Email Encryption

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."[1]
>
> "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 should be encrypted or sent through collaboration tools that send encrypted links rather than plain text data."[2]
>
> "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."[3]

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. **Protected Trust**: https://protectedtrust.com/ - this is easily my favorite option.

---

[1] 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.

[2] ibid., quoting Marco Maggio.

[3] ibid., quoting Steve Santorelli.

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

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

d. **Hightail**: https://www.hightail.com/ - this service was formerly known as YouSendIt.com. It's designed for sending enormous attachments, but also offers encryption for those attachments. Incredibly easy to use and inexpensive.

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

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

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

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

3. **Encrypt Email Attachments**: Word, WordPerfect and every good PDF program including Acrobat offers file encryption. This functionality is built-in so you only have to learn how to use it. With file encryption file simply cannot be opened without a password. You email could unencrypted and simply say "Please see attached." However, the attached file containing the sensitive information would be encrypted on its own.