

Information Security Agreement

Revised 01/21

1. 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 home staff, students, and other authorized users may have access to confidential information in the performance of their duties. Those charged with this responsibility must comply with information confidentiality/security policies in effect at UnityPoint Health (UPH) and its affiliates. This agreement applies regardless of the method of access used.
2. In consideration of being allowed access to UnityPoint Health information systems, I, the undersigned, hereby agree to the following provisions:
3. I agree to abide by all confidentiality/security policies and procedures for UPH and its affiliates. Updates to state and federal regulations and/or risk mitigation concerns will prompt policy changes from time to time, and I understand it is always my responsibility to abide by the then-current UPH policies. I understand that such policies and procedures are available on the Intranet or will be provided to me upon request.
4. I will not operate or attempt to operate UPH computer equipment without specific authorization.
5. I will not demonstrate the operation of UPH computer equipment or applications to anyone without specific authorization.
6. I will not install or use software that is not licensed by UPH (or that is otherwise unlawful to use) on any UPH information systems, computer equipment, devices, or networks. I understand that unauthorized software may pose security risks and will be removed by UPH.
7. 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, and it is my responsibility to reset my password immediately if I suspect it has been compromised.
8. I agree only to access the patient, financial, and/or other UPH business-related information needed for the performance of my duties and responsibilities. I understand that accessing my own patient record or the patient records 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.
9. 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 account has been compromised.
10. 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.
11. 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 UPH who has a "need to know" in order to provide continuing care of the patient.
12. I understand that applications are available outside of the UPH network via various remote access methods (i.e. VPN, Citrix, and/or Web), and I agree to abide by the following when accessing UPH computer systems from remote locations:
13. I will only access UPH computer systems from remote locations if I am authorized to do so and from only locations in the United States unless I have received prior approval from UPH.
14. I will use discretion in choosing when and where to access UPH computer systems remotely in order to prevent inadvertent or intentional viewing of displayed or printed information by unauthorized individuals.
15. I will use proper disposal procedures for all printed materials containing confidential or sensitive information.

16. I understand that if I choose to use my personal equipment to access UPH computer systems remotely, it is my responsibility to provide internet connectivity, configure firewall and virus protection appropriately, properly maintain security patches, and to install any necessary software/hardware. UPH is not responsible if the installation of software necessary for accessing UPH computer systems remotely interferes or disrupts the performance of other software/hardware on my personal equipment. UPH will restrict personal devices from connecting to UPH information systems if security posture checks do not pass.
17. I understand that by using my personal equipment to access UPH computer systems that my computer is a de facto extension of the UPH network while connected, and as such is subject to the same rules and regulations that apply to UPH owned equipment.
18. If I will be using a mobile device to access the UPH network or network services (through a personally-owned or UPH-owned device) that include, but is not limited to, email, VPN, or other remote access capabilities, I will allow UPH limited control of my mobile device for the protection of UPH 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 UPH network, its data, or applications.
19. I understand using the talk-to-text feature built into the mobile device, like Siri, is not HIPAA-compliant, and I agree to avoid using talk-to-text features if patient information is included unless the talk-to-text tool has been specifically approved by UPH IT.
20. In the event of loss or theft of my personal 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.
21. In the event of an investigation or inquiry by the internal compliance department at UPH or the government, or in the event of litigation, I agree to provide UPH 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 UPH will take reasonable steps to limit access to personal information, such as using key word searches to identify relevant material.
22. I understand the UPH computer systems are intended to be used for business purposes with limited personal use, such as saving a family picture or my resume, is permitted. If I chose to save my personal files or emails on UPH computer systems, I will save them in a folder clearly marked "personal". I understand that upon my departure with the organization, all business-related emails and files that are not clearly saved in my "personal" folder may be transferred to my manager or their designee in order to continue business operations.
23. I understand that UPH regularly audits access to UPH computer equipment, applications, and the data contained in these systems. I agree to cooperate with UPH regarding these audits or other inspections of equipment and data, including UPH inquiries that arise as a result of such audits.
24. I agree to report any activity which is contrary to UPH policies or the terms of this agreement to my supervisor, the affiliate compliance officer, or to the IT Service Center at 800-681-2060.

I understand that I must sign this Agreement as a precondition to issuance of a computer password for access to the UPH network and/or 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.

Signature:

Date:

Email Address:

Your Date of Birth:

Last 4 digits of your Social Security Number: