UNIVERSITY MEDICAL CENTER, INC.

University of Louisville Hospital / James Graham Brown Cancer Center

Volunteer Confidentiality Form
Confidentiality and Acceptable Use Agreement

Employee Notice, Acknowledgement and Certification of Signature

Electronically submitting a response to statements made below constitutes an electronic signature. Any record containing an electronic signature shall be deemed for all purposes to have been signed and will constitute an original when used or printed from electronic records established and maintained by UMC or its agents in the normal course of business and /or as a part of its Corporate Responsibility Program. By clicking "Submit" below, you attest that you have read, understand and voluntarily agree to provide your Acknowledgement by electronic signature. Please note that prior to completing this section and the final submission of your responses, you may change any of your responses or cancel your agreement/authorization to provide your Acknowledgement by electronic signature. Once submitted however, your agreement to provide Acknowledgement by electronic signature cannot be canceled.

University Medical Center treats information about UMC business and about individuals such as the patient or resident and their families, and employees as confidential and take precautions to protect the privacy, confidentiality, and security of this information. UMC confidential information means any information regardless of the format that it is in (for example, paper, electronic, oral conversations, films) about a patient, resident, employee, student, physician, professional staff, or UMC business and financial operations that is not available to the public. Confidential information includes, but is not limited to, protected health information, billing, payroll, employment records, employee benefits, trademark, copyright, intellectual property, technical ideas and inventions, written published works, contracts, supplier lists and prices, price schedules, business practices, marketing, or strategy, confidential information of third parties for business purposes, or information that is only intended for internal use.

During the course of your employment or association with UMC, you may have access to UMC confidential information. In order to access confidential information you must read the following statements and conditions and indicate you intent to comply.

I understand

I will look at and use only the confidential information I need to perform my job duties such as to provide health care for a patient, resident, member or other individuals, or to perform UMC business related job duties.

I understand and agree

I will not look at confidential information that I do not need to perform my job, for my own personal benefit or profit, for the personal benefit or profit of others, or to satisfy personal curiosity, or to disclose or divulge confidential information to others.

I understand and agree

I will not share confidential information with anyone who is not authorized by UMC to have access to it. If my responsibilities include disclosing confidential information with outside parties such as healthcare providers, contractors, consultants, or insurance companies, I will follow CHI policies and procedures for these types of disclosures.

I agree

I will take reasonable precautions and follow UMC policies and procedures for safeguarding confidential information to prevent the unauthorized use or disclosure of confidential information.

I agree

I will ensure that confidential information that I no longer need will be returned and maintained in the appropriate UMC department or location, or in accordance with UMC policies and procedures.

I agree

I understand that passwords, verification codes, or electronic signature codes assigned to me are the equivalent to my personal signature; and

> I will only use my password, verification or electronic signature code, in accordance with UMC policies and procedures;
> I will not use the password, verification or electronic signature code of other UMC employees or individuals authorized by UMC to have such password, verification or electronic signature code;
> I am responsible and accountable for all entries made and retrievals accessed using my password, verification or electronic signature code regardless of whether it is used by me or by another individual; and
> I will not use my password, verification or electronic signature code after my employment or affiliation with UMC ends.

I understand and agree

If I become aware that another individual has access to or is using my password, verification or electronic signature code or is using his/hers or another individual's password, electronic signature or verification code improperly, I will immediately notify my direct supervisor or the UMC Privacy Officer.

I agree

I understand that my obligation to maintain the confidentiality of UMC's confidential information extends beyond termination of my employment or association with UMC, and I agree that I will not disclose or use UMC confidential information for any purpose after my employment or association ends.

I understand

During the course of my employment with UMC I may need to have access to information systems, applications, and information technology network infrastructure (UMC IT Assets) to obtain and use UMC information for my job duties. In order to obtain and maintain access privileges to UMC IT Assets I agree to read the following statements and conditions and indicate my intent to comply with UMC policies and procedures and this Confidentiality and Acceptable Use Agreement.

I understand
I am responsible for complying with the UMC Acceptable Use Policy. If I have any questions about my use of UMC IT Assets I am to ask my immediate supervisor and/or the IT Help Desk for assistance. The Acceptable Use Policy is available on Inside UMC or from my manager.

I understand and agree

I understand that UMC maintains ownership of UMC IT Assets and the UMC Information contained on these IT Assets. UMC Information includes information that I may create, access, or obtain on behalf of UMC.

I understand

I am not permitted to install or remove any software on UMC IT Assets. If I need specific software for specific job duties, I will request services from IT Help Desk to install or remove such software.

I agree

I am responsible for complying with software licensing, copyright, and patent requirements, and the laws which protect these rights. I understand that I am not permitted to download, reconfigure, or reverse engineer any software that UMC uses with its IT Assets.

I agree

I am responsible for handling UMC Information in such a manner as to prevent unauthorized use or disclosure of UMC Information. I am also responsible for preventing unauthorized access and use of UMC IT Assets reasonably within my scope of influence, including, but not limited to, taking additional physical precautions to protect IT Assets such as logging out of my computer when not in use, and physical protection of IT Assets to prevent theft or loss, such as with mobile devices and laptop computers.

