Consilio Institute: Practice Guide

AN OUNCE OF PREVENTION: FUNDAMENTALS OF DATA PROTECTION

Jonathan Fowler
Chief Information Security Officer

Matthew Verga
Director of Education

Consilio / ADVANCED LEARNING INSTITUTE

Consilio / ADVANCED LEARNING INSTITUTE

Consilio Institute: Practice Guide

AN OUNCE OF PREVENTION: FUNDAMENTALS OF DATA PROTECTION

CONTENTS

Consilio / ADVANCED LEARNING INSTITUTE

AN OUNCE OF PREVENTION: FUNDAMENTALS OF DATA PROTECTION

Introduction

It is axiomatic that the volumes of electronically-stored information (ESI) generated by organizations are vast and ever-increasing. Correspondingly, the amount of ESI that must be preserved, collected, processed, and reviewed for internal investigations, active litigation, and regulatory compliance never stops growing. Today, it is a practical and ethical requirement for practitioners in these areas to take the necessary steps to protect the ESI they are managing for those purposes, which means keeping up with evolving security and compliance best practices – as well as adapting to the rapidly changing tactics to threat actors.

In this practice guide, we will discuss why ESI must be protected and how you can protect it, including fundamentals of security compliance frameworks, role-based access control, cloud storage vs. on-premises storage, and data encryption.

Why ESI Must Be Protected

So, why is data protection something lawyers and other legal practitioners need to know? Isn't that IT's job? The short answer is that data protection is everyone's job, and the long answer is that data protection in the legal industry is critical both because of lawyers' ethical duties and because of the potential consequences of a breach into such sensitive data.

Lawyers' Ethical Duties

In August 2012, the American Bar Association (ABA) implemented changes[1] to its Model Rules of Professional Conduct, including a change to make the need for technology competence explicit. In the eleven years since the change to the Model was implemented, forty states have adopted some form of this technology competence requirement for lawyers.[2] Although this change was spurred in large part by the rapid rise of eDiscovery, it is not limited to just that area.[3] It encompasses technology competence in several contexts, including "safeguarding client information" and "the technology that lawyers use to run their practices."

In addition to the duty of technology competence, lawyers have an ethical duty to protect client confidentiality. For example, ABA Model Rule of Professional Conduct 1.6(c)[4] says that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." The ABA has elaborated on this duty in the contexts of cybersecurity and remote work:

[1]Debra Cassens Weiss, *Lawyers Have Duty to Stay Current on Technology's Risks and Benefits, New Model Ethics Comment Says*, ABA JOURNAL, http://www.abajournal.com/news/article/lawyers_have_duty_to_stay_current_on_technologys_risks_and_benefits/ (Aug. 6, 2012).
[2]Robert Ambrogi, *Tech Competence*, LAWSITES, https://www.lawsitesblog.com/tech-competence (last visited Dec. 20, 2023).
[3]Steven M. Puiszis, *Perspective: Technology Brings a New Definition of Competency*, BLOOMBERG LAW, https://news.bloomberglaw.com/business-and-practice/perspective-technology-brings-a-new-definition-of-competency (Apr. 12, 2016).
[4]ABA Model Rules of Prof'l Conduct R. 1.6 (2023), available at https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/.

- ABA Formal Opinion 477R[5] (2017) discusses lawyers' obligation to understand and use electronic security measures to safeguard client communications and information. The opinion discusses a range of best practices to employ, including: using strong, unique passwords; enabling multifactor authentication; securing Wi-Fi networks; updating software regularly; and enabling antivirus software and firewalls.
- ABA Formal Opinion 498[6] (2021) discusses lawyers' obligations to safeguard information when working remotely. The opinion discusses a range of best practices that overlaps with the recommendations from Formal Opinion 477R and adds some additional recommendations related to the use of encryption, virtual private networks (VPNs), data backups, breach policies, and more.

Potential Consequences Of A Breach

Beyond lawyers' ethical duties, there are also a range of potential consequences of data breach, loss, or exposure that range from embarrassing to costly to criminal. Any pool of ESI collected for discovery or investigation may contain not only privileged materials but also a wide range of other sensitive materials such as personally identifiable information (PII), personal health information (PHI), customer information, proprietary information, trade secrets, and even classified information.

