1-1-2022

Ethics_ How to Discuss Security with Your Clients

Indiana Continuing Legal Education Forum (ICLEF)

Ethics: How to Discuss Security with Your Clients
February 8, 2022
Index

Ethics: How to Discuss Security with Your Clients
February 8, 2022
Index

ICLEF Electronic Publications

Feature Release 4.1
August 2020

To get the most out of your *ICLEF Electronic Publication,* download this material to your PC and use Adobe Acrobat® to open the document. The most current version of the Adobe® software may be found and installed by clicking on one of the following links for either the free Adobe Acrobat Reader® or the full retail version of Adobe Acrobat®.

Feature list:

1. **Searchable** – All ICLEF Electronic Publications are word searchable. To begin your search, click on the "spyglass" icon at the top of the page while using the Adobe® software.
1. **Bookmarks** – Once the publication is opened using the Adobe Acrobat® software a list of bookmarks will be found in a column located on the left side of the page. Click on a bookmark to advance to that place in the document.
2. **Hypertext Links** – All of the hypertext links provided by our authors are active in the document. Simply click on them to navigate to the information.
3. **Book Index** – We are adding an INDEX at the beginning of each of our publications. The INDEX provides "jump links" to the portion of the publication you wish to review. Simply left click on a topic / listing within the INDEX page(s) to go to that topic within the materials. To return to the INDEX page either select the "INDEX" bookmark from the top left column or right-click with the mouse within the publication and select the words "*Previous View*" to return to the spot within the INDEX page where you began your search.

Please feel free to contact ICLEF with additional suggestions on ways we may further improve our electronic publications. Thank you.

Indiana Continuing Legal Education Forum (ICLEF)
230 East Ohio Street, Suite 300
Indianapolis, Indiana 46204
Ph: 317-637-9102 // Fax: 317-633-8780 // email: iclef@iclef.org
URL: https://iclef.org

ETHICS –
HOW TO DISCUSS SECURITY WITH YOUR CLIENTS

February 8, 2022

WWW.ICLEF.ORG

DISCLAIMER

The information and procedures set forth in this practice manual are subject to constant change and therefore should serve only as a foundation for further investigation and study of the current law and procedures related to the subject matter covered herein. Further, the forms contained within this manual are samples only and were designed for use in a particular situation involving parties which had certain needs which these documents met. All information, procedures and forms contained herein should be very carefully reviewed and should serve only as a guide for use in specific situations.

The Indiana Continuing Legal Education Forum and contributing authors hereby disclaim any and all responsibility or liability, which may be asserted or claimed arising from or claimed to have arisen from reliance upon the procedures and information or utilization of the forms set forth in this manual, by the attorney or non-attorney.

Attendance of ICLEF presentations does not qualify a registrant as an expert or specialist in any discipline of the practice of law. The ICLEF logo is a registered trademark and use of the trademark without ICLEF's express written permission is prohibited. ICLEF does not certify its registrants as specialists or expert practitioners of law. ICLEF is an equal opportunity provider of continuing legal education that does not discriminate on the basis of gender, race, age, creed, handicap, color or national origin. ICLEF reserves the right to refuse to admit any person or to eject any person, whose conduct is perceived to be physically or emotionally threatening, disruptive or disrespectful of ICLEF registrants, faculty or staff.

INDIANA CONTINUING LEGAL EDUCATION FORUM

OFFICERS

TERESA L. TODD
President

LYNNETTE GRAY
Vice President

HON. ANDREW R. BLOCH
Secretary

SARAH L. BLAKE
Treasurer

ALAN M. HUX
Appointed Member

LINDA K. MEIER
Appointed Member

DIRECTORS

James H. Austen
Sarah L. Blake
Hon. Andrew R. Bloch
Melanie M. Dunajeski
Lynnette Gray
Alan M. Hux
Dr. Michael J. Jenuwine
Shaunda Lynch
Thomas A. Massey
Linda K. Meier
Whittley Pike
Richard S. Pitts
Jeffrey P. Smith
Teresa L. Todd

ICLEF

SCOTT E. KING
Executive Director

James R. Whitesell
Senior Program Director

Jeffrey A. Lawson
Program Director

ETHICS – HOW TO DISCUSS SECURITY WITH YOUR CLIENTS

Description

Addressing security within your office is only half the battle! Unfortunately, your clients often don't know how to protect their own data and security is definitely a team sport. Therefore, it's important to educate your clients about proper security processes and make sure they are okay with the risks associated with electronic communication and storage (if you intend to use them). Nothing is without risk, but by exercising good practices, you and your client can fully enjoy all the benefits of technology and electronic collaboration.

In this session, we'll discuss your communication and confidentiality duties under Rules of Professional Conduct, security issues you should address in engagement agreements, security measures both you and your clients should employ, client portals, email encryption, virtual private networks and other best practices. Finally, we'll cover the breach notification laws and how they impact lawyers.

Faculty

Mr. Barron K. Henley, Esq.
Affinity Consulting Group, LLC
1550 Old Henderson Road, Suite S-150
Columbus, OH 43220
ph: (614) 602-5561
e-mail: bhenley@affinityconsulting.com

February 8, 2022

Barron K. Henley, Affinity Consulting Group, LLC, Columbus OH

Barron K. Henley, Esq. is one of the founding partners of *Affinity Consulting Group*, a legal technology consulting firm focused on automating and streamlining law firms and legal departments. He earned his B.S./B.A. (marketing and economics) and J.D. from The Ohio State University and is a member of the American, Ohio and Columbus Bar Associations, and the Worthington Estate Planning Council. He is a Fellow of the College of Law Practice Management, a Fellow of the American Bar Foundation, a member of Ohio Supreme Court Commission on Technology and the Courts, and a member of both the ABA Law Practice Management and the Real Property Trust and Estate Law ("RPTE") Sections. He's also a former member of RPTE Futures Task Force, a former Board Member for the ABA TECHSHOW, and the former Chair of the Ohio State Bar Association Law Office Automation & Technology Committee. Mr. Henley heads Affinity's document assembly/automation and software training departments. Barron is also an expert in launching new law firms, overhauling existing firms, and documenting and re-engineering law firm processes. Finally, Barron teaches continuing legal education (CLE) classes throughout the U.S. and Canada covering a wide variety of topics related to law practice management, technology, and ethics.

