Remote Access Guidelines

When accessing your office computer from home, out of town or simply another location it is your responsibility to follow the rules and standards of the workplace while using remote access.

Federal laws require us to restrict unauthorized access to Protected Health Information (PHI).

State laws require us to protect unauthorized access to personal information that could be used to gain access to one’s personal financial information.

Immediately report all unauthorized disclosures that occur due to lost/stolen equipment (laptop or any hand held device), or lost/stolen documents.

**DOs**

**DO** make sure your Home PC/Laptop has an Anti-Virus program with current virus definitions installed.

**DO** make sure your Home PC/Laptop has the latest operating system updates installed. If you are using MS Windows, turn on the “auto-update” feature.

**DO** use a Virtual Private Network (VPN) connection each and every time you connect to sensitive school resources.

**DO** make sure patient information (PHI), and other sensitive information is NOT viewable by those NOT authorized to see it…..even your spouse, neighbor or children.

**DO** immediately report any unauthorized disclosures.

**DO** password protect ALL handheld devices, laptops, memory keys, etc.

**DO** encrypt all external media such as smart cards, memory keys, CDs/DVDs.

**DO NOTs**

**DO NOT** dispose of sensitive material in your personal trash unless you process them through a crosscut shredder. Better yet, bring all sensitive documents to the office and dispose of them in a Shred-it bin.
**DO NOT** access your data unless you are using a secure connection (i.e. VPN, SSL, Citrix, or other approved method).

**DO NOT** leave sensitive documents unattended in your home if other family members are present.

**DO NOT** leave PHI or other sensitive data unattended in a public place if you must step away.

**DO NOT** use public “hot spots” for internet access when working with PHI.

**DO NOT** discuss, share or expose your IDs or passwords with anyone.

**DO NOT** ask co-workers to leave PHI or sensitive information on your family’s voicemail.

Click here for a printable brochure of the information provided in this message.

If you have further questions, please reply to this message.