Tools for Sharing and Collaborating Securely

MPLP 5th Friday Webinar, April 2021

With MPLP/MAP IT Staff and Special Guest - Michael Cunningham
IT Technician, Lakeshore Legal Aid
Fifth Friday Webinar Series

Schedule for remainder of 2021:

- July 30, 2021 - 25 Tech Tips
- October 29, 2021 - topic TBD

Recordings of and supporting materials for previous webinars available at:

- [http://www.mplp.org/Taskforces/technology](http://www.mplp.org/Taskforces/technology)
Agenda

- Why are data sharing policies important?
- What are some tools in use right now?
- Deeper dive into some of these tools:
  - SharePoint for collaboration
  - Teams for collaboration
  - Secure E-Signature using Adobe Sign
  - Sending encrypted Emails with Virtru and others
- Q&A
Sharing Securely

- Sharing data electronically is key to partnerships and communication.
- Security is critical to the attorney-client relationship.
- The goal is to achieve both.
Policy and Practice Considerations

- What data requires encryption/protection?
- Sharing data on your platforms with external partners/clients
- Adding your client info to another partner’s platform
- Data sharing agreements
- Training
LLA Security Apps/Software
Michael Cunningham

- Virtru (256-bit encryption)
- Bitdefender (updates in real time)
- 365 Encryption Adobe Pro D
- Future Security:
- Barracuda- Email catch (virus, phishing emails, encryption, spam email)
LLA Methods for Document Storage
Michael Cunningham

- HIPPA Compliant File Storage/Sharing
- Email
- Upload to SharePoint/OneDrive
- Provide links to folder (like Google Drive/Dropbox)
- Sometimes provides passwords to access the folders, either through phone or encrypted email
MAP Methods for Security and Sharing

- SharePoint Sites and Teams (internal only) for sharing and collaborating on sensitive documents with MAP staff.
- SharePoint Sites and Teams (internal+external) for sharing and collaborating on sensitive documents with partners, co-counsel, etc.
- Google Drive for sharing and collaborating on less sensitive documents with MAP staff, partners, co-counsel, etc.
- Box (MIRC only) for sharing and collaborating on sensitive documents with partners, co-counsel, etc.
- Virtru email encryption for sharing highly sensitive documents with clients, partners, co-counsel, etc.
- Gmail confidential mode for sharing more sensitive documents and passwords.
- Bitwarden “Send” for sharing sensitive, temporary information like access information, usernames, passwords, etc. to internal and external partners.
- Adobe Sign through Acrobat Pro and Reader for securely obtaining and transmitting signed documents.
Collaborating w/ Sharepoint – creating site

- **Video Demo** of how to create a Sharepoint site; **PDF Slides** of the same
- Sharepoint-->Create site-->Team site-->Name, URL-->Add internal members
- If you plan to copy a large amount of info into a newly created site, please plan to allow 24 hours between creation of the site and import of information
Collaborating w/ Sharepoint – external users

- External members must be added/removed via Outlook (2) from a link in Sharepoint (1); can be removed via Sharepoint (3)
- Video Demo of how external users authenticate/access Sharepoint sites that have been created; PDF Slides of the same
- MAP IT requires external users to sign a Data Sharing Agreement; we have templates available if desired
External SharePoint - folder-level external sharing

In MAP’s SharePoint it’s possible to share with external users at the folder-level so that users don’t have access to the entire document library.

MAP’s External SharePoint Sites require external users to complete Multi-factor authentication before accessing any documents.

Information Rights Management

Microsoft Information Rights Management (IRM) is a feature of SharePoint that allows an organization apply end-to-end encryption to all the files in a SharePoint site so that files cannot be lost or shared beyond the intended recipient. As of now, IRM does not allow co-editing of Office 365 documents. However, this feature is in development.
Google Shared Drives are a good way to save less-sensitive documents with teams, so ownership isn’t tied to an individual and access can’t be lost when a user leaves the organization.

Google Shared Drives recently added a feature that allows you to share documents with individuals outside of your team, and optionally outside of your organization.

MAP-IT uses an internal Shared Drive and an external Shared Drive for different purposes.
Adobe Sign securely handles large volumes of online signature processes, including:

- Managing user identities, authentication and access control (such as an Adobe ID)
- Certifying document integrity
- Verifying e-signatures
- Logging recipient acceptance or acknowledged receipt of documents
- Maintaining audit trails

Additionally, Adobe Sign cloud signatures enable remote digital signatures backed by digital certificates from trust service providers (TSPs) with verified Cloud Signature Consortium (CSC) standard integrations to Adobe Sign.
Data encryption

- Adobe Sign employs [PCI DSS approved encryption algorithms](https://www.pcisecuritystandards.org/) to encrypt documents and assets at rest with AES 256-bit encryption and uses HTTPS TLS v1.2 to protect data in transit.
- Documents at rest can only be accessed with appropriate capability-based security permissions through the application data access layer in a private subnet. [Document encryption keys](https://www.adobe.com/corp/adobe-sign/dataSecurity.html) are stored and managed in a secure environment with restricted access.
Electronic signature with Adobe Acrobat Reader

For user who does NOT have Adobe ID yet, select Get Started and Continue with Google

*You can send up to 2 documents for signature for free everyone 30 days*
Electronic signature with Adobe Acrobat Reader

Adobe ID verification process on a browser requires your date of birth

Note: Depending your account type (personal or company, Adobe Acrobat Reader or Adobe Acrobat Pro), the sign-in process could be slightly different.