Your organization may be obligated to protect such information by court rules, by contract, by federal and state law, and by international law. For example, in the U.S., disclosure of personally-identifiable medical information generally needs to be prevented to comply with the Privacy Rule of the Health Insurance Portability and Accountability Act (HIPPA).[7] When dealing with ESI in the EU, disclosure of personally-identifiable information may need to be prevented to comply with the General Data Protection Regulation (GDPR).[8]

Failing to prevent a data breach or other inadvertent disclosure can obviously result in privilege waiver, but it can also create an obligation to report the breach to regulators and individuals, result in a loss of trade secret status, or cause significant reputational damage – and, of course, investigating and remediating the issue is also likely to be expensive and time-consuming.

How To Protect ESI

In order to reduce the potential for those negative outcomes, legal and compliance practitioners responsible for managing ESI need to understand the fundamentals of security compliance frameworks, role-based access control, cloud storage vs. on-premises storage, data encryption, and adaptation to evolving adversarial tactics.

Security Compliance Frameworks: ISO, SOC2, and NIST

Security compliance frameworks play a crucial role in ensuring the protection of data and the security of eDiscovery processes, and selecting service providers that adhere to them will help ensure the protection of the ESI you are managing. There are three notable frameworks that are often applied in the legal industry: ISO 27001, SOC2, and NIST SP 800-53.

1. ISO 27001/27002 (International Organization for Standardization)

   ISO 27001/27002 are internationally recognized standards for information security management systems (ISMS). In the eDiscovery industry, compliance with ISO 27001/27002 demonstrates a systematic approach to managing sensitive information, reducing

[5]"ABA Formal Opinion 477R: Securing communication of protected client information," American Bar Association (June 2017), available at https://www.americanbar.org/news/abanews/publications/youraba/2017/june-2017/aba-formal-opinion-477r--securing-communication-of-protected-cli/
[6]"ABA issues guidance on model rules, ethical tech duties to consider when working remotely," American Bar Association (Mar. 10, 2023), available at https://www.americanbar.org/news/abanews/aba-news-archives/2021/03/aba-issues-guidance-on-model-rules--ethical-tech-duties-to-consi/.
[7]U.S. Dep't of Health & Hum. Servs., Summary of the HIPAA Privacy Rule, HHS.gov, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (July 26, 2013).
[8]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 59, 1 (May 4, 2016), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434.

risks, and ensuring data security. While ISO 27001 defines the standards an organizations are required to meet, 27002 offers a comprehensive set of controls that include policies, procedures, technical measures, and employee training. eDiscovery providers that adhere to ISO 27001/27002 standards are indicating a commitment to safeguarding client data that includes support from the top of the organization down.

2. SOC2 (Service Organization Control)

   SOC2 is a set of auditing standards developed by the American Institute of CPAs (AICPA) for service organizations. It focuses on security, availability, processing integrity, confidentiality, and privacy. In the eDiscovery context, SOC2 compliance is particularly relevant as it assesses the effectiveness of an organization's controls over data security and privacy. When reviewing a provider's overall security program, it is important to identify whether they have obtained a SOC2 Type 1 or SOC2 Type 2 certification. Type 1 certification means that the security controls the provider has in place were reviewed at a single point in time, while the more common Type 2 certification shows that the effectiveness of those security controls were assessed over a period of time. eDiscovery providers that obtain SOC2 compliance demonstrate their commitment to meeting high standards of security and privacy.

3. NIST SP 800-53 (National Institute of Standards and Technology)

   NIST SP 800-53 is a comprehensive framework that provides a catalog of security controls for U.S. Federal Government information systems and organizations. While originally developed for the U.S. government, it has been widely adopted in the private sector, particularly among those organizations that provide software and/or services to the Federal Government. The Federal Risk and Authorization Management Program, more commonly known as FedRAMP, draws its security controls directly from this publication, and service providers who wish to handle sensitive data should be knowledgeable of them.

Role-Based Access Control

Role-Based Access Control (RBAC) is a fundamental principle of data protection in the eDiscovery industry. It is a security model that restricts system access to authorized users based on their job-specific roles within the organization. RBAC ensures that individuals only have access to the data and resources necessary for them to perform their job functions. This not only enhances security but more importantly helps maintain the "principle of least privilege," which reduces the risk of data breaches by ensuring users only have access to the ESI and resources they need to complete their required tasks.

