Personal Attestation for Research Electronic Health Record Access

Electronic Health Record (EHR) access for certain researchers will require the Principal Investigator* (PI) of the research to personally attest to the Researcher's qualifications and need for access, and the measures in place to ensure compliance with relevant regulations and policies. The personal attestation may be in the form of a letter, email, or documented conversation/phone call with a member of the Health Information System Access Review Committee (HISARC).

*The attestation should come from a credentialed provider on the Medical Staff at OSUWMC. If the PI does not fulfill these requirements, the attestation can come from a supervisor or co-investigator who does meet these criteria.

The information requested and documented should include:

- For visiting scholars, his/her home institution and the arrangement that has been made for his/her visit here
- For students, where the student is attending school and course of studies (major)
- Name and title of person who will be directly supervising him/her
- Description of the activities the Researcher will be involved in
- Description of any payment the Researcher will receive
- Expected duration of his/her involvement in research, including an end date when known
- Justification for access requested and reasoning as to why this is the minimum necessary amount of access needed to perform the research
- Confirmation of understanding that the supervisor will be directly responsible for the Researcher's actions
- If the Researcher is not credentialed to practice medicine in the state of Ohio, that he/she will not participate in the patient's routine clinical care
- If the Researcher will be directly interacting with patients, he/she will have vaccinations as required by the medical center
- A statement that the Researcher will complete the annual "HIPAA Privacy and Security" eLearning and "HIPAA Privacy and Research" eLearning prior to starting work in their role
- A statement about how the information will be kept secure on electronic devices (i.e., only using encrypted devices, stored within the firewall);
- Any past issues with HIPAA compliance and/or any experience with HIPAA compliance
- Any deterrents for HIPAA violations