HIPAA

DO

- Discard Protected Health Information in appropriate shred container.

- Send securely (encrypt) when you have to include resident information in an email.

- Engage the screensaver when leaving the workstation unattended.

- Use automatic locks on desktops or any mobile devices. Always remember to log out.

- Ask questions of an individual you don't recognize who is accessing resident information.

- Use minimum necessary standard when accessing PHI.

- Utilize caution when speaking in areas where information may be overheard by others not directly involved in the care of the resident.

- Report all HIPAA concerns immediately to your supervisor, compliance official/officer, privacy officer or compliance hotline.

DON'T

- Share your passwords or login credentials with anyone.

- Browse residents' records without a valid reason, such as treatment and payment purposes.

- Leave paper on desk or counter that contains sensitive information.

- Post anything about residents, including pictures, on social media.

- Click on links embedded in emails if the sender isn't someone you know.

- Open email attachments from unidentified senders.

- Release anything to outside parties without authorization or approval of privacy officer.

- Text PHI unless through an encrypted system.

FSA
COMPLIANCE &
RISK MANAGEMENT