In eDiscovery, RBAC is essential for controlling access to sensitive legal and case-related information. Different personnel, such as lawyers, paralegals, IT administrators, and external counsel, should have distinct roles with corresponding access permissions. For example, a lawyer might have full access to case files and legal documents, while an IT administrator may only have access to system configuration settings. Implementing RBAC helps organizations adhere to data protection and privacy regulations, like the GDPR in Europe and HIPAA in the United States.

Data Storage: Cloud Vs. On-Premises

Most of the data implicated in eDiscovery or compliance activities is highly sensitive in nature. The choice of whether to store that data on-premises (often in a data center) or to allow that data to be stored in the cloud is a critical decision with significant implications for data protection and security, both when considering your own organization's storage and when considering the storage used by any legal services providers with whom you work.

- Cloud Storage

  Public cloud providers like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud have become increasingly popular options in which to store massive amounts of data. Data storage in the cloud offers numerous advantages, such as massive scalability for large-scale datasets and an ease of accessibility, as the data can be accessed from any device that is connected to the Internet. However, data protection in the cloud must be approached with care. Legal practitioners should evaluate the security controls in place with cloud-based data storage providers, in particular with respect to access management controls to ensure that the data is only available to those who should have access. There have been multiple instances of cloud data repositories being accessible to the world due to misconfigurations in their access management settings. Additional considerations include encryption of data in transit to get to the cloud storage repository and the potential access by storage administrators from the cloud storage provider.

- On-Premises Storage

  On-premises data storage provides organizations with a greater amount of control over their data, including knowing exactly where their data is physically located and where it is is backed up. This approach is ideal for organizations with specific regulatory requirements or heightened security requirements, as it allows for full control of the environment in which sensitive data will be used. Additionally, where certain types of projects require special or additional security controls to be applied, having full control of the environment provides the ability for a more granular approach to security.

Hybrid approaches, combining the benefits of cloud and on-premises storage, have gained popularity in the eDiscovery industry. This allows organizations to maintain sensitive data on-premises while using the cloud for backup, collaboration, and data processing. Ultimately, the choice between cloud and on-premises storage should align with an organization's specific security, compliance, and operational requirements.

Data Encryption

Data encryption is a cornerstone of data protection, not only in the eDiscovery industry, but globally. It ensures that sensitive information remains confidential and secure, even in the event of unauthorized access. There are two contexts in which the encryption of your ESI must be considered: encryption at rest and encryption in transit.

- Encryption at Rest

  - Encryption at rest protects data stored on physical and digital media, such as hard drives, servers, and databases. In the context of eDiscovery, this means that case files, legal documents, and client data should be stored in an encrypted format. The encryption keys should be securely managed and stored separately from the data to prevent unauthorized decryption.
  - Common encryption techniques for data at rest include full disk encryption (FDE) and file-level encryption. Many eDiscovery providers rely on industry-standard encryption algorithms like AES (Advanced Encryption Standard) to protect their stored data. Additionally, organizations may opt for hardware security modules (HSMs) included as part of large storage arrays to enhance the security of encryption key management.

- Encryption in Transit
  - Encryption in transit ensures that data remains secure while it is being transmitted over networks, including the internet. Legal practitioners and eDiscovery providers often exchange sensitive information with clients, partners, and regulatory bodies. Therefore, it is essential to use secure communication protocols such as SSL/TLS to encrypt data during transmission. Secure email and file transfer solutions are also commonly employed in eDiscovery to protect the confidentiality of messages and attachments.
  - The integration of end-to-end encryption (E2EE) can add an extra layer of protection, ensuring that only the intended recipients can decrypt and access the data. E2EE is particularly crucial when transmitting highly sensitive legal documents and case-related information.

Adapting To Ransomware Threats

The legal industry is certainly not immune to the evolving landscape of ransomware threats. In recent years, cybercriminals have increasingly targeted organizations across all sectors, including law firms and eDiscovery providers, with ransomware attacks. These attacks can have severe consequences, including data breaches, data loss, legal liabilities, and significant financial losses.

To defend against ransomware threats, organizations must establish robust security programs that continually evolve to match changing adversarial tactics. Here are some key strategies for mitigating ransomware risks:

1. Regular Backup and Recovery Procedures

   Regularly back up critical data and test the restoration process to ensure it is effective. Backup data should be stored in a secure and isolated location, away from the primary network, to prevent ransomware attacks from compromising the backups.

