HIPAA ALWAYS

- Use hospital equipment/cameras to take patient photos, not your cell phone
- Dispose of patient information in shredding/confidential bins, not regular trash
- Ensure Valid Authorization is signed when taking photos not for patient care (i.e., publications)
- Encrypt all internet-directed email containing ePHI
- Understand HIPAA definitions of PHI, Privacy Breach, Security Breach
- Be familiar with each hospital's HIPAA policies
- Obtain verbal permission from patient before discussing care in front of visitors
- Encrypt mobile devices containing PHI (phones, laptops, USB devices)
- Provide timely review and response to Record Amendment requests
- Report violations to Code of Conduct
- Lock your computer before you walk!

HIPAA NEVER

- Take patient records or notes off premises (e.g., hospital, clinic)
- Take/share patient photos with personal cameras or cell phones
- Discuss patient status or care in public places such as elevators, cafeterias, or hallways
- Leave patient information, including your own personal notes, unattended or in public view (e.g., conference rooms, whiteboards, lunch areas)
- Discuss patient care in front of visitors without patient permission
- Access patient records without a need to know (e.g., clinical, business)
- Leave patient information in your car – your car is not secure
- Share your login or password – you're responsible for anything done using your credentials
- Share patient information with anyone who does not have a "need to know" the information in order to do his/her job

When in doubt, ask!

303-724-0983 | ucdenver.edu/HIPAA

Health Insurance Portability & Accountability Act (HIPAA)

OFFICE OF REGULATORY COMPLIANCE

UNIVERSITY OF COLORADO
DENVER | ANSCHUTZ MEDICAL CAMPUS