# Visiting Rotator Application

*This form must be completed and submitted to Lynn.Romer@uchealth.com with required documentation attached and all signatures obtained no less than 30 days prior to the rotation start date.*

***Trainee Information***

First Name: _____ Middle Initial: _____ Last Name: _____

Email: _____ Phone: _____ Pager: _____

Degree: _____ Date of Birth: _____ SSN: _____ NPI: _____

Medical School: _____ Graduation Date: _____

PGY: _____ Ohio License/Training Certificate: _____ Expiration Date: _____

ECFMG # (if applicable): _____ ECFMG Issue Date (if applicable): _____

Have you trained in EPIC as an EMR? Yes: ☐ No: ☐

***Sponsoring (Home) Institution***

Home Institution: _____

Current Program: _____ Coordinator Name: _____

Coordinator Email: _____ Coordinator Phone: _____

***Participating Site (UCMC) Information***

Rotation Department: _____

Supervising UCMC Physician(s): _____

Rotation Start: _____ Rotation End: _____

Have you rotated here before? Yes ☐ No ☐ If yes, what program? _____

This certifies that Dr. _____ (trainee) is in good academic standing in the aforementioned training program. Our Graduate Medical Education Office has verified their qualifying credentials in accordance with Joint Commission and applicable regulatory standards, including standard background checks prior to employment. This resident/fellow is fully covered by health and malpractice insurance, has current training certificate or license to practice medicine in Ohio, all immunizations are up to date, is in compliance with UCH standards for TB testing and immunization, has completed training in Universal Precautions, Bloodborne, and Airborne Pathogens within the past year, complies with OSHA standards, and received training with respect to the HIPAA standards for patient confidentiality and privacy.

Home Institution Program Director (signature): _____

Home Institution Program Director (printed): _____ Date: _____

UCMC Program Director (signature): _____

UCMC Program Director (printed): _____ Date: _____

# Required Attachments

The following documents are **REQUIRED** & **MUST** accompany the rotator application.

Forms Below:

- Authorization for Release of Health Information
- Confidentiality and Data Security Agreement

Additional Attachments:

- Medical School Diploma (include translation if applicable)
- ECFMG Certificate (if foreign medical diploma)
- Ohio Medical License/Training Certificate from State Medical Board website
- Current Curriculum Vitae (CV)
- Copy of Malpractice Insurance
- Influenza Vaccine Documentation (if rotation occurs between 11/1 and 3/31)
- Digital Photograph in .jpg Format
  **Please send this photo as an additional attachment. It will be printed on trainee badges and uploaded to MedHub.*

# Authorization for Release of Health Information

Name: _____
Maiden Name: _____
Address: _____
Phone Number: _____
Birthdate: _____ Social Security Number: _____

I authorized the use of disclosure of the above named individual's health information described below.

Organization making disclosure: _____
Information may be disclosed to: _____
Address: _____
For the purpose of: _____ dates of visits: _____

**Place an (X) to indicate the information to be released:**

| | | | |
|---|---|---|---|
| Drug Screen Results | ☐ | Physician Reports | ☐ |
| Immunization Records | ☐ | Therapy Reports | ☐ |
| Chest X-Ray Report | ☐ | Consultation Reports | ☐ |
| Titer Results | ☐ | Other | ☐ |
| TB Test Results | ☐ | | |

I understand that I have the right to revoke this authorization at any time by sending a written revocation to Alliance Employee Health 3200 Burnet Avenue Cincinnati, Ohio 45229. I understand that the revocation will not apply to information that has already been released in response to this authorization. Unless otherwise revoked, this authorization will expire on your date of termination.

I understand that authorizing the disclosure of this health information is voluntary and Employee Health will not condition the provision of treatment or payment to me on the signing of this authorization, except for the provision of research related treatment to me in the signing of this authorization for the use or disclosure of my personal health information for such research.

I understand that authorizing the disclosure of information carries with it the potential for an unauthorized redisclosure and the information may not be protected by federal confidentiality rules.

I understand that my health record may include information related to alcohol and/or drug dependence abuse, behavioral or mental health conditions, acquired immunodeficiency syndrome, or human immunodeficiency virus. This release is sufficient for release of drug/alcohol diagnosis and treatment and HIV test results or diagnosis.

_____ _____
Patient or Representative Date

_____ _____
Relationship to Patient Witness

CONFIDENTIALITY AND DATA SECURITY AGREEMENT

Vendor Acknowledgement of Requirements of All UC Health Contractors or Non-Employees Regarding Protected Health Information (PHI) and Confidential Information

The services provided by UC Health for its patients and other customers are highly confidential and must not be released, disclosed or discussed with unauthorized individuals or organizations. There are both Federal and State Laws that protect the privacy and confidentiality of PHI and other confidential information from unauthorized access, use or disclosure.

Vendor acknowledges that by signing this agreement on behalf of its employees, who will use or access UC Health systems or perform their duties within UC Health facilities, that there may be legal, ethical, and personal ramifications to those employees for violating its terms. **Vendor employees who will not access or use UC Health systems or perform their duties within UC Health facilities are not subject to the terms of this agreement.**

Confidential information includes, but is not limited to, information about a patient's condition, treatment or payment for services, aggregate clinical data, employee records, processes, marketing plans or techniques, product or service plans, strategies, forecasts, customer/patient lists, supplier lists, discoveries, ideas, pricing policies and financial information. This confidential information can be obtained through a variety of means including seeing or hearing it, access to computer systems or access to it in paper or other electronic form.

Vendor agrees to the following on behalf of those employees who will have access, use, create, or maintain UC Health confidential information when using or accessing UC Health systems or performing their duties within UC Health facilities. Furthermore, vendor agrees to educate affected employees on these requirements.

