`

STATE BAR OF WISCONSIN
PINNACLE
Your Practice. Our Purpose.

WSSFC 2024

Technology Track – Session 2

Securely Sharing Documents

Presenters:
Nerino J. Petro, Jr., NerinoPetro LLC, Rockford, IL
Bryan Sims, Sims Law Firm, Ltd., Naperville, IL

About the Presenters...

Nerino Petro (IL & WI) is President of the Erickson Group of companies in Rockford, IL and previously the Chief Information Officer for HolmstromKennedyPC. He served as the first Practice Management Advisor for the State Bar of Wisconsin's Practice411™ Law Office Management Assistance Program from 2006-2014. Licensed in Illinois and Wisconsin, Nerino uses his years of legal practice and experience being CEO/Senior Legal Technologist for CenCom Legal Technologies, to help lawyers and their staff deal with the technology and practice management issues confronting them. He has worked with numerous leading products including TimeMatters, NetDocuments, TABS® time, billing and accounting software, Practice Master® practice management software, and many others. Nerino was the ABA LPM Magazine Product Watch columnist through 2012 and is a regular contributor to other local, state, and national publications including the Illinois Bar Journal, Wisconsin Lawyer, Wisconsin InsideTrack and ABA GP|Solo Magazine. He has presented throughout the US and abroad and has served on the ABA TECHSHOW Planning Board from 2012-2014 and is serving again for the 2018 ABA TECHSHOW. He was the 2019 Chair for the State Bar of Wisconsin Solo & Small Firm Conference Planning Committee and is a longstanding co-chair of its Technology Track. Nerino was named to the inaugural Fastcase 50 list of the top legal techies in 2011. Nerino continues to provide technology consulting, training and practice management services to lawyers and firms throughout the United States through CenCom Technologies.

Bryan Sims is a shareholder and founder of Sims Law Firm, Ltd., where he concentrates his practice in the areas of commercial litigation, civil appeals, and real estate matters. He's a member of the Illinois Bar and the Northern District of Illinois Trial Bar and is also admitted to practice before the United States Supreme Court, the United State Court of Appeals for the Seventh Circuit, the United States courts in the Central District of Illinois, the Southern District of Illinois, and the Eastern District of Michigan. Bryan is a member of the Illinois State Bar Association, the American Bar Association, the DuPage County Bar Association, and the Will County Bar Association as well as a member of the ISBA Standing Committee on Legal Technology, where he has previously served as the chair three times and the newsletter editor for 5 years. Since 2006, he has been a member ISBA Solo and Small Firm Conference Planning Committee. He is a past chair of the DuPage County Bar Association Law Practice Management and Technology Committee. Bryan has spoken on legal technology issues at the ISBA Solo and Small Firm Conferences, Wisconsin Solo and Small Firm Conferences, for the DuPage County Bar Association, the Chicago Bar Association, the Winnebago County Bar Association, the Lake County (Indiana) Bar Association, the Lake County (Illinois) Bar Association, the International Technology Law Association, National Business Institute and at ABA Techshow. Also, he was the featured speaker at the 2014 Oklahoma Solo and Small Firm Conference. Bryan has contributed to TechnoLawyer and was recognized as the 2005 TechnoLawyer of the Year. He has also written for PDA JD and regularly wrote reviews for Law Office Computing. Bryan blogs about the intersection between law and technology at www.theconnectedlawyer.com. Before entering private practice, Bryan worked as a judicial law clerk for Illinois Supreme Court Justice S. Louis Rathje. He has also worked as a staff attorney for the Second District of the Illinois Appellate Court. He is a 1993 Cum Laude graduate of Wheeling University and a 1996 Magna Cum Laude graduate of Loyola University Chicago School of Law. While in law school, Bryan served on the staff of both the Loyola Law Journal and the Loyola Consumer Law Reporter.

Securely Sharing Documents

2024 Wisconsin Solo & Small Firm Conference
October 17 – 19, 2024
Kalahari Resort,
Wisconsin Dells, WI

Presented by:

Nerino J. Petro, Jr.
Bryan M. Sims

Artificial Intelligence Disclosure

These continuing legal education materials were proudly brought to you with a little help from artificial intelligence (AI). Yes, the same technology that can predict the weather, recommend your next binge-watch, and maybe someday argue in court (we are not there yet!). While AI may have helped with drafting, modifying, or offering its two cents, rest assured that the final document was carefully reviewed, redrafted, approved, and lawyered-up by an actual human with a law degree. So, if you find any brilliance, we will take credit; if you find any glitches, well… let's just say the robots are still learning!