Addressing Security Issues with Your Clients

Barron K. Henley, Esq.
bhenley@affinityconsulting.com
Affinity Consulting Group, LLC
1550 Old Henderson Rd., Suite S-150
Columbus, MN 43220
614.340.3444
www.affinityconsulting.com

Addressing Security with Your Clients
Table of Contents

I. **A LAWYER'S SECURITY REQUIREMENTS**: The Rules of Professional Conduct more fully described in Section III below require lawyers to make *reasonable efforts* to prevent the disclosure of confidential client information. The comments to Rule 1.6 require lawyers to *act competently* to safeguard client information, and use *reasonable safety precautions* when transmitting a client communication. Further, Rule 1.4 requires that lawyers communicate with their clients, keep them reasonably informed as to status, and promptly inform them about anything requiring their informed consent.

If law firms do not protect client communications and data, they could violate the attorney-client privilege, face malpractice actions, lose clients, damage their reputation, and possibly also lose their license to practice.

II. **ISSUES TO ADDRESS**: In the average representation, there is a lot of communication occurring between lawyer and client, much or most of which is electronic. There is also quite a bit of other electronic data and information being passed between lawyer and client. As we all know, electronic information is much more difficult to protect against disclosure than analog information. In order for all of those communications and data to remain confidential, both parties need to know how to protect it. Therefore, it makes sense to discuss with your clients the following issues before you even agree to represent them.

A. **Communication**: How can lawyer and client communicate electronically while ensuring confidentiality?

B. **How You Protect Client Data**: It makes sense to explain to your clients what you're doing to protect their (and your) data.

C. **Where You Store Client Data**: The comments to Rule 1.6 indicate that the client can ask you to do more than required by the rules to protect their information. That's an issue you definitely want to know their disposition on *before* you start representing them. If you're storing data in the cloud, it would make sense to let them know that even if you're not otherwise required to do so.

D. **How Clients Protect Their Own Data**: What advice should lawyers be giving technically unsophisticated clients about protecting their data and communications?

III. **RELEVANT ETHICS RULES**: I've only reproduced the sections of the rules and comments below which are relevant to this discussion. Further, I've bolded the particularly important text. In 2012, the American Bar Association promulgated amendments to the Model Rules of Professional Conduct which dealt with technology and data security. 38 states have adopted those changes although Indiana has not adopted all of them (for a full list, see https://www.lawsitesblog.com/tech-competence/).

A. **IN RULE 1.1 - Competence**: A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

B. **IN Rule 1.1 Comment 6**:

[6] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, ***including the benefits and risks associated with the technology relevant to the lawyer's practice***, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

C. **IN RULE 1.6 - Confidentiality of Information**:

(a) A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

…

D. **ABA Model Rule 1.6 - Confidentiality of Information**:

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

(c) 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.

E. **IN RULE 1.6 Comment 16 - Acting to Preserve Confidentiality**:

[16] A lawyer ***must act competently to safeguard information*** relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision.

F. **ABA Rule 1.6 Comment 18 - Acting Competently to Preserve Confidentiality**:

[18] Paragraph (c) requires a lawyer ***to act competently to safeguard information*** relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. ***The unauthorized***

access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the ***sensitivity of the information***, the ***likelihood of disclosure*** if additional safeguards are not employed, the ***cost*** of employing additional safeguards, the ***difficulty*** of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). ***A client may require the lawyer to implement special security measures not required by this Rule*** or may give informed consent to forgo security measures that would otherwise be required by this Rule.

G. IN Rule 1.6 Comment 17:

[17] When ***transmitting a communication*** that includes information relating to the representation of a client, the lawyer ***must take reasonable precautions to prevent the information from coming into the hands of unintended recipients***. This duty, however, ***does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy***. ***Special circumstances***, however, ***may warrant special precautions***. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the ***sensitivity of the information*** and the ***extent to which the privacy of the communication is protected by law or by a confidentiality agreement***. ***A client may require the lawyer to implement special security measures not required by this Rule*** or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.

H. IN RULE 5.1 - Responsibilities of a Partner or Supervisory Lawyer:

(a) A partner in a law firm, and a lawyer who individually or together with other lawyers possess comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.

(b) *A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.*

(c) **A lawyer shall be responsible for another lawyer's violation of the Rules of Professional Conduct if**:

(1) **the lawyer orders or, with knowledge of the specific conduct, ratifies the conduct involved**; or

(2) **the lawyer having direct supervisory authority over the other lawyer knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action**.

I. IN RULE 5.3 - Responsibilities Regarding Nonlawyer Assistants: This rule makes Rule 1.6 apply to everyone that works for the lawyer (not just the lawyers). It further makes the lawyer(s) responsible for the conduct (and mistakes) of nonlawyer assistants.

With respect to a nonlawyer employed by, retained by, or associated with a lawyer:

(a) **a partner, and a lawyer who individually or together with other lawyers possess comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;**

(b) **a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and**

(c) **a lawyer shall be responsible for the conduct of a nonlawyer that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if**:

(1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or

(2) **the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.**

IV. <u>INDIANA BREACH DISCLOSURE LAW</u>: Ind. Code § 4-1-11 et seq.; § 24-4.9-1 et seq.

IC 24-4.9-2-2 "Breach of the security of data"

Sec. 2. (a) "Breach of the security of data" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person. The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.

(b) **The term does not include the following:**

(1) Good faith acquisition of personal information by an employee or agent of the person for lawful purposes of the person, if the personal information is not used or subject to further unauthorized disclosure.

