Sharing passwords is prohibited. Epic and other systems contain valuable health, financial, student, research, and other information. Who has access to these systems, and how is the information contained within protected? The first line of defense is providing access strictly on a need-to-know basis. The University utilizes a role-based model when granting access to business and health information systems. This ensures each individual is given access only to the information they need to do their job. Once access has been granted, the second layer of security is selecting a strong password. Every user is responsible for ensuring their password is strong and not easy to crack. Refer to UF’s [Password Complexity Standard](#) for password creation requirements. Finally, the University uses two-factor authentication to further secure accounts to address weaknesses with password only authentication. Password reuse must be avoided. Each user is responsible for the activity in every system to which they have been assigned.
Thank you for your attention and all your efforts in ensuring that the University of Florida continues to operate lawfully and ethically. Compliance is Everyone’s Responsibility!