Best Practices in Data Management

Protecting Privacy Builds Trust & Improves Data Quality

Permissions & Passwords

Practice “Need to Know”

- Keep day to day reference files separate from sensitive personal history data
  - A client roster with names, numbers and addresses should be separate from a client list that includes treatment plans, diagnoses, or criminal justice system involvement

Password Protection

- Password protect electronics and specific files that contain personally identifiable information
- Do not store password on keychain or other password service
- Do not store your password in files or share electronically.
  - If someone needs access, give them a call!

Accessing Sensitive Files

- Make sensitive/private data entry permission based, so you know who has access at any given time
- Track when permission is given and when passwords are changed in a separate file.

Only a few people should have access to the client/client identifier key for sensitive data entry!

Everyone Makes Mistakes

Foster a workplace culture where staff feel comfortable to come forward with mistakes or ask questions.

- Early disclosure is essential to limiting damage from a data breach. People are less likely to report if they fear repercussions.
- Sometimes data needs to be entered twice, better to enter it twice than work off of low quality or inaccurate data
- Excel, and data in general, can be intimidating or frustrating. Onboard staff with hands-on training to identify points of confusion early.
- Focus on building up that skill set at a pace that doesn’t exceed someone’s frustration tolerance

No use crying over spilled milk!

RDA CONSULTING

40 YEARS of Systems Change

Best Practices in Data Management

Protecting Privacy Builds Trust & Improves Data Quality

On-Site Data Security

Researchers have rigorous data security requirements, consider adopting practices that work for your organization

- Secure paper documents in a locked cabinet, in a locked office, and keep track of who has keys.
- Retain paper documents for at least as long as you are collecting data. For context, many researchers retain documents for up to two years after the study concludes.
- Destroy documents with a “super cross cut” or “micro cut” shredder, or a secure shredding service. Document when various batches of documents are destroyed.
- Do not store documents or electronics in your car for longer than absolutely necessary
- Create a log and cadences for when documents are placed into a locked location
    - Regularly place paper copies in a locked cabinet at the end of each day or week, and log who is entering them.

HIPPA & Data Security Training

HIPPA Training is Your Friend!

- Even if you are not a healthcare provider or bound by HIPPA laws, HIPPA provides an excellent framework for limiting access to sensitive data.
- Check out this accredited, low-cost HIPPA training option
    - $15 State of California HIPPA Training Course

Avoid Phishing

- Ensure all staff know when and under what circumstances they would be required to release information.
- Only share information via encrypted email or other secure methods
- Keep a list of client email addresses to cross check suspicious emails against
- Check out free or low cost options for cybersecurity training
    - Cybersecurity Non-Profit

RDA CONSULTING

40 YEARS of Systems Change