(2) **Unauthorized acquisition of a portable electronic device on which personal information is stored, if all personal information on the device is protected by encryption and the encryption key:**

(A) **has not been compromised or disclosed; and**

(B) **is not in the possession of or known to the person who, without authorization, acquired or has access to the portable electronic device**.

V. **<u>RELEVANT DEFINITIONS</u>**: There are a couple of things worth understanding as it relates to this discussion.

A. **Encryption**: For purposes of this discussion, encryption can be defined as follows.

> "Encryption is the process of converting data to an unrecognizable or 'encrypted' form. It is commonly used to protect sensitive information so that only authorized parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the Internet.
>
> …
>
> An encrypted file will appear scrambled to anyone who tries to view it. It must be decrypted in order to be recognized. Some encrypted files require a password to open, while others require a private key, which can be used to unlock files associated with the key."[1]

B. **Encryption In Transit**: This simply means that data is encrypted as it is traveling through the internet. Here's a good definition:

> "Data in transit, or data in motion, is data actively moving from one location to another such as across the internet or through a private network. Data protection in transit is the protection of this data while it's traveling from network to network or being transferred from a local storage device to a cloud storage device – wherever

[1] See http://techterms.com/definition/encryption

data is moving, effective data protection measures for in transit data are critical as data is often considered less secure while in motion."[2]

C. **Encryption At Rest**: This is encryption of data that is stationary on a particular device, computer or server.

> "Data at rest is data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way. Data protection at rest aims to secure inactive data stored on any device or network. While data at rest is sometimes considered to be less vulnerable than data in transit, attackers often find data at rest a more valuable target than data in motion."[3]

D. **Two Factor Authentication**: Here's a good definition.

> "Two-factor authentication (2FA), often referred to as two-step verification, is a security process in which the user provides two authentication factors to verify they are who they say they are. 2FA can be contrasted with single-factor authentication (SFA), a security process in which the user provides only one factor -- typically a password.
>
> Two-factor authentication provides an additional layer of security and makes it harder for attackers to gain access to a person's devices and online accounts, because knowing the victim's password alone is not enough to pass the authentication check. Two-factor authentication has long been used to control access to sensitive systems and data, and online services are increasingly introducing 2FA to prevent their users' data from being accessed by hackers who have stolen a password database or used phishing campaigns to obtain users' passwords.
>
> The ways in which someone can be authenticated usually fall into three categories known as the factors of authentication, which include:
>
> 1. **Knowledge factors** -- something the user knows, such as a password, PIN or shared secret.

---

[2] Data Protection: Data In transit vs. Data At Rest by Nate Lord for Digital Guardian, published September 19, 2018, see http://bit.ly/2L4Rygd.

[3] Id.

2. **Possession factors** -- something the user has, such as an ID card, security token or a smartphone.

3. **Inherence factors, more commonly called biometrics** -- something the user is. These may be personal attributes mapped from physical characteristics, such as fingerprints, face and voice. It also includes behavioral biometrics, such as keystroke dynamics, gait or speech patterns."[4]

VI. RECOMMENDATIONS:

A. If You Use Email, You Need An Encryption Service: Revisit Rule 1.6 Comment 16.

> "[16] A lawyer must ***act competently*** **to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure** by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision."

The question to consider is: What constitutes "acting competently" to protect the client's data; and do you have a reasonable expectation of privacy when you use email? I would argue that reasonable precautions means that you must encrypt your email when sending sensitive documents. Further, although the ethical rules and case law presume that lawyers have a reasonable expectation of privacy when sending an email, common sense has to tell you otherwise.

1. **What The Experts Say**: Here are a couple of quotes to consider.

> "A secure email account that the attorney is assured protects the content of correspondence. No attorney should use Gmail or other free services that in fact admit that they use personal information from email content. They should encrypt their client correspondence. Before sending sensitive correspondence, they should check by phone or text with the client to see what method of delivery is preferred."[5]
>
> "The level of encryption may vary based on practice areas or, more importantly, the firms' clients. At a minimum, emails and attachments that contain confidential data

[4] See http://searchsecurity.techtarget.com/definition/two-factor-authentication

[5] Law Firm Data Security: Experts on How to Protect Legal Clients' Confidential Data, by Nate Lord, DigitalGuardian, October 13, 2015, quoting Robert Ellis Smith. See http://tinyurl.com/h6nzvjb.

should be encrypted or sent through collaboration tools that send encrypted links rather than plain text data."[6]

"It's all about encryption of the 3 main risk areas for data held: data in transit, at rest and in backups. It doesn't matter if it's email, Instant Messages, case files, discovery or 3rd party expert communications, the principle of encryption is the ONLY way you can really satisfy due diligence requirements."[7]

2. **Email Encryption Services**: There are many ways to encrypt email, but the easiest is to use an encryption service. The options listed below are inexpensive and easy. They encrypt both the emails and any attachments to the email. In most cases, a password must be entered by the recipient to open the email and any attachments.

   a. **RMail**: http://www.rmail.com/ - registered email service which can prove delivery + encrypted email

   b. **Office 365 Message Encryption**: This is included with the Office 365 E3 and E5 bundles[8]. For more information, see http://bit.ly/2L8zW2I

   c. **ShareFile**: https://www.sharefile.com/

   d. **SenditSecure**: https://www.senditsecure.com/

   e. **SenditCertified**: http://www.senditcertified.com/ and note that they offer discounts through several bar associations.

   f. **EchoWorx Encrypted Mail**: http://tinyurl.com/h6sm668

   g. **Hushmail**: https://www.hushmail.com/

   h. **ZixMail**: https://www.zixcorp.com/

   i. **ProofPoint**: http://bit.ly/2L6cFi5

3. **Poor Man's Encryption**: If you don't want to spend the money on an email encryption service, you could always keep the text of the email innocuous ("Please see attached.") and encrypt the attachments. Word,

[6] ibid., quoting Marco Maggio.