Sign-in with Federated ID
Electronic signature with Adobe Acrobat Reader

- **Steps to follow to digitally sign in Adobe Reader**
- **Get documents signed by others**
- **Signer's experience**
- **Track agreements sent for signature**
Electronic signature with Adobe Acrobat Reader

Send documents for signature

- You can get documents signed by others using the Fill and Sign tool.
- You may view your agreements via Adobe Reader app
Send documents for signature

- The signed agreement is certified by Adobe Sign.
- You may also manage your agreements via Adobe Sign online.
- After you login, you will be redirected to Adobe Acrobat.
Virtru Email Encryption and alternatives

Purpose of email encryption - Add a layer of protection to emails beyond that offered by "certificate-based", TLS encryption of Gmail. While Gmail is encrypted "in-transit" and "at-rest", Virtru offers "end-to-end" encryption which allows only the intended recipient to see the contents of an email if that email is forwarded to a party that was not the intended recipient of the email.

End-to-end, "key-based" encryption works by storing a unique key for a user that they must authenticate in order to access. Only this key can unlock the contents of the encrypted document. So, if a user cannot access the key, they cannot access the document.

If your account is hacked, encryption will not prevent the hacker from seeing the contents of all your encrypted emails. Virtru stores encryption keys so a user doesn't have to walk around with the encryption key in the pocket. So, short version, you still need to use Multi-factor authentication.

Examples of email to encrypt - Anything with identifying client information, sensitive information, passwords, etc. Regulatory compliance

Process of encrypting emails - Very simple, just toggle the switch and add your settings. Virtru has some Data Loss Prevention (DLP) capabilities of detecting when a document is sensitive and turning itself on by default. MAP has not activated those features yet.

End-user experience - Those with Virtru Chrome extension installed can read emails directly in the gmail interface, while those without Virtru Chrome extension are directed to a web portal for viewing and interacting with email

Good, free alternative to Virtru - Gmail "Confidential Mode" and Bitwarden "Send"
Virtru email encryption settings

Disable forwarding - The recipient of your email cannot forward the email you send them.

Expiration Date - The recipient only maintains access to the email contents for the time permitted.

Watermark - Adds a watermark to attachments, mostly for preventing screenshots.

Persistent Protection - Insures that the recipient cannot give your document to an unintended 3rd party. The unintended 3rd party wouldn't be able to get a key to unlock the document.

https://support.virtru.com/hc/en-us/sections/360006689714-How-to-Use-Virtru-
Gmail confidential mode

Google Workspace has a “confidential mode” that replicates many of the features of Virtru that prevent Data Loss.

https://support.google.com/mail/answer/7674059?co=GENIE.Platform%3DDesktop&hl=en#zippy=%2Csee-how-confidential-emails-work
Encryption of temporary data using Bitwarden

Expiration Date - The Send will expire on the specified date and time. By default, Never.

Maximum Access Count - The Send will be disabled after the specified access count is reached. By default, unspecified.

Password - Require a password to be entered by recipients of this Send in order to gain access.

Notes - Enter private notes for this Send, which will only be visible to the Sender.

Disable this send so that no one can access it - Check this box to prevent this Send from being accessible to any recipients. You will still be able to interact this Send from your Send view.

End-to-end Encrypted: Data in a Send is encrypted on creation, and only decrypted when a recipient opens the Send link. The contents of a Send are stored encrypted in Bitwarden systems, just like a traditional Vault item. The link generated for each send doesn’t contain any data related to the Send’s contents, so it’s safe to share over intermediary communications services without exposing information to Bitwarden or any used intermediary services.

https://bitwarden.com/help/article/about-send/
Thank you! Any questions?

We are:

Angela Tripp, trippa@mplp.org, Co-Managing Attorney, MPLP

Scott Ellis, scoellis@mplp.org, IT Systems Administrator

Matt Olgren, molgren@lsscm.org, MAP Administrative Assistant/Desktop Support

Wilson Suprapto, wsuprapto@lsscm.org, MPLP Website Developer

And special guest, Michael Cunningham, mcunningham@lakeshorelegalaid.org, IT Technician at Lakeshore Legal Aid