apply security controls to other, more sensitive information. The challenge is to decide which information should be available to which people, and to then develop and implement the processes, integrations and automations required to apply security appropriately.

When considering a hybrid approach, some firms start by shifting from client and matter-level security to larger access control groups such as practice groups, jurisdictions or offices. For example, if a firm has an Intellectual Property (IP) practice, the firm could implement security so only IP lawyers have access to documents associated with IP matters, or a *doctype* of *Patent*. Documents for other practice groups would remain accessible to all users. This approach works best when certain document types can be grouped well with certain users.

One benefit of this approach is that it respects the efficiency and productivity gains afforded by sharing and collaboration within the practice group, while mitigating the risks that result from general exposure. Trust & Estate and Tax, Insurance Defense, Product Liability, and/or Medical Malpractice, Healthcare, Securities and Mergers & Acquisitions practice groups are other potential candidates because, in many firms, such practice groups handle large amounts of especially sensitive information that can reasonably be restricted to practice group users.

Other possible hybrid approaches include securing documents by client or matter, creating separate open libraries for sanitized KM, creating separate legal and back office libraries, restricting back office staff (e.g., Billing, HR, and parts of IT) to only the back office library and finally, applying appropriate security only to documents considered to be sensitive (e.g., documents containing PHI, PII, or other client proprietary information).

It is worth noting that while all document repositories have some method of granting or restricting access to groups of documents, there are many tools available which can help automate this process, making it much easier either for the end user, or for the department charged with maintaining security.

Figure 1 below attempts to visually show how these options might look when mapped against the two dimensions of *How Secure* and *Ease of Access*. Note that while solutions towards the upper right-side of the graph are often more desirable, they might be more difficult to implement.

