CAN MY FIRM'S OFFICE SOLUTIONS MEET TODAY'S PRIVACY REQUIREMENTS?

Canon
SEE IMPOSSIBLE

The preservation of client confidentiality and the legal profession have always been synonymous. National and international legislation have heightened security awareness and expectations in priority areas for law firms, such as medical records, Personally Identifiable Information (PII), intellectual property, and prospectuses. Recent headlines from the BBC and other media outlets about alleged high-profile security breaches at law firms[1] highlight the need for IT administrators and senior partners to have technology in their offices that can help them protect client data.

Can your office solutions assist you with your compliance efforts? Here's a fast Q&A to help you identify areas where your firm can make changes to help improve workflow security:

Q: DO YOUR FIRM'S CONTENT WORKFLOWS AND ASSOCIATED SOLUTIONS ALIGN WITH YOUR HIPAA OMNIBUS AND GDPR COMPLIANCE STRATEGY?

A: HIPAA, the Health Insurance Portability and Accountability Act of 1996, underwent rule changes in 2013[2] broadening the law's application to attorneys in some cases. Law firms with access to protected health information (PHI) may be classified as business associates, so it is important that they implement processes to ensure the security and protection of the PHI they possess and transmit. PHI includes Social Security numbers, medical records, insurance information, and other data law firms may collect in the course of their practices.

Those law firms collecting or storing personal data of European Union (EU) citizens or individuals located in EU nations should also familiarize themselves with their compliance with the General Data Protection Regulation (GDPR).[3] A U.S. law firm may be subject to GDPR regulatory action, including fines, for failure to comply with applicable regulations.

Firms should investigate whether their content workflows and associated solutions are aligned with their HIPAA and GDPR compliance strategies. Consider a secure ecosystem that authenticates and allows document access based on assigned roles and associated privileges that align with the characteristics of the content.

[1] BBC, *Paradise Papers: Everything You Need to Know About the Leak*, Nov. 10, 2017
[2] HHS.gov, "HIPAA Guidance Materials"
[3] EUGDPR.org, "Controversial Topics"

Q: DO CLIENTS HAVE A SECURE WAY TO SEND AND RETRIEVE DOCUMENTS TO AND FROM US?

A: A single data breach in the U.S. is estimated to cost an average of $7.35 million in 2017, according to The Ponemon Institute.[4] The data lost in a breach can be enormous. News reports about one alleged security breach that has been called the "Panama Papers" claim that 11.5 million documents affecting 214,000 organizations and individuals may have been compromised.[5]

Even as data breaches make news, there's no denying that technology has increased the level of service clients expect from their attorneys. This includes the ability to use file sharing or content collaboration platforms securely. It is up to IT administrators to implement a process to give clients the access they want while preserving the security of the data and the system in place to help protect it.

Consider investing in or enhancing your existing workflow systems to solutions that can help seamlessly bridge content integration points and offer advance security capabilities that will align with your firm's security and compliance policies. Such technology can offer users the ability to securely access documents within or outside the firm. Also consider solutions that offer integrated authentication and discrete content controls that are specific to a particular document, file, or client.

Q: WOULD I BE ABLE TO SUPPLY INFORMATION ABOUT DOCUMENT ACCESS AND HANDLING DURING A CYBERSECURITY AUDIT OR A POST-BREACH AUDIT?

A: Concerns about the impact of a data breach are expected to cost businesses and organizations in the U.S. upwards of $2 billion in 2017 on premiums for cyber liability insurance policies helping to cover them in the event of a security breach.[6] A workflow system that allows administrators to digitize hard-copy content can provide tools to track document access, and it can help firms comply with security audits that may be required by the insurance companies and with the recordkeeping that may be required by HIPAA and GDPR.

Tight integration of a secure document ecosystem can permit administrators to quickly access login information, device activities, document tracking, and more. This information can be instrumental in helping with routine audits and workflow mapping for gap analysis, and it can assist with post-breach remediation efforts.

[4] Ponemon Institute, *2017 Cost of Data Breach Study*, June 2017
[5] BBC, "Panama Papers Q&A: What is the Scandal About?", Apr. 6, 2016
[6] Washington Post, "Cyber-insurance Becomes Popular Among Smaller, Mid-size Businesses", Oct. 12, 2014

Q: ARE THERE PLACES WHERE I CAN IMPROVE ON SECURITY GAPS IN CLIENT DATA PROTECTION?

A: Law firms and offices of all types can struggle with some common security gaps, including:

- Frequently leaving out papers and documents at printers, fax machines, and other devices without an authorized person present to retrieve them.
- Utilizing a secure content management solution to centralize data storage.
- Preventing individuals from purchasing and using devices that don't align with the firm's security and compliance policies.

Evaluate your current document workflows for their ability to provide comprehensive control and oversight throughout the entire chain of custody. Consider enhancements that prioritize integrated content security features.

Government regulatory agencies are increasing efforts with respect to the security of the personal data that law firms possess. Clients expect that documents and data entrusted to their attorneys will remain private and secure. So, it is up to firms to employ a holistic approach to their integrated document management strategies and the supporting workflow solutions to better align systems with firm security and compliance policies.

Learn how CANON can help provide security surrounding your document management.

Canon SEE IMPOSSIBLE