Introduction:

Protecting your confidential and privileged information is critically important 1n your firm. Whether you are handling contracts, litigation matters, family law matters or estate planning documents, sharing information and documents securely is a crucial responsibility for you and your staff. But you also need to navigate these complex security concerns when sharing documents while maintaining efficiency in your office. These materials will provide you with information to help you establish your best practices for securely sharing documents in today's digital world, while adhering to the Wisconsin Rules of Professional Conduct ("SCR").

1. The Importance of Secure Document Sharing in Your Law Practice.

One of the core concepts of any successful (and ethical) legal practice is the protection of client confidentiality and information. Sharing sensitive files and information without properly safeguarding that information can lead to significant legal, ethical, and even financial repercussions. Given the sensitive nature of the data you maintain in your files such as social security numbers, bank details, litigation strategies, and privileged communications, lawyers and their firms are increasingly being targeted by cybercriminals.

Wisconsin lawyers, and their firms, are bound by SCR 20:1.6, which mandates that you take reasonable steps to ensure confidentiality when sharing client information, including the requirement that you use the technology in your practice responsibly and securely. A core principle of this Rule is its prohibition against revealing information related to the representation of your client unless the client provides informed consent. Bottom line - you and your staff need to make sure that all documents shared electronically are protected with security measures such as encryption, passwords or sent by secure download.

Failing to protect this information can result in a data breach, leading to severe consequences, such as lost client trust, reputational damage, malpractice claims, and disciplinary action by OLR.

2. Key Threats to Document Security

External attacks by bad actors are not the only threat; internal mishaps can be just as dangerous. Accidentally sending an email to the wrong recipient or leaving confidential files exposed on an insecure network can also result in data breaches. Email interception, another common risk, can compromise sensitive information if the information is not properly encrypted. In the world of TLA (Three Letter Acronyms), this is known as Business Email Compromise ("BEC") and has many forms. One form of BEC is the Attorney Impersonation: A bad actor impersonates a lawyer and takes advantage of low-level staff at the recipient office counting on the fact that the staff will comply with the request because it is a "lawyer" sending the email. We have seen a rise in Attorney Impersonation over the last several years including the rash of bogus wiring instruction emails sent to title companies. These emails direct the title company to wire the funds to an account that the bad actor controls. The funds are rapidly transferred out of the country and unrecoverable. Another example of BEC is Executive Phishing or CEO Impersonation, where the bad actor is able to direct Accounting or HR to send a payment or confidential information to an outside recipient. To learn more, check out: See **How Business Email Compromise Works** https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-email-security/business-email-compromise-bec/ ; **CEO Fraud Attacks** https://www.knowbe4.com/ceo-fraud ; **What is Business Email Compromise?** https://www.cisco.com/site/us/en/learn/topics/security/what-is-business-email-compromise-bec.html

Once again, SCR 20:1.6(d) comes back into the picture: specifically, Rule 1.6 requires you to make reasonable efforts to prevent unauthorized access to or disclosure of client information. This makes using secure communication methods essential to mitigate these risks. Lawyers should also be mindful of SCR 20:5.1 and SCR 20:5.3, which require partners and supervisors to ensure that non-lawyers and third-party services, such as AI tools or file-sharing platforms, comply with confidentiality and other privacy laws or regulations such as the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requirements.

3. Best Practices for Secure Document Sharing

a. Encryption

Encryption should serve as the foundation of securing your information. According to Google Cloud's post **What is encryption?** https://bit.ly/4esUWOU

> *Encryption is used to protect data from being stolen, changed, or compromised and works by scrambling data into a secret code that can only be unlocked with a unique digital key.*

You may have heard terms like "encrypted in transit" or "encrypted at rest," but what do those terms really mean? According to **What is data at rest?** https://bit.ly/47HYIBl from CloudFlare:

> *Data at rest" is data currently in storage, typically on a computer's or server's hard disk. Data at rest contrasts with data in transit — also called data in motion — which is the state of data as it travels from one place to another. It also contrasts with data in use — data loaded into memory and actively in use by a software program.*

In simple terms, this means that all the computers in your office need to have full disk encryption enabled so that in the event your computers are stolen, bad actors cannot access any of the data. So how do you do this? The easiest way is to use tools that should already be part of your computer's operating system.

