

# Security & Confidentiality

# Security and Confidentiality

## Policies and Procedures



Division of Disease Prevention  
Office of Epidemiology  
Virginia Department of Health

# What is PHI

- Protected Health Information (PHI) is any individually identifiable health information including demographic data, (i) that relates to the individual's past, present or future physical or mental health or condition (pg.42).
- Can be in oral, paper or electronic form
  - Reports
  - Invoices/supporting documentation
- Types of information that could reveal the identity of a client if found
  - Name or initials
  - Date of Birth
  - Medical Record or Social Security numbers
- What else?

# Who has access to PHI?

*Anyone who comes in contact with confidential client information*

- Testing personnel?
- Patient Navigators?
- Data Entry Operators?
- Receptionists?
- Custodians/Janitors?
- Case Managers?
- Fiscal tech?
- Who else?

# How do you protect PHI?

- Data Communications pp.32-35
  - Only share confidential communication (written, verbal or electronic) on a strict need to know basis (pg.32).
  - Protect workstations, laptops and/or other devices
  - Protect user names/login names/passwords/codes
  - **Do not send confidential information by email**
- Computer/Data Security pp. 17-21
  - Ironkey thumb drive

# PHI Confidentiality Breach

- If someone in your agency is aware of a known or suspected breach it should be immediately reported to their supervisor, DDP contract monitor and the DDP director
  - Refer to guidelines: “Incident Handling Summary Procedures for Suspected Confidentiality Breaches (pg.48).”

End.