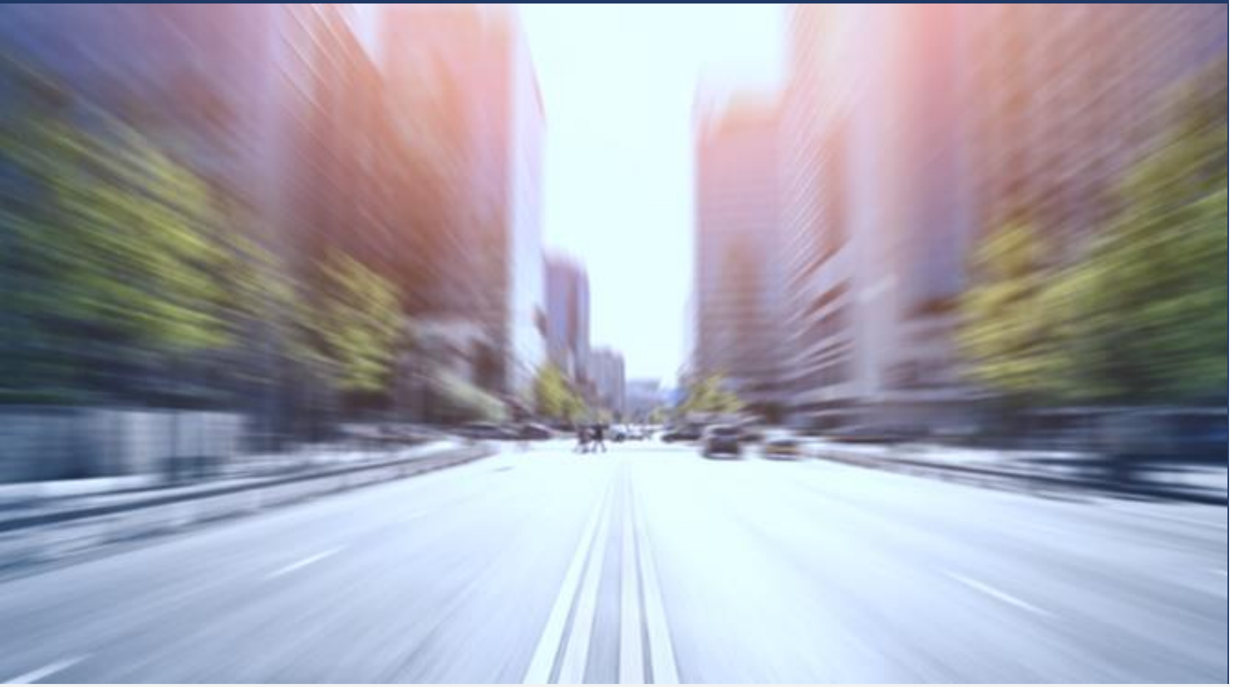
Secure PHI Transfer
Solutions & Technology



RRS MEDICAL

RRS MEDICAL | News Sprint

COVID-19
Working from Home with PHI

In Five Minutes or Less!

Sue Chamberlain, MSCTE, RHIA, CDIP, CCS-P

VP, Compliance and Education

Working from home does not have to increase the risk to PHI

We only covers SOME things for each individual to consider. Use critical thinking to ensure workspace fully protects patient rights.

*See your IT team for Technical specifics, e.g., encrypted e-mails, firewalls, virus protection, faxing PHI, VPN's, internet connection security.

- **Only work with PHI in your home**

  Even though, when allowed, it would be nice to work from the local coffee shop as a change of scene – Just Don't! Even if you work with your back to a wall, there are WIFI security concerns, or even just someone who grabs your computer.

- **Try not to transport any PHI unless protected**

  If you need to transport any paper with PHI for any reason, it should be secure. Electronic format should be password protected. Consider encrypted scanning for example. Do NOT leave documents or equipment in your car, not even for a few minutes

RRS MEDICAL

Keep PHI Safe – Always!

- Work in a private, closed location away from distractions and other family members

- Take more precautions than you may with co-workers;
  - —Clear your screen if anyone is nearby
  - —Logout when you walk away – even if just for a minute
  - —Ensure you completely log out from the company network when you are done.
  - —Keep your voice down (e.g., zoom, phone)
  - —Do not print! Don’t write down PHI. If you must, lock it up when not using it.
  - —DO NOT throw PHI in the trash. Use a shredder if you need paper or unprotected CD’s, etc.
  - —Never use Personal e-mail or forward to personal e-mail

Stay for Vigilant – Protect Your Laptop & Data

- Be vigilant against phishing and spear phishing
  - Do not open suspicious emails. Do not click on any emailed links if you are not completely sure are safe.
- Do not plug in mysterious drives
  - That thumb flash drive you found in a parking lot might actually be a front door into your secure system. Fight the urge to see what’s on it.
- Do not store any PHI on the remote computer or device
  - Do not save to Desktop, thumb drives or other areas. Work only within the systems.
- Password Protect your equipment
  - Create a separate password protected local user when using a shared computer. Do not record login information on or near the computer – EVER!

Remember Your HIPAA Training

- Reassess your security practices frequently.
  - —Don’t become complacent, reassess your own personal security practices on a regular basis.

- File an incident report for anything that may be found while working from home, just as you would in the office.

- Remember, HIPAA violations can result in fines ranging from $50,000-$250,000 with 1-10 years in prison. This can even increase depending on the amount of compromised information.

RRS MEDICAL

RRS
MEDICAL

www.rrsmedical.com

Empowering
Your Patient’s
Healthcare
Journey with
Innovation,
Security, and
Kindness