All your computers should have Microsoft BitLocker installed and turned on. This means that you must have the correct version of Windows 10 or 11 installed. For lawyers, BitLocker is only available in Windows 10 or 11 Pro and Enterprise versions – Windows 10 or 11 Home are not acceptable for law office use. If you are running Windows older than Windows 10, you are not meeting your ethical obligations as those operating systems are no longer updated or patched and pose security risks that you can mitigate buy updating to the latest version of Windows. In other words, if you are using one of those older operating systems and suffer a data breach, the safe harbor exception discussed later in this section, will most likely not apply.

While you can encrypt only the drives in your computer, you can also use BitLocker to encrypt external storage devices like portable drives and USB Flash drives. For Mac users, FileVault is Apple's native encryption product, much like BitLocker. To learn more about BitLocker, its requirements and how to set it up, check out JC Hernandez 's article **Essential Guide to BitLocker**

Encryption: Secure Your Data Today https://preyproject.com/blog/bitlocker . For FileVault, checkout Aya Masango's article on mackeeper **What is FileVault Disk Encryption on Mac and How to Use it** https://mackeeper.com/blog/filevault-disk-encryption-mac/

But do not forget about your portable devices such as smartphones, tablets, and portable storage. Modern smartphones and tablets have encryption capabilities, and you should be using it. Do an internet search to find out how to enable it and set it up. For example, if I want to know how to use encryption on my Samsung Galaxy phone, I will search "How do I encrypt my samsung galaxy phone" and for iOS "How do I encrypt my iphone."

If you are taking confidential or sensitive information out of the office on portable media, such as an external drive or USB Flash drive, then that media should also be encrypted. You can use Microsoft BitLocker for Windows devices and FileVault (or other built-in tools depending on the MacOS Version) for Mac. Many external storage devices also include a separate encryption program I if you do not have BitLocker of FileVault or want to use something simpler. Another option is to purchase external devices with a built-in keypad and encryption that is not dependent on your computer. Examples of these include the Kingston IronKey Vault Privacy 80 960GB External SSD (https://amzn.to/3BjgPRM) or the Apricorn Aegis Secure Key 3 NX 32GB 256-Bit Encrypted FIPS 140-2 Level 3 Validated Secure USB 3.0 Flash Drive (https://amzn.to/47LXc11). Note that these types of drive cost more than drives without keypads and built-in encryption, and their storage capacity is also lower, than a non-keypad storage device.

But why is the use of encryption so important? Most data breach laws, and SCR 20:1.6, recognize a "Safe Harbor" exception if you have made reasonable efforts to safeguard the information. Foley and Lardner, LLP created a downloadable PDF document **Safe Harbor Laws** https://bit.ly/4elBBPu that is a useful resource for questions on these types of laws.

If you are using cloud storage services such as Dropbox, Google Drive, Box.com and others, you need to make sure that your files are encrypted at rest and in transit and who has access to the encryption key. In other words, read the FAQ's (Frequently Asked Questions) and TOS (Terms of Service) for your service or those you may be considering. For example, the Security Information for ShareFile can be read at https://bit.ly/3TLYgvW . If they are not encrypted or your storage service does not offer it, then do an internet search on encryption tools for your storage service, such as "encryption software for Google Drive."

b. Two-Factor Authentication (2FA) aka Multifactor Authentication (MFA)

Layering security measures is also essential: 2FA adds an extra layer of security, requiring more than just a username and password to access the information. If you are not already using 2FA on your important business accounts, you need to start doing so right now. Yes, it adds a step to your login process; however, the added security is worth it. When you enable 2FA on your account, for anyone else to access your account, they must have not only your username and password, but they must also have your 2FA information as well. So how does 2FA work?

In addition to your username, 2FA usually requires at least two additional things: 1) *something you know* and 2) *something you have* or *something you are*. For Something you know, this is your username and password. For something you have, think an authorization code from an authenticator app, code sent SMS text to your phone, or a USB security dongle. For something you are, think a fingerprint or face scan. The more secure option is to use an authenticator app, if compatible with your service. For examples of authenticator apps, checkout **The Best Authenticator Apps for 2024** https://bit.ly/4dvkdqa , and **The Best Two-Factor Authentication App** https://nyti.ms/4eBIZWs. Popular authenticator apps include Google Authenticator, Microsoft Authenticator, Authy and Duo.