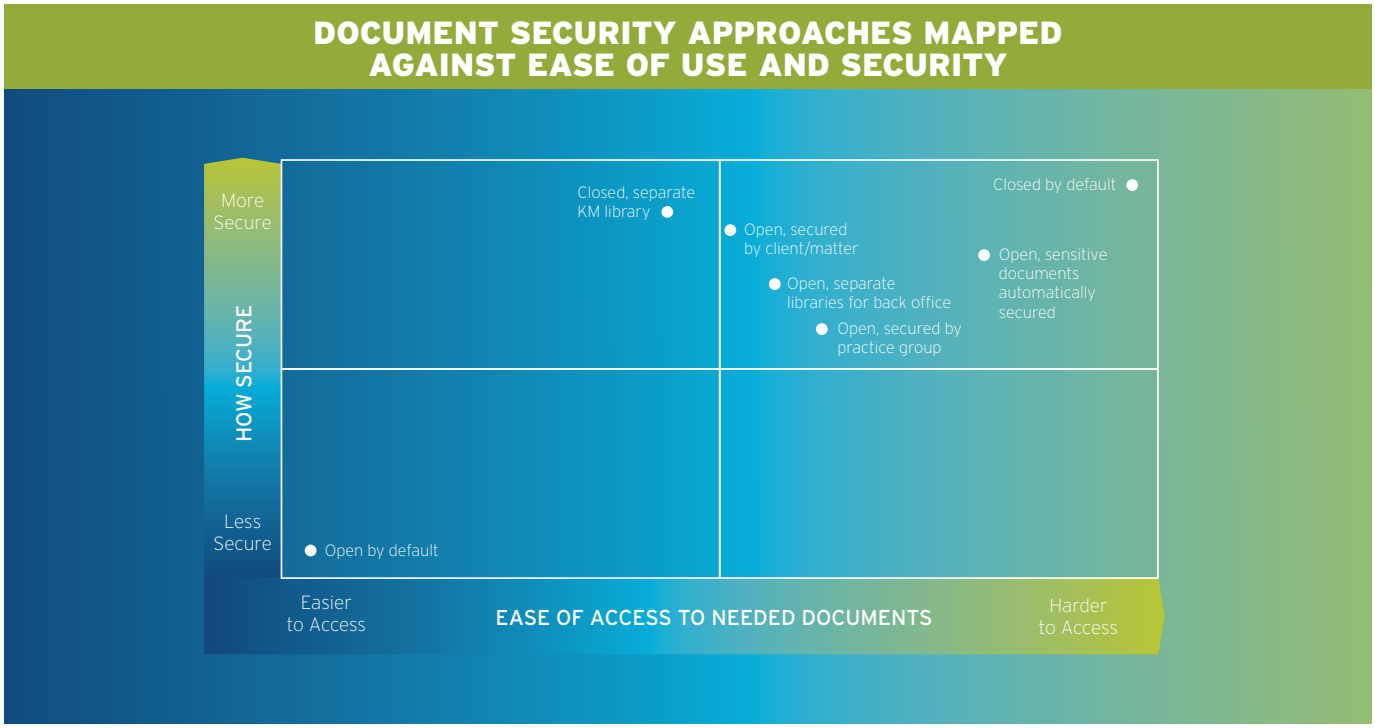

FIGURE 1

In addition to being able to effectively apply access restrictions technically, the two principle administrative challenges firms should anticipate when considering a hybrid approach are workflow automation, and managing exceptions to access policies. Information governance and new business intake stakeholders must collaborate to assign responsibility for reviewing incoming matters to ensure they are tagged appropriately. Ethical walls or OCGs may require that some matters within a secure practice group, jurisdiction, or office receive additional security. In these circumstances, the firm must override group policies with more granular controls. Many matters, moreover, may require work from attorneys in separate groups, so the firm should prepare to manage exceptions to hybrid rules that respect business requirements. Finally, firms should consider activity monitoring on the DMS, SharePoint, or file shares as a compensating control on information in practice areas they are not ready to lock down. Analyzed appropriately, system usage activity patterns can reveal anomalies that may signal a problem, so that the firm can gain some control over information use without impacting attorney and staff work habits.

PRACTICAL GUIDANCE

End users typically agree that security is important as long as it inconveniences someone else! Even when a major client mandates changes to restrict who can view their documents, people charged with making such changes should carefully consider what to change, and how to make those changes successful and sustainable. Below is practical guidance for moving to a more restrictive access security model.

1. Based on your firm culture, build a coalition within your firm to help guide decisions and champion the changes you are about to make. Typical candidates include KM, IT, IG, Ethics, HR and key practice groups.

2. Examine the makeup of your clients, your firm's culture, the size and complexity of your systems and your security requirements to determine if the firm should start with an open, closed or hybrid approach.

3. Determine which access control approach to use: centralized, distributed or mixed. Develop an efficient process to allow changes in document security using automation where appropriate. Consider applying security at matter inception, based on client, practice group or other requirement that makes sense for your firm.

4. Consider data classification when making your decision. Because data classification has two meanings, there are two items to consider. First, consider the type of data and information you are managing. Certain classes or categories of data require stricter security than others. The second consideration for data classification is more traditional to security, which requires sorting data into secret, top-secret, confidential and other classes which can then drive security designations and procedures. This may be based upon matter sensitivity and other factors.

5. Educate users on why the change in security is necessary, how to use the process to change document security and the consequences of circumventing the system.

6. Implement an audit function to monitor compliance with established policies and procedures.

7. If there is not enough support to overcome cultural resistance, look for quick-win opportunities based on client requirements, regulations or practice groups. Pick solutions that provide the best combination of securing documents, while maintaining ease of access for authorized users.

8. Track the types of exceptions that happen frequently and adjust your processes accordingly. Otherwise, revisit the effectiveness of processes at least annually, or when firm or client requirements dictate a potential change.

9. Consider technology such as encryption, secure email and/or data leak prevention to provide security beyond access rights.

10. Be prepared to change or create additional processes, such as sanitizing knowledge management, handling attorney departures or translating OCGs into security requirements to enable a successful change to more restrictive security.

11. Most firms will start with the DMS, but don't forget other information stores, such as file shares, SharePoint and even data stores external to the firm.

