NC COALITION to end HOMELESSNESS

Keep HMIS@NCCEH Data Safe

Keeping electronic sensitive data isn't as easy as putting a lock on a file cabinet. We are entrusted to keep client identifying information (client names, Social Security Numbers, Dates of birth, etc.) safe. Follow these tips to protect sensitive data from theft and vulnerability.

Protect sensitive data

Use encryption when storing or transmitting sensitive data. Remove files containing sensitive data from your system when they are no longer needed. Remember that simply deleting files rarely means it's truly deleted permanently. If you store sensitive information on a flash drive or external hard drive, make sure to keep these locked as
well. Unsure about how to store, handle or remove sensitive data? Contact us!

Practice good password management

FACT: We have too many passwords to manage. It's easy to take short-cuts, like using simple passwords repeatedly to remember them, but this isn't safe. We highly recommend using long passwords with a strong mix of characters.
Update passwords frequently, and once you use a password, don't re-use it. Don't share your passwords or write them down.

Never leave your computer unattended

The physical security of your computer is just as important as its technical security. Do not let others access NC HMIS through your account. If you need to leave your computer- lock it so no one can use it. When finished using your computer, turn it off! Leaving your computer on and connected to the internet opens the door for nasty malware.

Keep software up to date

Operating system updates can be super annoying but they are necessary! These updates contain critical security patches that will help protect your computer from recently discovered threats. Failing to install these updates will put your computer at risk. Consider turning on automatic updates for your operating system. We recommend using web browsers such as Chrome or Firefox that receive frequent, automatic security updates. Be sure to keep browser plug- ins (Flash, Java, etc.) up to date, too.

Install anti-malware protection

Malware includes computer viruses, worms, spyware, scareware and more. It can be present on websites and emails, or hidden in downloadable files. The best way to avoid getting infected is to install good protection, do periodic scans for spyware, and avoid clicking on suspicious email links or websites.