1847Financial | HTK

Information handling best practices for financial professionals

As a financial professional, you interact daily with client and company confidential information. Not all information carries the same sensitivity and being aware of and adopting information classification is recommended to minimize risk associated with sensitive information in your business and when working with Penn Mutual and 1847Financial|HTK.

Please refer to our Penn Mutual Information Security's Information Classification Standard as an example on how our Company classifies information/data based on risk and value to the Company and to our policyholders, contract owners, all Company employees, financial professionals, and third parties.

Here are some common information handling best practices that you may encounter day-to-day to safeguard data that is entrusted to you by your clients.

Verbal Communication	• Communicate only needed data with authorized individuals. • Avoid being overheard by lowering voice or moving to a private area.
Email Being Sent Externally	• Consider if there is a safer method to send the information. • Choose an email provider that allows you to encrypt emails to protect confidential information in emails • Never place confidential information in the Subject Line. Subject lines for any email always appear in plain text when in transit. • Verify accuracy of email addresses of all intended recipients. • Confirm receipt via reply or telephone if warranted.
Email Received From External Senders	• If messages or attachments containing PII are received without encryption, contact the external sender to ensure future messages are encrypted or another safe method is utilized to send the information. • Do not click on links or open document attachments contained in email messages unless you are absolutely certain the email is safe. • Contact sender by calling phone number on file to verify email and report all malicious emails to your email provider.
Fax	• Remove unnecessary confidential information. • Telephone notification prior to transmission. • Telephone confirmation of receipt. • Incoming fax - physically wait at the machine. • Pickup fax confirmation pages in a timely manner. • Verify that information is not left on machine.
Social Media	• Prohibited from sending or posting confidential information at all times. • Printing and Data Destruction
Printing	• Print from a personally owned printer and/or on your private network. (Public Wi-Fi or network connections are not safe e.g. coffee shops, libraries, etc.) • Pick up all printed information in a timely manner - Verify that information is not left on printer.
Data destruction - Paper	• Shred all documents containing confidential information when no longer needed. • Don't place in trash cans or recyclables.
Data destruction - Old Devices	Technology has a lifecycle, just like does data. When you get a new technology, you often work on transferring data from the old device to the new device. However, it is equally important to ensure that the old device's data is properly handled to ensure it doesn't accidentally leak into other's hands. Often, the best thing to do is to physically remove and/or destroy the hard drive and/or storage device of any electronic device before recycling the device or selling it. This ensures that the data that was once stored on the device is no longer accessible.

For financial professional use only.

Last reviewed: 11/2024