UnityPoint Health - Meriter
Information Security Agreement

Patient, financial, and other business-related information in any form, electronic or printed, is a valuable asset, and is considered private and sensitive. Employees, physicians, physician office staff, consultants, vendors, contracted agency staff, nursing faculty and students may have access to confidential information in the performance of their duties. Those charged with this responsibility must comply with applicable information confidentiality/security policies in effect at UnityPoint Health and its affiliates. This agreement applies regardless of the method of access used.

In consideration of being allowed access to UnityPoint Health information systems, I, the undersigned, hereby agree to the following provisions:

1. I agree to abide by all confidentiality/security policies and procedures for UnityPoint Health and its affiliates. I understand that such policies and procedures are available on the Intranet or have been provided directly to me.
2. I will not operate or attempt to operate computer equipment without specific authorization.
3. I will not demonstrate the operation of computer equipment or applications to anyone without specific authorization.
4. I agree to maintain a unique password, known only to myself, to access the system to read, edit and authenticate data. I understand that my unique password constitutes my electronic signature and that it should be treated as confidential information. I agree not to share my password with any other individual or allow any other individual to use the system once I have accessed it. I understand that I may change my password at any time
5. I agree only to access the patient, financial, and/or other UnityPoint Health business-related information needed for the performance of my duties and responsibilities. I understand that accessing my own patient record or the patient record of my family members is only appropriate to do via the patient portal or through the Release of Medical Information process. I agree that I will not use my access granted to me for my job role to look at my record or the records of my family members or others, unless it is in accordance with my professional job duties and responsibilities.
6. I will contact my supervisor, the affiliate compliance officer or Information Security Officer (ISO), or the IT department if I have reason to believe the confidentiality and security of my password has been compromised.
7. I will not disclose any portion of the computerized systems to any unauthorized individuals. This includes, but is not limited to, the design, programming techniques, flow charts, source code, screens, and documentation created by employees, outside resources, or third parties.

8. I will not disclose any portion of the patient's record except to a recipient designated by the patient or to a recipient authorized by UnityPoint Health who has a "need to know" in order to provide continuing care of the patient.
9. I understand that applications are available outside of the UnityPoint Health network via various remote access methods (i.e. Dial-up, VPN, Citrix, and/or Web), and I agree to abide by the following when accessing UnityPoint Health computer systems from remote locations:
    a. I will only access UnityPoint Health computer systems from remote locations if I am authorized to do so.
    b. I will use discretion in choosing when and where to access UnityPoint Health computer systems remotely in order to prevent inadvertent or intentional viewing of displayed or printed information by unauthorized individuals.
    c. I will use proper disposal procedures for all printed materials containing confidential or sensitive information.
    d. I understand that if I choose to use my personal equipment to access UnityPoint Health computer systems remotely, it is my responsibility to provide internet connectivity, configure firewall and virus protection appropriately, and to install any necessary software/hardware. UnityPoint Health is not responsible if the installation of software necessary for accessing UnityPoint Health computer systems remotely interferes or disrupts the performance of other software/hardware on my personal equipment.
    e. I understand that by using my personal equipment to access UnityPoint Health computer systems that my computer is a de facto extension of the UnityPoint Health network while connected, and as such is subject to the same rules and regulations that apply to UnityPoint Health owned equipment.
10. I agree to report any activity which is contrary to UnityPoint Health policies or the terms of this agreement to my supervisor, the affiliate compliance officer, or a security administrator.
11. If I will be using a mobile device to access the UnityPoint Health network or network services (through a personally-owned or UnityPoint Health-owned device) that include, but is not limited to, email, VPN, or other remote access capabilities, I will allow UnityPoint Health limited control of my mobile device for the protection of UnityPoint Health data and its assets. For this context a mobile device is currently identified as a mobile phone, tablet, or other miniaturized computing system. This limited control can include the enforcement of a password/pin and/or remote wiping of the mobile device in the event of loss or theft or other factors that may present a risk of harm to the UnityPoint Health network, its data, or applications.
12. I agree to comply with all relevant UnityPoint Health Compliance Policies, including but not limited to the Mobile Device Policy.
    a. I understand that I must sign this Agreement as a precondition to issuance of a computer password for access to patient information and that failure to comply with the preceding provisions will result in formal disciplinary action, which may include, but will not be limited to, termination of access, termination of employment in the case of employees, termination of agreements in the case of

contractors, or revocation of clinical privileges in the case of medical staff members, taken in accordance with applicable medical staff by-laws, rules and regulations.

b. In the event of loss or theft of my device, I agree to the remote wiping of all content on my mobile device, including any personal information I may have stored on the device, such as (but not limited to) photos, videos, and other content stored on the hard drive of the device.
c. In the event of an investigation or inquiry by the internal compliance department or the government, or in the event of litigation, I agree to provide UnityPoint Health and/or its affiliate(s) with access to my device to copy and retain information related to the investigation, inquiry or litigation. I understand that UnityPoint Health will take reasonable steps to limit access to personal information, such as using key word searches to identify relevant material.

I have read and understand the above. I understand that I must treat all patient, resident, client and customer (hereinafter defined as "patient") information with strict confidentiality and that I may access, review or disclose patient information only to the extent needed to perform my specific job functions and/or responsibilities. I also understand that breaching patient confidentiality could lead to disciplinary action up to and including termination and/or legal action. I further understand that my obligation to maintain patient confidentiality continues during the course of my clinical rotation at Meriter and thereafter.

_____ _____

Printed Name Signed Name

_____ _____

Unit and School (if applicable) Date

_____

Preceptor/Instructor (if applicable)

Original: Department File
Copy: Student