Managing PPI

YouTube Video

What is PPI?

PPI stands for **Protected Personal Information**. Any client information than can identify that client to a third party is considered PPI. You may also see "PII" which stands for Personal Identifying Information. However, HUD standards refer to PPI, so that is the language that MDHA has chosen to use.

Types of PPI

PPI can include a client's name and/or a combination of any of the follow information:

- First and Last Name
- Date of Birth (DOB)
- Social Security Number (SSN)
- ZIP Code
- Project Entry & Exit Dates
- Address
- Phone Number
- Email Address
- Certificate and/or License Numbers
- Full Face Photos

Using and Sharing PPI

A **Data Breach** can be defined as any time one of the following occurs while you are accessing, using, or sharing PPI in either physical or digital forms:

Loss of Control, Compromise, Unauthorized Discloser, Unauthorized Acquisition or Access

Best Practices for Managing PPI

Use the reference table **Managing PPI: Best Practices** on Page 2 of this document to determine appropriate and inappropriate practices for managing client PPI.

NOTE: *Some of the lines in the table below have been emphasized in **bold** to bring attention to common or recurring issues noted by the HMIS Team. However, reading the entire document is very strongly encouraged, as failing to follow any one of these best practices could result in noncompliance during a Security Review by MDHA.*

Managing PPI: Best Practices

Use Type	Do	Do Not
Email	• **Attach PPI in a separate document.** • Password-protect or encrypt the document containing PPI. • Send the password or encryption code by separate communication.	• **Never email PPI to a personal email address.** • Avoid mentioning in the email subject that the email contains PPI. • Be careful when replying all. Ask yourself, who needs this information?
Hard Copy	• **Lock the file or cabinet drawer where hard copies are kept.** • Keep the room where files are stored locked when possible. • Shred documents that contain PPI when they need to be disposed of.	• **Never throw a client's file directly in the trash.** • Never leave documents out on desks, printers, copiers, etc. unattended. • Do not remove PPI hard copies from your work location.
U.S. Mail	• Seal all envelopes containing PPI. • Use opaque envelops or contains. • Use First Class or Priority Mail, or another traceable service, to track the mail and ensure it arrives at its intended location.	• Do not label the exterior of envelopes with "sensitive" or "confidential".
Websites & Shared Drives	• **Only use shared access software that can verify users and/or viewers.** • Use drives or networks that allow you to minimize access on a "need to know" basis.	• **Never use public sharing sites like Google Docs to access, store, or share PPI.** • Never share PPI on social networking sites. • Never send PPI in a Spiceworks help desk ticket to the HMIS team.
Accounts	• **Ensure your login and password information are protected and not accessible to anyone else** • Confirm the identity of anyone who may request or receive PPI from you digitally, especially via email • Pay attention to your accounts and update password regularly, or if you notice suspicious activity	• **Never allow your browser to save or auto-fill your password.** • Never share accounts, even with people you trust or people you report to. Logins and passwords must be unique and private • Avoid repeating the same username and password combination on multiple sites, as this makes your account less secure.