[7] ibid., quoting Steve Santorelli.

[8] See https://products.office.com/en-us/business/compare-more-office-365-for-business-plans

WordPerfect, and the PDF programs Adobe Acrobat, Nuance Power PDF, Nitro Pro, and Foxit PhantomPDF all allow users to encrypt the individual files so they cannot be opened without a password. This capability costs nothing if you already have one of those programs.

B. Consider Using a Secure Portal for Exchanging Documents: Here's a good definition of a Client Portal:

> "A client portal is an electronic gateway to a collection of digital files, services, and information, accessible over the Internet through a web browser. The term is most often applied to a sharing mechanism between an organization and its clients. The organization provides a secure entry point, typically via a website, that lets its clients log into an area where they can view, download, and upload private information."[9]

I realize that the foregoing sounds a little fancy, but it really isn't. It's just a secure way of sharing documents and information with your clients without using email. Nearly all of the popular legal case management systems now have a portal as a standard feature. For example, ActionStep, Centerbase, CosmoLex and Clio all have portals, among others. Further, there are many services which provide this function (they're often marketed as "secure file sharing" or "data room" services.

1. **ShareFile by Citrix**: https://www.sharefile.com/ - This is a fantastic service that allows you to create virtual "rooms" for others and share documents with them securely. You decide what rights each user has to the collection of documents.

2. **Merrill DataSite Virtual Data Room**: See http://tinyurl.com/laam53o.

3. **Firmex Virtual Data Room**: See https://www.firmex.com/.

4. **SmartRoom Virtual Data Room**: See http://smartroom.com/.

5. **Ansarada Virtual Data Room**: See https://www.ansarada.com/

6. **IntraLinks Virtual Data Room**: See http://preview.tinyurl.com/lt6d899.

7. **Microsoft Office 365 or OneDrive for Business**: OneDrive is Microsoft's cloud storage offering and it comes with nearly every Office 365 plan. For only $5/user/month (Business Essentials plan), you get 1 TB of online storage. See this: http://tinyurl.com/h9mdn2v

[9] See https://en.wikipedia.org/wiki/Client_portal

8. **G Suite by Google Cloud**: The Basic edition is $5/user/month and includes 30 GB of cloud storage; the Business edition is $10/user/month and includes unlimited cloud storage. See your options here: http://tinyurl.com/kkocuto

9. **Dropbox Business Standard or Advanced**: Standard is $12.50/user/month and Advanced is $20/user/month. For an explanation of their business plans, see https://www.dropbox.com/business/plans-comparison.

10. **SpiderOak Professional**: See this for more: https://spideroak.com/business_pricing/

11. **Syncplicity**: See https://www.syncplicity.com/.

12. **Box.com**: https://www.box.com/pricing

13. **TrueShare**: http://www.trueshare.com/

14. **FileGenius**: http://www.filegenius.com/

15. **OneHub**: Secure file sharing - see https://onehub.com.

C. **Talk About Communication Protocols Up Front**: Specifically, I recommend addressing the following issues. Ideally, these issues could be addressed in the engagement agreement your client signs.

1. How do you prefer to be contacted for normal (non-emergency) communications (phone, email, text, etc.)?

2. Can you be reached during non-business hours in the case of an emergency; and if so, by what method? Is there a higher cost?

3. If you're not available during normal business hours, then who should the client contact instead (if anyone)?

4. Is regular email acceptable for non-confidential communication?

5. Is encrypted email acceptable for confidential communication? Of course, this requires that you have email encryption.

D. **Only Use Online Services That Offer Encryption in Transit and Encryption at Rest**: This is worth explaining to clients who may be worried about internet security. If you have both encryption in transit and at rest, then you've met any reasonableness standard imposed by the Rules of Professional Conduct.

E. Use a Password Manager and Encourage Clients To Do The Same:

1. **What Is a Password Manager**: A password manager is a program that helps one store, create and organize passwords (and logons and websites, etc.).

2. **Why You Need A Password Manager**: First, it's part of your estate plan. Second, it's a place to keep logons, websites, account numbers and passwords all in one place. I use Dashlane and it will generate and store strong passwords for me (so I don't have to make them up). As a result, all of my passwords like something like this: jC7_!U-/M!qmQ[fwF|ew. In other words, they're nonsense and nearly impossible to remember. However, I don't have to remember them because the password manager does that for me. I only need to remember the ONE strong password that unlocks my password manager. It will also let me know if my passwords are weak and recommend that I change them. It tells me how many different websites I'm using the same password for (it's not recommended that you use the same password for everything). It also lets me know if there are any reported security breaches for any of the websites it holds passwords for and recommend that you change them. Finally, it will hold all of my credit card information, secure notes about anything I want and personal information like my driver's license, passport, etc.

3. **Good Options**: Top rated password managers include the following (and I strongly recommend the versions you have to pay for - almost all offer a free version that is missing features):

