Fact sheet on:

What do we do to keep HIV data secure?

HIV data are kept secure as possible employing HIPAA, CDC, HIV epidemiology, and other health deport policies. These include, but are not limited to:

- Training staff at time of hire and annually thereafter
- Training includes signing of confidentiality oaths at least annually
- Adhering to a minimum use policy. Most data analyses are stripped of protected health information (PHI) such as names, phone numbers and medical record numbers
- Seeking to have redundant levels of security for the most identifying information (data kept in locked cabinet in a locked room in a keycard only access floor or data in a locked keycard access room kept in a hard drive in a locked safe and accessed only on a computer that is stand-alone (not connected to the internet)
- Limiting access to back of cubicles with signage for occasional users of PHI, secure room access for regular users. (This includes staff who regularly need to talk on the phone with PLWH or providers)
- Discouraging working at home on individual level data and never permit PHI data to be emailed or transferred without strong protection (encryption, pass phrase key sharing)