Microsoft 365, for example, integrates 2FA into its system, ensuring that sensitive emails remain secure even if login credentials are compromised.

c. Secure File-Sharing Platforms

Dedicated secure file-sharing platforms - in our opinion - are crucial for law firms. ShareFile, Egnyte, Box for Business, are just a few of the general business secure file sharing platforms. Many cloud based legal practice management systems such as Clio and MyCase, to name just two of them, include secure file sharing as part of their platforms, designed with robust security features including end-to-end encryption, client portals, and secure storage. These platforms generally provide audit trails, secure cloud storage, and may also include e-signature capabilities, which should be considered by lawyers handling sensitive documents.

d. Role-Based Access Control (RBAC)

You should also consider compartmentalizing information by implementing role-based access controls. This limits document access to only those who truly need it. For example, only your

accounting team and ownership should have access to your checking accounts and bookkeeping information, not general staff. This can help prevent unauthorized access, especially in firms where multiple parties may be working on the same case. There is an argument to be made that SCR 20:5.1, requires lawyers with supervisory roles must ensure these controls are in place to meet the firm's confidentiality and information protection requirements.

e. Client Portals vs. Email

While many clients prefer the familiarity of email, unless encrypted email is used, it is the least secure method of sending information. Client portals offer superior security by allowing law firms to securely manage and share documents, schedule meetings, and exchange sensitive information. While some clients find the process of using portals cumbersome, the trade-off is significantly enhanced security compared to email. This is where client education by you and your staff comes to the fore. You may even consider a pamphlet on why you use a client portal and how it works including a step-by-step guide.

4. Legal and Ethical Obligations

Lawyers have a stringent duty of confidentiality as outlined in SCR 20:1.6, requiring lawyers to protect client information from unauthorized disclosure. Encryption is strongly recommended to maintain confidentiality.

Under SCR 20:1.1, lawyers are also required to maintain competence, which includes staying abreast of technological changes. Comment [8] to this rule emphasizes that lawyers must understand the benefits and risks associated with relevant technology. As such, lawyers must be competent not only in legal matters but also in understanding how technology like AI, encryption and cloud-based services impact their duty to protect client data.

Compliance with data protection laws, such as Europe's General Data Protection Regulation (GDPR) https://bit.ly/3ZJ3tbN (you would be surprised how far this law reaches) and Wisconsin Privacy Laws https://bit.ly/4eZUveP , is also vital. These regulations impose severe penalties for failing to protect personal data. Bottom line is that you and your firm must stay up to date with security technologies to avoid falling behind and risking professional liability.

5. Tools for Secure Document Sharing**

So, what are examples of tools for securely sharing documents that can help lawyers meet their legal and ethical obligations?

Microsoft 365 (formerly Office 365) with Azure Information Protection (AIP): This platform provides built-in encryption, data loss prevention (DLP), and 2FA. In typical Microsoft fashion, it can be difficult to decipher what plan you need. While it may be tempting to go with the least expensive plan, most law firms (under 300 users) need to use Microsoft 365 Business Premium. Here is a link to an article, **Guide to the different types of Microsoft and Office 365 licenses** https://www.smartdeploy.com/blog/guide-to-office-365-licenses/ that explains the differences. For pricing information check out this Microsoft link: https://bit.ly/3N1yrEq.

ShareFile by Citrix: A comprehensive solution for business and legal professionals, ShareFile provides encrypted email, client portals, secure file storage, sending large files via email and e-signature functionality, making it a reliable choice for law firms. ShareFile recently dropped its minimum number of users from 5 to 3 and its prices a bit. For pricing and a feature comparison, check out: https://www.sharefile.com/plans-pricing .

Zix mail (NKA Webroot™ Advanced Email Encryption powered by Zix™): A US based email encryption provider that has been an industry leader for more than a decade. Zix allows you to share large files securely by email as well. To learn more, go to: https://zix.com/products/email-encryption

PreVeil: PreVeil provides email encryption and secure file storage and sharing for many industries as well as law firms. PreVeil provides powerful encryption for both emails and files, with features like secure file sharing based on zero trust security. Learn more at: https://www.preveil.com/

6. Electronic Signature

Electronic signature (e-signature or signature) allows you to securely share documents requiring signatures with your client or others and have them signed and delivered to all parties with little fuss. According to TechTarget's post **e-signature (electronic signature)** at https://bit.ly/3Bk4TPY :

An e-signature (electronic signature) is a digital version of a conventional handwritten signature. In many countries, including the United States, an e-signature can provide the same legal commitment as a handwritten signature if it meets certain criteria.

The terms e-signature and digital signature are often used interchangeably, although this is incorrect. A digital signature is a type of e-signature, but not all e-signatures are digital signatures.