    a. **1Password** - https://1password.com/

    b. **Dashlane** - https://www.dashlane.com/

    c. **Keeper Desktop** - https://keepersecurity.com/

    d. **LastPass** - https://www.lastpass.com/

    e. **LogMeOnce** - https://www.logmeonce.com/

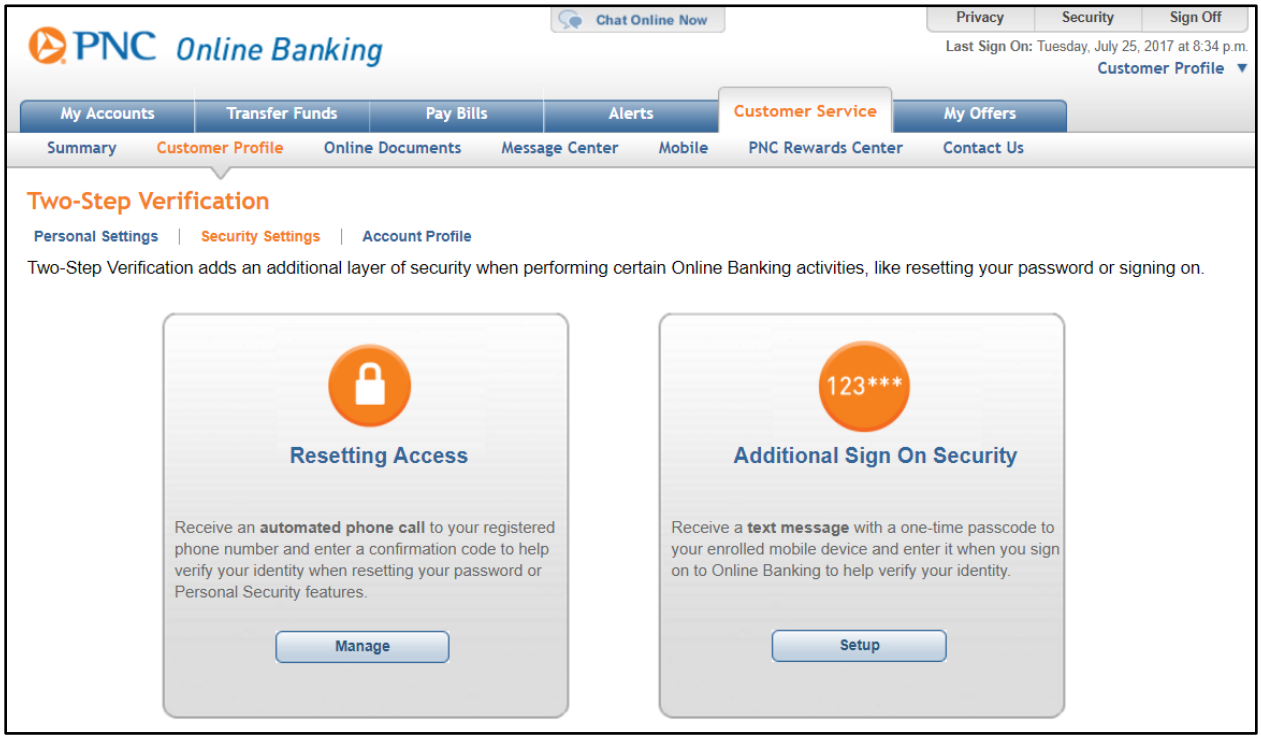
    f. **RoboForm** - https://www.roboform.com/

    g. **Sticky Password** - https://www.stickypassword.com/

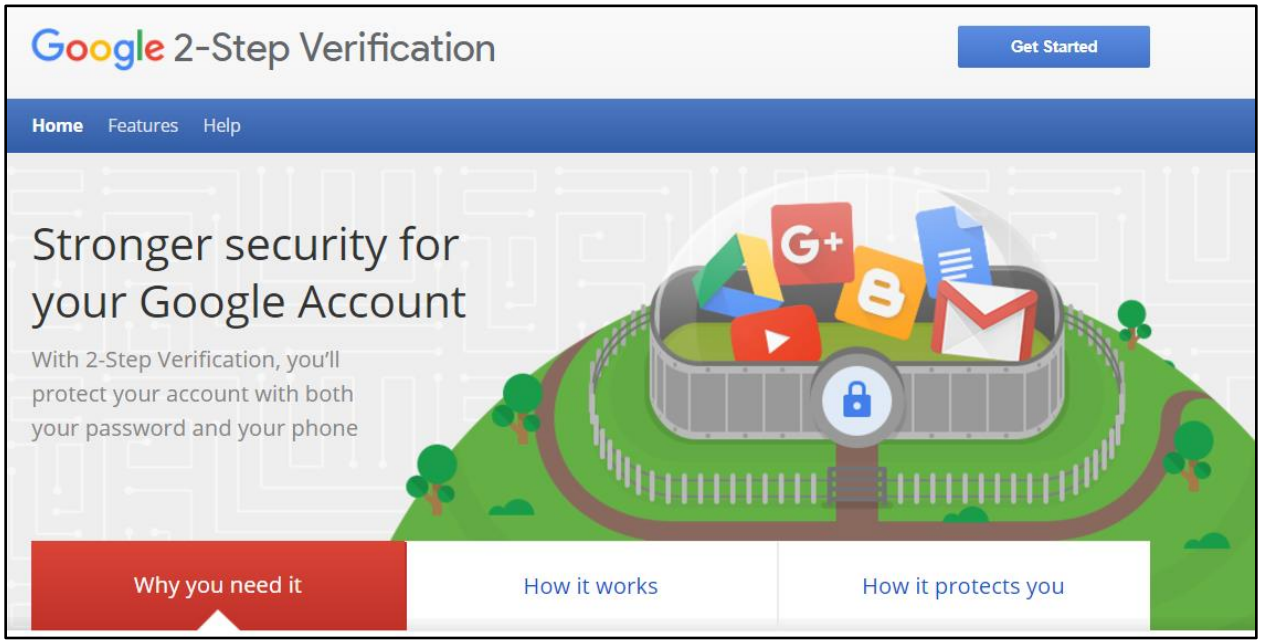
    h. **TrueKey** - https://www.truekey.com

F. You Should Use Two Factor Authentication And So Should Your Clients: For critical services you access online, check to see if they offer any type of 2FA. Keep in mind that 2FA is ANNOYING, but better security is almost always more

