**HIPAA Tips for Protecting Privacy and Security**

- Contact Security at 2-6262 if you see suspicious individuals in patient care or restricted areas.
- Wear your ID badge at all times.
- Discard documents containing patient information only in approved shredding containers.
- Discard disks, CDs, thumb drives, etc. containing patient information only in approved shredding containers.
- Use private areas to discuss PHI. Do not discuss patient information in cafeterias, elevators, or other public places.
- Lower voices when having conversations concerning patients in non-private areas.
- Report any suspicious activity appearing on your computer to the IS Help Desk at 2-3456 as soon as possible.
- Do not leave messages concerning a patient's condition or test results on voice mail. Do not leave messages containing highly confidential patient information (i.e. mental health, substance abuse, HIV/AIDS, genetic testing, etc.) on voice mail.
- Do not open unknown email attachments or unrecognizable emails.
- Do not access protected health information unless it is necessary to perform your job duties, including that of your friends, family members, and colleagues, and only then access the minimum necessary.
- Use private areas to discuss patient information with patients, family, or visitors.
- Access only electronic information that you “need to know” to perform your job; use the minimum necessary standard.
- Log-off or lock your computer screen when away from your workstation.
- Turn computer monitors away from the public so they cannot be viewed by unauthorized persons.
Guidance: HIPAA Tips for Protecting Privacy and Security

• Verify a caller’s identity or applicable patient access code before releasing patient information by phone.
• Lock laptop computers and other portable devices in secure location when not in use.
• Store passwords in secure areas and not accessible by others.
• Remove patient information from copy machines, fax machines, printers, or conference rooms.
• Obtain patient verbal permission before discussing information in front of family and friends.
• Never share your computer user ID or password with anyone.
• Do not access the PHI of family members, friends, or other individuals for personal or other non-work related purposes even if written or verbal authorization has been obtained.
• Medical records should not be taken away from the UC campus or off-site property.
• Clinic schedules, surgery schedules, and procedure schedules that contain PHI should not be left out in view of others. When no longer needed, schedules should be placed in approved shredding bins, not regular trash cans and recycle bins.
• If you do not need PHI to do your job, do not seek it out.
• If you overhear a conversation concerning a patient, keep it to yourself.
• Report all suspected privacy violations to the Privacy Program by calling (773) 834-9716 or emailing hpo@bsd.uchicago.edu.
• You can report issues anonymously by calling the toll-free HIPAA Resource Line at 1-877-440-5480, select option 2.

Any questions/comments/concerns please feel free to reach out to the Privacy Program at:

773-834-9716 or hpo@bsd.uchicago.edu