I understand and agree

I am responsible for securing UMC Information when it is used and disclosed electronically, such as using encryption when sending confidential information.

I understand and agree

I am responsible for knowing and following the UMC defined acceptable uses of the Internet, email, Instant Messaging, file transfer, and proper data storage as set forth in the UMC Acceptable Use policy.

I understand and agree

I am responsible for protecting UMC IT Assets, including my company computer, from viruses and the introduction of malware. If I have any questions or concerns about unknown emails or Internet web sites, I will contact the ITS Help Desk for assistance.

I understand and agree

I am responsible for securely protecting any mobile device(s) I use to access UMC change/Outlook (email, calendars and contacts) or other UMC systems or applications and the information stored on such a mobile device in accordance with ITS Security Standard ITS13-S8 Mobile Device Security. This requirement applies to all UMC Workforce members (including, but not limited to, full-time employees, part-time employees, physicians and physician groups, clinicians and clinician services, trainees, students, volunteers, contractors, consultants, vendors, temporary workers) and includes mobile devices owned by a UMC, an individual, or a third party. The Mobile Device Security Standard can be accessed on Inside UMC or a copy can be obtained by contacting my manager.

I am responsible for complying with the Mobile Device Security Standard as it applies to my use of a mobile device to access UMC information. If I have any questions about my use of a mobile device to access UMC Systems and applications, I am to ask my supervisor and/or ITS Service Desk for assistance.

I understand and agree

I am responsible for adherence to the conditions contained in the Mobile Device Security Standard. This requirement applies to all CHI Workforce members, regardless if an individual currently accesses UMC Exchange/Outlook or any other CHI systems or applications. I may access the Mobile Device Security Standard on Inside CHI or from my manager.

I understand and agree

I acknowledge that if my mobile device receives 10 attempted login failures, then the information contained on the mobile device will be deleted. I acknowledge that the information includes UMC Information and my personal information.

I understand

If my mobile device is lost or stolen, I will immediately report this to the UMC ITS Service Desk and I grant UMC permission to conduct a remote wipe of the mobile device. I acknowledge that the remote wipe may remove my personal information and applications on my mobile device.

UMC's policy on remote wiping of UMC information contained on personal devices does not apply to an employee who has not been granted access to UMC Exchange/Outlook (email, calendars, and contacts) or other UMC IT systems or applications, or otherwise does not maintain UMC Information.

I understand and agree

Upon my resignation or termination of my employment or association with UMC, I grant UMC permission to de-provision my personal mobile device; or if the mobile device is

owned by UMC, I will return it. I acknowledge that de-provisioning will remove and wipe all UMC Information and that my personal information that is maintained on the mobile device may be deleted, including my personal photographs, calendar, and address book.

UMC's policy on remote wiping of UMC information contained on personal devices does not apply to an employee who has not been granted access to UMC Exchange/Outlook (email, calendars, and contacts) or other UMC IT systems or applications, or otherwise does not maintain UMC Information.

I understand and agree

I will immediately report any security incident involving UMC IT Assets to the ITS Help Desk regardless of how insignificant I may think the incident is.

I agree

I understand that UMC:

Issues user identification and secure passwords to access confidential information that is maintained electronically; regularly monitors access and use of UMC confidential information to determine my compliance with UMC policies and procedures and the terms of this Agreement;
and will monitor my access, use, and transmission of information on UMC IT Assets.

I understand

I understand that I do not have, and should not expect any personal privacy rights when using UMC IT Assets.

I understand

I understand and agree to abide by the obligations of this Confidentiality and Acceptable Use Agreement and associated UMC policies and procedures related to privacy, information security, information technology and confidentiality. I understand that UMC may take disciplinary action if I do not abide by the UMC policies and procedures, including up to termination of my employment, contract, or association with UMC.

I understand

I understand that UMC is entitled to take legal action against me, including seeking money damages, if I do not follow UMC policies and procedures or if I inappropriately use or disclose UMC's confidential information.

I understand

I understand that agreeing to comply with the Confidentiality and Acceptable Use of UMC IT Assets Agreements and related UMC policies and procedures to protect confidential information is not an employment contract. I understand that these policies and procedures may be revised or amended at any time and I will be made aware of the updated policies and procedures.

I understand

I understand that by responding and submitting an answer to any of the questions above I am consenting to provide by Acknowledgement and Certification of the applicable statement(s) by electronic signature. I understand that by responding and submitting an answer to any of these is the equivalent of actually “signing” my name to the statement(s) that precede(s) it. My electronic signature will constitute my “original” signature as well as my Acknowledgement and Certification of the applicable statement(s) when used or printed.

I understand

I understand that I may access a copy of the Privacy and Security Policies and Standards including the Mobile Device Security Standard on Inside UMC or from my manager.

I understand

I understand that I may also choose to print a copy of this Confidentiality and Acceptable Use Agreement now by pressing CTRL+P on my keyboard. A signed copy of this agreement will be maintained in my LEARN Transcript and can be printed at any time by clicking on “View Certificate.”

I understand

_____

Volunteer Name

_____

Date