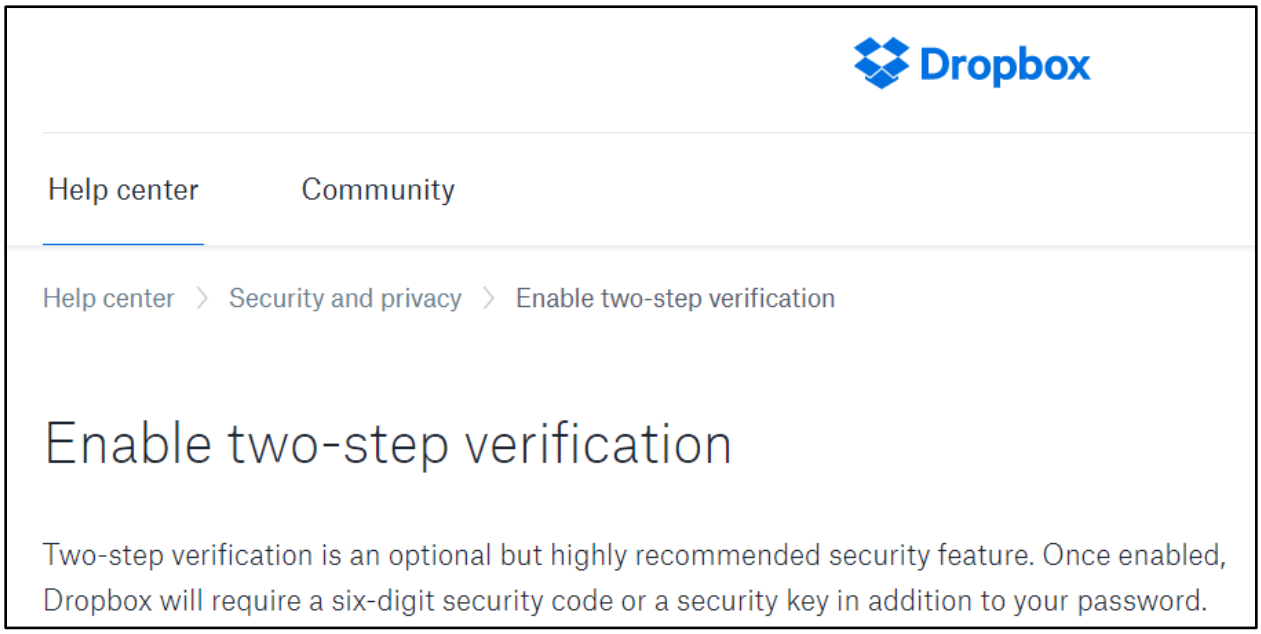
annoying. If you want to protect yourself well, be prepared to be slightly annoyed. Anyway, here are some 2FA ideas. Banks probably offer it:



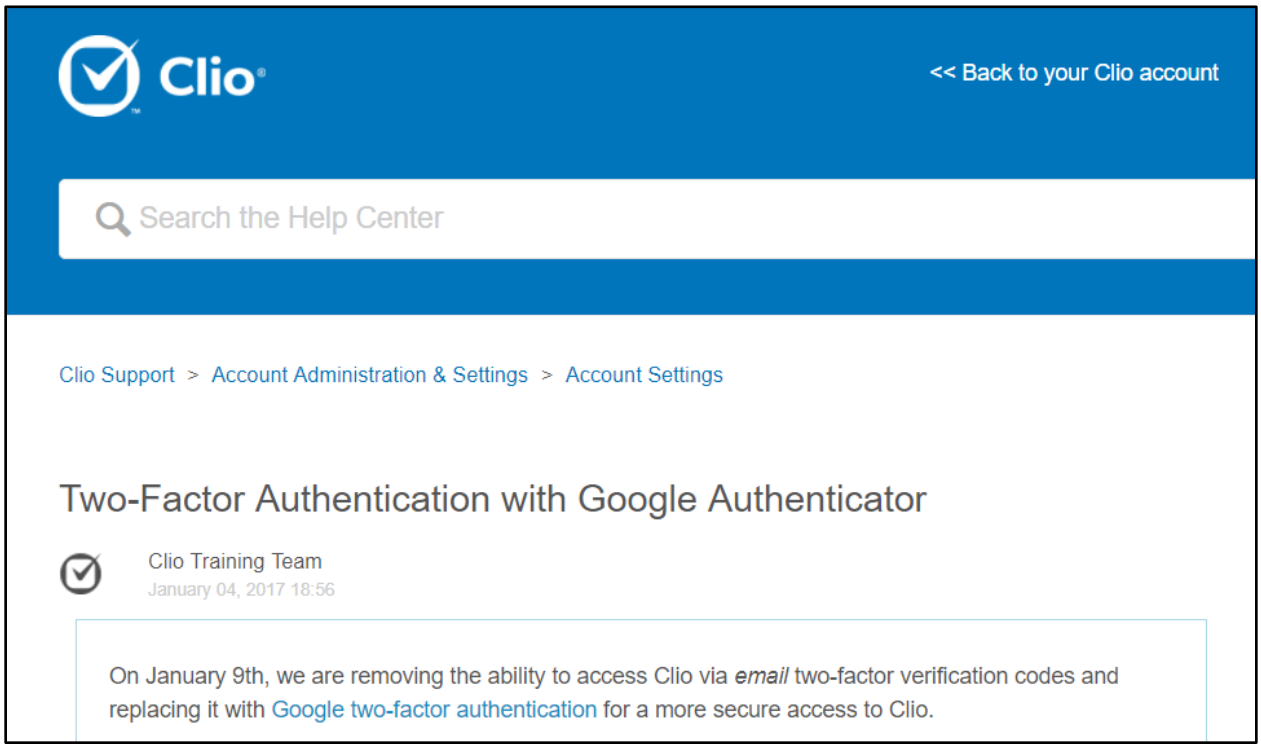
Email accounts probably offer it:



File sharing services probably offer it:



Case management systems probably offer it:



G. **Communication and Security Advice for Your Clients**: If your client is a business, they're obviously more likely to have some security protocols in place. If the client is an individual, I'd make sure to talk about the following with them:

1. **No Business Email**: A lot of people don't realize that their employer has the right to access anything they send or receive via their business email accounts. As such, employer email accounts should never be used to communicate with you.