2. Employee Training and Awareness

   Invest in cybersecurity training and awareness programs for employees to help them recognize phishing attempts and other social engineering tactics commonly used by ransomware attackers. A well-informed workforce is a critical defense against these threats.

3. Network Segmentation

   Implement network segmentation to isolate critical systems and data from less sensitive areas of the network. If a ransomware attack occurs, this can help contain the impact and prevent lateral movement within the network.

4. Patch Management

   Maintain up-to-date software and systems with the latest security patches. Many ransomware attacks exploit known vulnerabilities in outdated software.

5. Advanced Endpoint Detection and Response (EDR) Solutions

   Deploy EDR solutions that can detect and respond to unusual or suspicious activity on endpoints. These solutions can help identify and halt ransomware attacks in progress.

6. Threat Intelligence Sharing

   Participate in threat intelligence sharing communities, such as the Legal Services Information Sharing and Analysis Organization (LS-ISAO), and share information about emerging threats. Collaborating with industry peers and security organizations can provide

valuable insights into the latest tactics used by ransomware actors.

7. Incident Response Plans

   Develop and regularly update incident response plans to facilitate a coordinated and effective response in the event of a ransomware attack. This includes procedures for containment, eradication, and recovery.

Conclusion

For legal practitioners, a commitment to data protection is a matter of ethical duty, of legal and regulatory compliance, and of fundamental responsibility to clients and stakeholders. As the digital landscape continues to evolve, staying ahead of security challenges and mitigating risks must remain a top priority for all legal and compliance professionals. Doing so requires consideration of security compliance frameworks, role-based access control, cloud storage vs. on-premises storage, and data encryption.

KEY TAKEAWAYS

There are six key takeaways from this practice guide to remember:

1. Data protection is the job of everyone within an organization, and data protection in the legal industry is critical both because of lawyers' ethical duties and because of the potential consequences of a breach into sensitive data.
2. Security compliance frameworks like ISO 27001, SOC2, and NIST SP 800-53 provide a structured approach to safeguarding data and ensuring compliance with industry standards.
3. Role-Based Access Control (RBAC) is essential for maintaining a secure environment by limiting access to authorized personnel.
4. The choice between cloud storage and on-premises storage requires a careful assessment of an organization's specific security and operational needs.
5. Data encryption, both at rest and in transit, is a critical component of data protection, ensuring the confidentiality and integrity of sensitive information.
6. In the face of evolving ransomware threats, practitioners and providers must employ robust security programs that can adapt to changing adversarial tactics, including regular backups, employee training, network segmentation, patch management, and the use of advanced endpoint detection and response solutions.

ABOUT THE AUTHOR

Jonathan Fowler currently serves as Vice President and CISO for Consilio. He is a Subject Matter Expert (SME) in the fields of Electronic Discovery and Digital Forensics and advises clients on all aspects of the Electronic Discovery Reference Model (EDRM) from effective information governance strategies through document production and presentation. He previously headed up Consilio's global Digital Forensics team, overseeing all data preservation, collection, and fo rensic examination operations, including the allocation of human and technology resources at the matter level, also serving as the driving force behind the growth and strategic direction of the department. He has experience as an expert witness in Computer Forensics in both Federal and state courts, and has also prepared multiple expert reports, affidavits, and statements of fact for various clients.

Additionally, Jonathan serves as Adjunct Professor in the graduate program in Computer Forensics at George Mason University, teaching courses in Windows Registry Forensics, as well as the capstone Advanced Computer Forensics course.

Jonathan Fowler

Chief Information Security Officer

m +1.202.899.2881

e jon.fowler@consilio.com

consilio.com

ABOUT THE AUTHOR

Matthew Verga is an attorney, consultant, and eDiscovery expert proficient at leveraging his legal experience, his technical knowledge, and his communication skills to make complex eDiscovery topics accessible to diverse audiences. A sixteen-year industry veteran, Matthew has worked across every phase of the EDRM and at every level, from the project trenches to enterprise program design. As Director of Education for Consilio, he leverages this background to produce engaging educational content to empower practitioners at all levels with knowledge they can use to improve their projects, their careers, and their organizations.

Matthew Verga

Director of Education

m +1.704.582.2192

e matthew.verga@consilio.com

consilio.com