ADDRESSING DATA OUTSIDE OF THE FIRM

Material outside of the firm's firewalls requires a level of protection just as carefully planned as data inside the firm. The data found outside of the firm is often either the property of the client, or otherwise information that was sent to an outside party by one of the matter team members. Client property must be treated with great care, and its security should always be maintained. For example, if a member of the matter team takes a document to work on from home, that document should be expunged from any home equipment as soon as possible. The firm should make a concerted effort to stop the proliferation of client information.

The other challenge is to have policies in place governing dissemination of materials to any outside location. The policies applied to content in the DMS should also apply when the content is moved or copied to any of the locations listed below. This can be accomplished through software tools that ensure the corresponding policy travels with the content, or via (albeit with more difficulty) manual application. When content is taken home, travels on a laptop or moves to the listed areas, security set in the DMS must be maintained for true content security certification.

Collaboration sites: The firm should create a process to properly manage material before it's uploaded into a collaboration site (e.g., restricting access to the same groups defined in the DMS, enabling sharing or exporting only to those groups and only with the appropriate security, or completely disabling sharing and exporting, etc). Collaboration sites create a problem in that, while information is generally secure while in place (based on assignments made by the firm), many users tend to download information from such sites to work on it locally. It is very important to address collaboration sites in policy, training and through technology (where necessary) in order to ensure utmost confidentiality and unnecessary proliferation of information.

External storage sites (e.g., Google® Drive, Microsoft® OneDrive, Box®, Dropbox®, etc.): As a first step in addressing external storage sites, firms need to ensure that their information management policies include restrictions on posting internal materials to such sites, and to ensure that only secure FTP and firm-sanctioned collaboration sites are used. Should a firm allow access to such sites, they should still consider a security solution that will in some way encrypt the information so that confidentiality can still be maintained.

eDiscovery platforms: Similar to the above, firms need to ensure processes are in place to restrict access to a defined group.

Social media: Firms should maintain a social media policy for employees and vendors which restricts the posting of client and firm materials to any social media outlet or share space. The firm can also deploy monitoring tools to act as an alert of potential policy non-compliance. Again, appropriate encryption of information as well as matter security described within this document will help mitigate the risks of inadvertent posting by less-informed employees.

WHEN LAWYERS LEAVE

Attorney departures present a number of challenges to document security that can be met with a carefully designed process for managing them. Notification of an impending attorney departure should trigger at least these information management-related events:

- **Generating client/matter lists where the departing attorney has key designation (e.g., Originating/Billing/Responsible/Assigned Partner) and starting the process of either reassigning those roles to active attorneys, or closing those clients and/or matters to ensure unauthorized access, or additional work, does not occur.**
- **Identifying information in repositories of record (e.g., records inventory systems, document management systems) where a departing attorney may have checked out files or created private folders or documents and enacting a process for managing their disposition/resolution.**
- **Identifying information systems where a departing attorney may have non-network access (e.g., collaboration sites) and restricting that access appropriately.**

CASE STUDY/CONSIDERATIONS FOR IMPLEMENTING PRATICAL GUIDANCE

The following section provides real life examples from several firms who have grappled with moving from an open document repository to a more restrictive document repository. Most of the firms in these examples have technology and processes to set up and maintain ethical walls, and have extended (or are looking at extending) this technology to further restrict document access.

Example 1

A large, full-service international firm with nearly 1000 lawyers and approximately a dozen offices started to examine their document repositories due to client demands and restrictions unique to certain cases. While not all matters have restricted access, this firm does have a manual process for setting up restricted matters. They grant access based on timekeeper information from their billing system and an approved list of collaborators. This manual process can be handled by the Information Security Department, the Records Department or the Service Desk, however the firm reports they find the process challenging.

While the firm's work included collaboration sites and litigation support system access, which is closed by default, the biggest challenges came with the DMS. Like many large firms, their DMS libraries were centralized by region. Some international libraries were restricted to allow access only to that region. Other libraries were restricted so that only an approved subset of users outside the region could access the library. Additionally, the firm segmented their library databases for security purposes.

One particularly thorny issue for most firms considering this type of change is how to handle in-house support staff, such as word processing personnel, litigation support staff, secretary pools and similar groups. This firm started with a list of approximately 25 administrative staff members in the records and practice management groups who automatically have access to restricted matters. Others can be granted access upon request.