2. **Cloud Storage**: If you're storing client files in the cloud, you should probably explain this to your clients and add something to your engagement agreement reflecting this practice. I would also explain the security and encryption involved so they know the exposure risk is very low.

3. **Internet Security Is An Oxymoron**: Many security experts have said that you cannot completely protect any data, but you can take steps to make it very hard to hack. However, even if you don't expose any information to the internet, it's still possible for it to be stolen or destroyed. Everything involves *some* assumption of the risk. For example, U.S. vehicle deaths topped 40,000 in 2017[10], but most of us drive every day in spite of that. Putting data on the web is no different.

4. **Texting**: My advice is not to offer this as a communication method with clients, but some clients simply prefer it. For a great discussion of the issues with this, see The 411 on Texting for Lawyers[11] by Jim Calloway and Ivan Hemmans. In any event, if you're going to text with clients, it's important that you have some means of saving those texts to your client's file. You can take "screen shots" of text messages although that's a rather slow way of archiving them. As discussed in the aforementioned article, there are also tutorials on how to capture text messages such as How To Save Text Messages in Android and iOS[12] by Simon Hill on Digital Trends. Finally, for ensuring security with text messages, consider Signal[13] or WhatsApp[14].

5. **Encrypt Cell Phones**: People lose cell phones often and they almost always have access to email. If you're using email to communicate with your client, then the phone may be an easy point of breach. All smartphones have free encryption software built in. In some cases, it's already on and the user doesn't even know it. For example, I have a Samsung Galaxy Note

[10] See http://bit.ly/2L5FjQu

[11] See http://bit.ly/2L4X9mH

[12] See https://www.digitaltrends.com/mobile/how-to-save-text-messages/

[13] See https://signal.org/

[14] See https://www.whatsapp.com/

9 and the encryption is compulsory (you can't turn it off even if you want to). Of course, you should have your cell phone encrypted as well.

6. **Encrypt Their PCs**: If they're communicating with you and storing documents you send them on a personal computer, it makes sense for that device to be encrypted. Encryption would prevent a thief or finder of their laptop from obtaining any information from the hard drive, even if they remove the hard drive and install it in another computer. There are many choices for this type of software, including the following:

    a. **BitLocker** - included for free with Windows Professional 8, 8.1 & 10.

    b. **Mac FileVault** - included for free with OSX.

    c. **SecuriKey Pro** - https://www.securikey.com/

    d. **Symantec Drive Encryption** - http://tinyurl.com/39seow

    e. **AlertBoot** - http://tinyurl.com/63h36wt

    f. **Folder Lock** - http://www.newsoftwares.net/folderlock/

    g. **SecureDoc Full Disk Encryption** from Winmagic Data Security - http://tinyurl.com/4vek6ot

    Of course, your laptop should be encrypted as well.

7. **Encrypt Their Tablets**: All iPads and Android tablets have free encryption software built in. It just has to be enabled.

H. **Establish Security Policies For Your Office**: After they're established and being followed, it would probably be a good idea to let your clients know. There are many places to find sample policies for the following and a great resource is the SANS Institute. To see their sample policies, just go here: https://www.sans.org/security-resources/policies.

1. **Internet and Email Usage Policy**: There may be (and likely is) a big gap between what you would deem acceptable use of company internet and email and what your employees deem acceptable use of those resources. Thankfully, you can Google "internet usage policy" and find many free examples to start with.

2. **Document and Email Retention Policy**: Lawyers tend to hold onto every document and email forever and this is simply a bad policy. You can end up with so much irrelevant digital clutter that you're unable to find the things you actually need. Your policy should comply with any applicable

federal or state laws, the Rule of Professional Conduct and any other relevant regulations. It's also a great idea to contact your malpractice insurer to see what they recommend (they may even have a sample policy you could start with). The ABA has a nice compilation of records and document retention resources (http://tinyurl.com/7z8ksye) and another excellent article to read on the subject is Sample Document-Destruction Policy by Megan Zavieh, 1/21/14, Lawyerist.com (see http://tinyurl.com/hrs3hxy).

3. **Secure Password Policy**:

   a. **Why You Need This**: You need a secure password policy because of the plethora password crackers that are out there.

   b. **Types of Password Hackers**: Here are the main types (there are many more):

      i. **Dictionary attack**: This attack uses a file that contains a list of words that are found in the dictionary. This mode matches different combinations of those words to crack your device open.

      ii. **Brute force attack**: Apart from the dictionary words, brute force attack makes use of non-dictionary words too.

      iii. **Rainbow table attack**: This attack comes along with pre-computed hashes. When user passwords are stored by a service (say www.Target.com), the raw (actual) passwords are converted into a string of random characters by complicated mathematical computations. This conversion process is called hashing. For an extremely interesting article on this technology, see Hacker Lexicon: What Is Password Hashing? by Andy Greenberg, June 8, 2016[15].

   c. **Examples of Password Hackers**: Just so you can appreciate how readily available these are to anyone.

      i. **John The Ripper** - http://www.openwall.com/john/

      ii. **Aircrack-ng** - https://www.aircrack-ng.org/downloads.html

      iii. **RainbowCrack** - http://project-rainbowcrack.com/

[15] See https://www.wired.com/2016/06/hacker-lexicon-password-hashing/

iv. **Crowbar** - https://github.com/galkan/crowbar

v. **Ophcrack** - http://tinyurl.com/3uyvmy

vi. **L0phtcrack** - http://www.l0phtcrack.com/#download-form

vii. **DaveGrohl** - https://github.com/octomagon/davegrohl

There are many others like Cain and Abel, THC Hydra and HashCat.

d. **Recommended Policy**: I will warn you that a really strong password security policy can be extremely annoying because most of them recommend that you change your password every 30 days, don't repeat old ones and use unique passwords for each logon. While I appreciate the value of those rules, they would drive most people batty in short order. Here are some less annoying rules that will still help ensure your passwords are secure:

- 12 Characters, Minimum: You need to choose a password that's long enough. There's no minimum password length everyone agrees on, but you should generally go for passwords that are a minimum of 12 to 14 characters in length. A longer password would be even better.