An e-signature provides a quick and easy way to sign electronic documents without the need to print paper or affix wet ink signatures. Essentially, it is a process where computers are used to certify the integrity of a document and to authenticate the person signing the document (signer).

At the national level, e-signatures are governed by the Electronic Signatures in Global and National Commerce (ESIGN) Act and the Uniform Electronic Transactions Act (UETA). The ESIGN Act established electronic signatures being legal within the USA while UETA established the framework for the individual states to adopt their own electronic signature laws that can work in conjunction with the ESIGN Act.

Wisconsin 's UETA is found in Wisconsin Statute Section 137 (WI Stat § 137 (2023)). Under Section 137.16 (1) of the WI UETA, there are three requirements for an electronically signed document to fall within the purview of this Act:

- The document cannot be one of the prohibited document types under Section 137.12;
- The parties must agree to use electronic records; and
- The electronic record is capable of being retained when it is received.

Prohibited documents include Wills and Trusts, court orders, records in divorce, adoption or family law matters and any other document listed in this Section.

U.S. Guide to Electronic Signatures (link to downloadable PDF) https://bit.ly/4dooID2

Electronic Signature Laws by State https://bit.ly/4erN7Ji

Electronic Signatures: The Law is Catching Up https://bit.ly/3BzD71G

Popular e-signature services include Docusign www.docusign.com, SignNow www.signnow.com, ShareFile https://bit.ly/4ekcfkR, Adobe Acrobat Sign https://adobe.ly/3N3LeGt , and PandaDoc www.pandadoc.com. Check out TechRadar's **Best eSign software solution of 2024** post https://bit.ly/3Y2jFnm for other options and reviews.

7. Electronic Fax

Byran Sims, one of the presenters on this session, says, “Fax machines are EVIL!.” They are slow, inefficient and there are better ways to communicate today. Fax machines are definitely old technology and, except for lawyers and the medical profession it seems, faxing has fallen out of favor and major use everywhere else. Even in the legal profession, we thought the end of faxing was nigh, but alas that is not the case. With the rash of BEC (described earlier) where title companies were getting wiring instructions via email that were from bad actors, many banks and title companies have gone back to requiring a fax to confirm wiring instructions (although some are now accepting secure email delivery). But this does not mean you have to pull that old fax machine from storage or go out and buy one. Long before the demise of faxing, electronic or internet fax services were available and still are. These services allow you to send any document from your computer via fax to the recipient. When the someone sends you a fax to your fax number, the service converts it to a PDF, and it arrives in your email inbox. As with online storage services, encrypted email services and online portals, you need to review the TOS of the service and see if it is secure and meets your obligations. Generally, if an internet fax service is HIPAA compliant it will meet your needs. Examples of internet services include eFax (www.efax.com); iFax which claims to be HIPAA compliant (https://www.ifaxapp.com/); RingCentral (https://www.ringcentral.com) and others. For other options and reviews, check out **The Best Online Fax Services 2024** from PC Magazine at https://bit.ly/3XG6cAd and **Best Online Fax Services Of 2024** from Forbes at https://bit.ly/3Y2MzUn .

Conclusion

Secure document sharing is not optional in the legal profession—it is an ethical and legal necessity. By employing encryption, secure platforms, and multi-factor authentication, legal professionals can protect client data and confidentiality while maintaining efficiency. Staying ahead of technological threats is critical, and adopting best practices ensures compliance with both legal and ethical standards. Wisconsin lawyers must also adhere to the specific requirements of SCR 20:1.1, 20:1.6, 20:5.1, and 20:5.3, ensuring they protect client information, maintain competence in technology, and supervise the use of any third-party tools effectively.

Additional Resources

1. Five Risks and Benefits that Show Why Lawyers Should Adopt Microsoft 365 for Secure Client Document Management https://bit.ly/3N1I3PJ
2. 6 Step Guide to Secure File Sharing with Clients https://bit.ly/3ZJ7kph
3. What is email encryption? (CloudFlare) https://bit.ly/3BkEeCl
4. What is email encryption? (Microsoft) https://bit.ly/4elJKU4
5. Secure Email For Business: Email Encryption Best Practices https://bit.ly/4em15fo
6. Sharing Secure Legal Documents: Client Portals vs. Email Attachments https://bit.ly/4gGsCdc
7. The Best Email Encryption Services for 2024 https://bit.ly/4gLtSvu
8. What is an Electronic Signature? https://bit.ly/3zCVUZt
9. Electronic Signature: An Instant, Convenient And Green Way To Sign Documents https://bit.ly/3Y0FGTg