Once a matter is created, a user needing access must request such access from the Service Desk. The Service Desk follows a protocol to get approval from screening partners, who are identified when the restricted matter is established. There could be one or more screen lawyers per matter. Most requestors have approval in-hand by email when they start the process.

The firm is just starting to examine the impact on KM functions, such as enterprise search, experience management, contact management, precedent documents, document assembly and collections processes for specific practice areas.

Because this firm has a very clear and visible focus on information security, users have been generally understanding of the need to take these extra security steps.

Example 2

Another large, full-service international firm of similar size is utilizing a different approach, but with the same motivation: specific clients requesting that their matters have restricted access. The New Business Department plays the largest role in setting up a client or matter to be restricted by default, relying heavily on an automated tool to apply appropriate security to various document repositories. This same software handles changes to the security of a restricted matter based both on a user's record of billing time to a matter, or a self-declaration process. They also have a small team of administrative people who have access to these restricted matters. Because they are currently focused only on those matters where clients have required restricted access, education and cultural change has been fairly straightforward, requiring only an email notification. As the need for this kind of security expands, they are addressing other document repositories, such as shared drives and their records repositories.

Example 3

A third full-service international law firm of similar size has not yet made the move to systematically restrict matters. While they do have file shares, they are considering eliminating them and focusing their efforts on the DMS. They are just starting to discuss restricting access by default, and client demand is a definite consideration. Today, they have a process in place to restrict document access based on ethical wall requirements. The Conflicts Department manages inclusionary and exclusionary walls. Individual users control access to specific documents. The Technology Department creates user groups for departments that have specific access (i.e., the HR Department or the Management Committee). They also utilize technology to ensure that certain document types in the DMS automatically default to private (e.g., personal, personnel, firm business and PHI).

Example 4

A smaller, domestic firm of about 500 attorneys and 15 offices is also just starting down the path of examining several repositories, such as their DMS, shared drives, SharePoint, practice support site and the firm's intranet. They are being driven by both client demands as well as the requirements around PHI and PII. They have technology in place to automate ethical wall security, and would consider using similar technology. They are currently examining issues such as how to handle external repositories, how to change security during the life of the matter and the best way to handle supporting staff.

Example 5

One firm is researching changing the model from restricting matters, to keeping them unrestricted, but sending notifications when someone who does not work on a matter accesses it. The primary motive behind this process is that the notice itself will serve as a deterrent to unauthorized access. The firm leading the charge on this is looking at DLP and big data tools.

FUTURE CONSIDERATIONS

As the information governance model continues to advance and mature, technology will inevitably advance as well. Reliance on digital information will continue to expand, and with it, consistent growth in law firm work product and related custodial data. Technologies to assist with securing and controlling access to sensitive data will possibly focus on automated access control and information governance as a service (IGaaS) and will become more directly aligned with information security management. Additionally, collaboration amongst law firms and their regulated clients will further develop best practices for firms to strengthen data security within their environment.

AUTOMATED ACCESS CONTROL

As data collection sizes increase, expansion of the number of approved repositories and the requirement for security at a more granular level, will drive the need for more automation to assist with securing and governing information. There are tools available now to assist with security and access control when documents or workspaces are created, and the use of ethical wall-type software will automate some of the ongoing maintenance for restricting access to clients and matters. Possible next steps in the evolution of automated access control will be based upon integrated access or contextual-based access. Moving beyond controlling access based simply on client or matter, access will be controlled by integrating firm-wide information based from multiple sources. Information from HR, Billing and Timekeeping, and Records Management can be used to assign access to new and existing data. Contextual access would utilize indexes of data and metadata to automate data security based on file content. One might imagine using historic patterns of records creation, position within the firm, practice area and historic billing and timekeeping, coupled with content metrics, to automate access across all firm work product and hosted custodial data. The concept would apply beyond the DMS, and apply to all approved repositories – onsite and/or cloud-based. This would be a very powerful tool similar to the use of predictive coding or assisted review.