**If accessing or having access to PHI whether incidental or intentional, acknowledge and agree:**

- **Examination of their own records, family member records or others for nonwork related purposes is not permitted and is a violation of UC Health policy.**
- UC Health HIPAA policies on privacy, confidentiality, and security govern the appropriate access, use, and disclosure of PHI. Vendor may request such policies be provided or made available to vendor employee.
- All UC Health workforce and system users have access to UC Health policies.
- Access, use or disclose only PHI for which they are authorized through their work for, or associated with, UC Health and as complies with UC Health HIPAA policies.
- Not to invade patient privacy by examining PHI or data for inappropriate review.
- Not to discuss PHI in unauthorized areas such as hallways, elevators, and cafeterias, where it could be overheard.
- Not to make unauthorized disclosures, copies, or transmissions of PHI in any form including electronic transfer of PHI to personal devices.
- Access to PHI for research purposes requires proper documentation and approval according to HIPAA policies.
- The use of interconnect functionality, e.g. Epic Care Everywhere, to retrieve or access PHI from non-UC Health hospitals for the purposes of research study participant recruitment is strictly forbidden. Interconnect functionality is limited to treatment, billing, or healthcare operations.

**If using UC Health provided accounts agree:**

- To keep passwords confidential and not share it (them) with any individual or allow any individual to access information through their user account(s).
- That giving a password to an unauthorized individual may result in account access termination.
- User account(s) may identify information that vendor employee has accessed, and such access may be monitored and audited.
- Their password will change in accordance to UC Health's requirements.

**If having access to UC Health data in any format or method, acknowledge and agree:**

- To protect data at all times – during its origin, entry, processing, distribution, storage, and disposal. This includes data in electronic, paper, film, video, or other forms.
- To protect data from unauthorized access (accidental or intentional), modification, destruction or disclosure.
- To never attempt to discover and/or divulge private, confidential, or protected patient, employee, business or computer systems information without expressed written and/or verbal direction from appropriate management personnel, Information Security, or the Privacy Office.
- UC Health data used in business and clinical operations is an asset of UC Health and must be protected from unauthorized access at all times.
- UC Health uses security systems or controls to protect its computing environment and this information should only be disclosed on a need to know basis. This includes the names of the systems used and any settings or configurations.
- Information accessible within any of the UC Health electronic communication and collaboration systems (e.g. Email, Teams, Voicemail, SharePoint, The Link, OneDrive, Shared Drives, etc.) is the property of UC Health and its member institutions and may be monitored.
- To access only those specific elements of information for which I have been authorized as part of my job responsibilities.

**If using / accessing UC Health technology, acknowledge and agree:**

- They should have no reasonable expectation of privacy when using any UC Health electronic communication or collaboration system, including the Internet and that usage of these systems may be monitored at any time and their usage or access of one or more of these systems may be restricted at any time.
- Should they have access to the Internet, it is provided by UC Health to assist in completion of work assignments (i.e. patient care, research, education) and that this access should be considered an extension of their work environment.
- Never intentionally harm UC Health computer hardware, software or application systems and further acknowledge and agree:
  - The use of unlicensed or unapproved software constitutes a serious risk to UC Health operations.
  - Not to install or use any software without obtaining proper approval from IS&T Information Security.
  - Never to attempt to circumvent the computer security system by using or attempting to use any unauthorized transaction, software, files, or resources.
- To always obtain permission from IS&T management and/or IS&T security administration before investigating suspected security threats, problems, or other related abnormalities outside areas of responsibility.
- Never to use UC Health computing resources for:
  - Personal gain or advantage,
  - Illegal or immoral activities,
  - Anything that knowingly impedes the performance of information technology resources,

- Significant personal communications via e-mail, online chat, or voice, including sending non-business e-mail to a large number of recipients,
- Downloading and/or storage of personal collections of software, pictures, sound, or video,
- Solicitation of products or services including, fund-raising for any causes, union activities, and/or non-UC Health sponsored events,
- Hacking, cracking, or related activities, including using or installing software for any of these purposes except when authorized by IS&T management or IS&T Information Security.

- To always report to management any activities suspected or observed which in any way could be threatening or detrimental to UC Health, its patients, employees, or resources, including information systems.
- To refuse any request believed to violate any of these agreed to terms and notify the UC Health Compliance Line should they have any such concerns.

**Upon completion of the work assignment vendor employees will**:

- Lose ability to access UC Health information.
- Not attempt to access UC Health systems or disclose any confidential information and/or PHI to any person or entity.
- Return or destroy any UC Health confidential information, including PHI, which is no longer needed as part of the UC Health relationship with the vendor.
- Continue to honor all of the applicable obligations mentioned above after termination of vendor contract or end of work with UC Health.

**Acknowledges the implications of inappropriate use, access, or disclosure:**

- UC Health reserves the right to immediately terminate access to UC Health systems if there is inappropriate access to PHI or other sensitive data.
- Unauthorized access, use, or disclosure may have serious legal repercussion for themselves and/or their employer.
- Unauthorized access, use, or disclosure of PHI may subject them and/or UC Health to Federal and State fines and penalties.
- Access to PHI for illegal purposes will subject them to prosecution to the fullest extent of the law.

Vendor has read this document and acknowledges that signature of an authorized representative constitutes acceptance of the terms of this agreement and that a violation of it can result in permanent termination of all UC Health access by vendor employee. Vendor acknowledges such violation may also constitute a breach of one or more terms of the contract between UC Health and vendor.

Name (Print) Organization (Print)

Signature Date of Signature