- Include Numbers, Symbols, Capital Letters, and Lower-Case Letters: Use a mix of different types of characters to make the password harder to crack.

- No Dictionary Words or Combination of Dictionary Words: Avoid obvious dictionary words and combinations of dictionary words. Any word on its own is bad. Any combination of a few words, especially if they're obvious, is also bad. For example, "Wagon" is a terrible password. "RedWagon" is also very bad.

- Doesn't Rely on Obvious Substitutions: Don't use common substitutions, either — for example, "RedWag0n" isn't strong just because you've replaced an o with 0.[16]

4. **Mobile Device Security Policy**: This policy describes protocols that must be used when using notebooks, tablets or phones to conduct legal work.

[16] See How to Create a Strong Password (and Remember It) by Chris Hoffman, 5/29/15, How-To- Geek, see http://tinyurl.com/kx6s7uf.

5. **Equipment Disposal Policy**: The general rule is that no mobile device, PC or copier should ever be disposed of while it still contains client data.

I. **Use Wireless Encryption**: If you're connecting to the internet via a wireless router in your office or home, then you should ensure that the highest level of encryption offered by the router is being employed. If you're connecting to the internet via a public or other ad hoc wireless connection and you're transmitting confidential client data, then you should secure your connection.

1. **Risk of Using Public WiFi**: First of all, lets talk about the risks. For a quick primer, here are two short articles that will bring this issue into focus: Here's what an eavesdropper sees when you use an unsecured Wi-Fi hotspot by Eric Geier, 6/28/13 (see http://tinyurl.com/ppm3oyc) and What Is A Packet Sniffer? by Andy O'Donnell, 12/15/14 (see http://tinyurl.com/jxvhf92). For an interesting discussion of this in the legal arena, see the now famous California Formal Opinion No. 2010-179 which states:

> "With regard to the use of a public wireless connection, the Committee believes that, due to the lack of security features provided in most public wireless access locations, **Attorney risks violating his duties of confidentiality and competence in using the wireless connection at the coffee shop to work on Client's matter unless he takes appropriate precautions, such as using a combination of file encryption, encryption of wireless transmissions and a personal firewall**. Depending on the sensitivity of the matter, Attorney may need to avoid using the public wireless connection entirely or notify Client of possible risks attendant to his use of the public wireless connection, including potential disclosure of confidential information and possible waiver of attorney-client privilege or work product protections, and seek her informed consent to do so."[17]

2. **How To Protect Yourself**:

   a. **Cellphone WiFi Hotspot**: Rather than connecting to the public WiFi where ever you are, consider using a cellular hotspot or MiFi. Properly configured, these connections are a secure way to connect your notebook or tablet to the Internet via the phone hotspot.

[17] See http://tinyurl.com/3szklcx, emphasis added.

b. **Consumer VPN Services**: There are many services that allow you to create a Virtual Private Network connection even though you're using a public and otherwise unsecured WiFi connection. "In the simplest terms, a VPN creates a secure, encrypted connection between your computer and the VPN's server. This tunnel makes you part of the company's network as if you are physically sitting in the office, hence the name. While connected to the VPN, all your network traffic passes through this protected tunnel, and no one in between can see what you are up to. A consumer VPN service does the same thing, but extends that protection to the public."[18] Here are some options for this. Private Internet Access is the one I use personally.

   i. **NordVPN**: https://nordvpn.com/

   ii. **Hide My Ass**: https://www.hidemyass.com/

   iii. **Private Internet Access**: https://www.privateinternetaccess.com/

   iv. **IPVanish**: https://www.ipvanish.com/

   v. **ExpressVPN**: https://www.expressvpn.com

   vi. **PureVPN**: https://www.purevpn.com/

   vii. **StrongVPN**: https://strongvpn.com

   viii. **Cloak** (Mac only): https://www.getcloak.com/

   ix. **CyberGhost**: http://www.cyberghostvpn.com/en_us

   x. **VyprVPN**: https://www.goldenfrog.com/vyprvpn

   xi. **Hotspot Shield Elite**: https://hsselite.com/

   xii. **Spotflux Premium**: http://spotflux.com/

J. If You Represent Businesses: You should download and read the **Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information** here (http://bit.ly/2B16AyW). If you don't already have to comply with it, then you may soon have to.

[18] The Best VPN Services for 2016, by Max Eddy, Fahmida Rashid, 3/9/2016, PCMag - see http://tinyurl.com/njuv7br.

K. **Be Involved In Your Own Information Technology**: None of this can be left to chance or assumptions. If you lose access to or control of your client data because of a technology issue, there's no one else to blame. You need to understand how your system is configured. You don't have to be a technology wizard, but whoever is handling your technology should be able to provide the information you don't presently have. If you don't have anyone helping you with your technology, then unless you're an IT expert, it's time to find someone. In any event, here are some questions you should be able to answer:

1. Do all of the PCs in your office have the latest security-related updates installed for the operating system (Windows or Mac) and your office suite (Microsoft Office, etc.)?

2. Where is your data located?

3. Do you have a firewall? If so, is it hardware, software or both? If you're relying on a router/firewall (hardware), when was the firmware updated last?

4. What antivirus/antimalware software is each of your computers running? Have you verified that the definitions are current?

5. Backups:

    a. How is your data being backed up and where is the data stored?

    b. How many versions of each file do you have backed up?

    c. How do you restore a file? Have you tested that?

6. Disaster recovery:

    a. How long would it take to recover from a total loss (office destroyed by fire, for example), or the loss of your personal computer (crash, theft, etc.)?

    b. If your current office were gone, how long would it take to re-establish a functioning office elsewhere?