INFORMATION GOVERANCE AS A SERVICE (IGAAS)

Many small firms cannot afford the headcount or expertise to properly invoke a solid IG practice. As firms continue to become more reliant on cloud and SaaS offerings, outsourced and predictive cost services for the implementation of information governance will continue to gain popularity. The reliance on cloud-based data repositories will require solutions that allow for the governing of information that will be mixed between on-premise and cloud, lending itself to a SaaS model for tools, policies, administration and enforcement. Providers are beginning to emerge and provide a service that scales based upon firm or repository size. Providing predefined packages or services allows for more expertise in related areas of information governance such as data security, access control, perimeter security, standards/best practices and certifications. These services are so closely tied that choosing in-house staff versus outsourcing becomes a question of resource management and predictive cost.

CREATING INDUSTRY STANDARDS (E.G., ILTA'S LEGALSEC GROUP)

The International Legal Technology Association (ILTA), along with a number of its member firms, have been leading an effort with the financial services industry to strengthen online security. According to an article published in The New York Times, "For nearly a year, banks and law firms have discussed setting up a legal group that would be affiliated with the banking industry's main forum for sharing information about threats from hackers, online criminals, and even nation states – the Financial Services Information Sharing and Analysis Center." The article went on to say that the establishment of this group may happen by the end of 2015 due to the "recognition that hackers are increasingly focusing on big law firms to glean information about their corporate clients."[5]

CONCLUSION

In February, 2015, a large US health insurance company announced that as many as 80 million customers had their account information stolen, which included employment information and medical IDs.[6] Days later, it was reported that hackers stole $1 billion dollars from banks worldwide, infiltrating more than 100 institutions in 30 countries since at least the end of 2013.[7] As the threat of cyber-attacks continues to increase across the global economy, so too, will the client and regulatory demand for law firms to increase their data security, both from outside threats, as well as unnecessary internal access. As illustrated in this report, transitioning from an open system to a closed system requires careful planning and consideration, from determining how security will be applied to identifying which individuals or groups will be responsible for monitoring and maintaining proper data access across the matter lifecycle. It also involves appropriate training, communication and support from senior management to ensure compliance throughout the firm. While such an undertaking will likely prove challenging, it is one that many firms have found – and will find – essential to maintaining client relationships, and by extension, their own future sustainability.

APPENDIX A: GLOSSARY

TERM	DEFINITION
Business Associate	A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.[8]
BAA (Business Associate Agreements)	Business Associate Agreements (also known as Business Associate Contracts) are put in place when a person or entity is providing service to, or on behalf of, a covered entity. The agreements describe the permitted uses of protected health information by the business associate provided that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract and requires the business associate to use appropriate safeguards to prevent an unauthorized use or disclosure of the protected health information.[9]
Client Data	For purposes of this report, client data is not work product generated by the law firm, but rather, data that has been provided to the firm to assist the client on a given matter (e.g., data provided as part of the discovery process in a litigation matter).
Covered Entity	A covered entity is a health care provider, a health plan or a health care clearinghouse. Individuals, organizations, and agencies that meet the definition of a covered entity under HIPAA must comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information.[10]
DMS (Document Management System)	A DMS is software that controls and organizes documents throughout an organization. It incorporates document and content capture, workflow, document repositories, COLD/ERM, and output systems, and information retrieval systems. It is also the processes used to track, store and control documents.[11]
Encryption	Encryption is a method of converting data from standard text into encoded text by means of an algorithm to prevent anyone other than the receiving party who has the key to the encryption code from being able to decrypt (translate) the text.[12]
HIPAA	HIPAA is the acronym for the Health Insurance Portability and Accountability Act of 1996. HIPAA is a federal legislation that created national standards to protect the privacy of patients' medical records and other personal health information.

KM (Knowledge Management)	Knowledge Management is a system or process for capturing, distributing and effectively using information within an organization.[13]
NBI (New Business Intake)	New Business Intake is the defined process that firms undertake to initiate new clients and matters. It includes assessing risks and ensuring proper setup within the firm's systems.
OCGs (Outside Counsel Guidelines)	OCGs are the set of standards that clients use to define their engagement with outside law firms. OCGs often include terms that address billing, conflicts, data privacy and management, override provisions, and copyright and ownership of work product.[14]
Optimistic Security	Optimistic security is a design whereby all matters and documents are open, unless secured otherwise.
Pessimistic Security	Pessimistic security is a design where all matters and documents are secured and only opened to those who require access.
PHI (Protected Health Information)	PHI is individually identifiable health information, held or maintained by a covered entity or its business associates acting for the covered entity, that is transmitted or maintained in any form or medium (including the individually identifiable health information of non-US citizens). This includes identifiable demographic and other information relating to the past, present, or future physical or mental health or condition of an individual, or the provision or payment of health care to an individual that is created or received by a health care provider, health plan, employer, or health care clearinghouse.[15]
PII (Personally Identifiable Information)	PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.[16]

REFERENCES

1 State of New York. (2014, December 10). *NYDFS Issues Examination Guidance to Banks Outlining New Targeted Cyber Security Preparedness Assessments*. Retrieved from http://www.dfs.ny.gov/about/press/pr1412101.htm

2 US Department of State. (2009). *Directorate of Defense Trade Controls* (Policy). Retrieved from http://pmddtc.state.gov/

3 It should be noted that maintaining KM at a law firm is a discipline, and this is not intended to be a solution template, but rather points to consider.

4 "Optimistic" and "pessimistic" are also terms used by Hewlett-Packard® iManage, Microsoft® and others to describe how multiple access rights are interpreted when in conflict. Other systems refer to these concepts as "non-restrictive" or "restrictive" security. For example, an optimistic security model allows the least restrictive access rights to take precedent, while pessimistic allows the most restrictive rights to take precedent.

5 Goldstein, M. (2015, February 23). *Wall St. and Law Firms Plan Cooperative Body to Bolster Online Security*. Retrieved from http://www.nytimes.com/2015/02/24/business/dealbook/wall-st-and-law-firms-weigh-cooperation-on-cybersecurity.html?_r=1

6 Weise, E. (2015, February 5). *Massive Breach at Health Care Company Anthem Inc*. Retrieved from http://www.usatoday.com/story/tech/2015/02/04/health-care-anthem-hacked/22900925/

7 The Associated Press. (2015, February 15). *Hackers Steal Up to $1 Billion From Banks, Security Co. Says*. Retrieved from http://www.nytimes.com/aponline/2015/02/15/us/ap-us-bank-hack-report.html?_r=0

8 US Department of Health and Human Services. (n.d.). *Health Information Privacy – Business Associates* (Policy). Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html

9 Ibid.

10 US Department of Health and Human Services. (n.d.). *Health Information Privacy – For Covered Entities and Business Associates* (Policy). Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/

11 Association for Information and Image Management (AIIM). (n.d.). *What Is Document Management (DMS)?* Retrieved from http://www.aiim.org/What-is-Document-Management

12 State of Delaware. (n.d.). *HIPAA FAQs*. Retrieved from http://dhss.delaware.gov/dhss/dph/morefaqshipaa.html

13 Koenig, M. E. D. (2012, May 4). *What is KM? Knowledge Management Explained*. Retrieved from http://www.kmworld.com/Articles/Editorial/What-Is-.../What-is-KM-Knowledge-Management-Explained-82405.aspx

14 Law Firm Information Governance Symposium. (2014, July). *Outside Counsel Guidelines Management: An Information Governance Issue*. Retrieved from http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/White-Papers-Briefs/E/Emerging-Trends-Task-Force-Report-Outside-Counsel-Guidelines-Management.aspx

15 National Institutes of Health. (n.d). *What Health Information Is Protected by the Privacy Rule?* Retrieved from http://privacyruleandresearch.nih.gov/pr_07.asp

16 US General Services Administration. (n.d.). *Rules and Policies - Protecting PII - Privacy Act*. Retrieved from http://www.gsa.gov/portal/content/104256

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organizations lower the costs, risks and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organizations around the world. Visit the company website at www.ironmountain.com for more information.

© 2015 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks of Iron Mountain Incorporated in the U.S. and other countries. All other trademarks are the property of their respective owners.

US-LAW-EXT-BR-081015-001