COMPLIANCE OFFICE
UNIVERSITY OF MICHIGAN HEALTH SYSTEM

UMHS COMPLIANCE OFFICE AUDIT OF ACCESSS MEMORANDUM

To: Human Resources Representative Staff / Office of Clinical Affairs
From: University of Michigan Health System Compliance Office
Re: Audit of Access Report / Required Investigation
File Number: COMPL-_____
User Name: _____

Attached is an Audit of Access Report. This report shows that the above User accessed or is believed to have accessed the electronic medical record (EMR) of a particular patient. Access to the patient's EMR may or may not have been appropriate, depending on the individual User's role/responsibilities. This Audit of Access Report requires your review and investigation in accordance with the following steps:

Step 1: Initial Review by Supervisor/Manager: The User's Supervisor/Manager must review the access to make an initial determination as to whether the access may be appropriate. *Note:* If necessary for investigation, the Supervisor/Manager *is* permitted to access/review the patient's EMR.

a. If the Supervisor/Manager determines the User's access is appropriate: The Supervisor/Manager must complete and sign immediately below.

I have followed the steps above and attest that the determination was made that the User's access to the patient's electronic medical record was appropriate as part of the employee's job responsibilities.	
Manager/Supervisor Name (print): _____	Title: _____
Manager/Supervisor Signature: _____	Date: _____
Return the signed attestation to the UMHS Compliance Office via e-mail at Compliance-group@med.umich.edu or via Fax at 734.936.4917.	

b. If Supervisor/Manager cannot determine if access is appropriate: If the Supervisor/Manager cannot initially determine a legitimate job-related reason for the User's access to the patient's/patients' EMR, continue to Step 2 below.

Step 2: Interview User: If the Supervisor/Manager cannot initially determine a legitimate job-related reason for the User's access to the patient's/patients' EMR, then the HR Rep or Office of Clinical Affairs, as applicable, and the Supervisor/Manager must interview the User.

Attachment A: Explanation of HIPAA Confidentiality Obligations and Acknowledgement

a. Explain and Discuss Attachment A to the User - See Attachment A entitled "*Explanation of HIPAA Confidentiality Obligations"*.
   i. Two copies of Attachment A are provided. The user should be requested to sign and date Attachment A both copies. User's signature is an acknowledgement that he/she received explanation and a copy of Attachment A.
   ii. Give one copy of signed/dated Attachment A to the User.
   iii. Submit one copy of the signed/dated Attachment A to the UMHS Compliance Office (via e-mail at Compliance-group@med.umich.edu or via Fax at 734.936.4917.)

   Note: If User refuses to sign Attachment A, the Manager must sign and date the Attachment with a notation that the document was reviewed and discussed with the User, but User refused to sign the acknowledgement. The Manager then submits the signed acknowledgment to the UMHS Compliance Office.

b. If the User cannot provide an explanation for his/her access: If User cannot provide a reason for the access that is legitimately related to the User's role/job responsibilities, then the access could be considered inappropriate and deemed a privacy violation under the Health Information Portability & Accountability Act (HIPAA). Disciplinary action steps are taken in accordance with UMHS Policy 01-04-390, Discipline for Violations of Privacy or Security of Protected Health Information (PHI) or Other Sensitive Information for All UMHS Workforce, available at http://www.med.umich.edu/i/policies/umh/01-04-390.htm, as well as any applicable collective bargaining agreement.

Patient privacy is important to us. We thank you for your assistance with investigating and handling this matter. Please contact us at 734-615-4400 if you have any questions or require assistance.

Attachment A: Explanation of HIPAA Confidentiality Obligations and Acknowledgement

The individual whose access to the electronic medical record (EMR) system is being discussed (User) is requested to sign below acknowledging the receipt of HIPAA confidentiality education and this document. It will be kept by the UMHS Compliance Office to show compliance with HIPAA's education and mitigation requirements. Two copies are provided. Return one to the UMHS Compliance Office and give one copy to the User.

WHAT IS HIPAA? The Health Information Portability & Accountability Act (HIPAA) Privacy Rule is a Federal law that establishes national standards to protect individuals' medical records and other personal health information. HIPAA applies to health care providers and members of its workforce, including those who have access to the health care provider's electronic medical record (EMR) system.

Penalties for HIPAA Violations: Individuals who violate HIPAA can be subject to both *civil and criminal penalties,* which can include significant fines (up to $1.5 Million per HIPAA violation per year) *and imprisonment up to 10 years.* These penalties can be applied for individuals who have "knowingly" obtained or disclose individually identifiable health information, who committed offenses under false pretenses and/or who committed offenses with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm.

Inappropriate Access to the EMR violates HIPAA: HIPAA sets rules and limits on who can look at a patient's EMR. Inappropriate access to one/more patient's EMR is a violation. Any confirmed inappropriate access to one/more patient's EMR is a HIPAA violation.

Auditing EMR Access & Discussion with User: Audits of access to the EMR system are conducted by the UMHS Compliance Office. Sometimes, it is not clear whether one or more accesses to one or more patient records are appropriate. When this happens, a discussion with the User is conducted to determine if the User can explain the accesses to those records. The User is expected to be truthful about his/her accesses.

We also use this discussion as an opportunity to further educate the User about appropriate and inappropriate accesses to the EMR System.

If There Is Inappropriate Access: If inappropriate access is believed to have occurred, mitigation steps are taken to prevent further potential HIPAA violations. The User is asked whether the patient information was disclosed by the User to any other person(s) and the circumstances of such disclosure. For example: If the User accessed a patient's record and subsequently told a friend or a family member about that patient's information, the User is expected to inform his/her Supervisor about that disclosure and the circumstances of that disclosure.

The User is also informed that while sanctions may be issued under the UMHS Disciplinary Action policy for Privacy and Security Violations and any applicable collective bargaining agreement, the User continues to be subject to HIPAA and is required to maintain the confidentiality of all patient information and not inappropriately access, inappropriately use and/or inappropriately disclose any patient information in the future.

ACKNOWLEDGEMENT: The UMHS Compliance Office requests the User to sign this as an Acknowledgement that any information accessed is confidential and subject to the protections under the Health Information Portability & Accountability Act.

By signing this document, the User acknowledges that this document has been discussed with the User and the User has been given a copy of this document.

_____	_____	_____
User Signature	User Name (printed)	Date

Attachment A: Explanation of HIPAA Confidentiality Obligations and Acknowledgement

The individual whose access to the electronic medical record (EMR) system is being discussed (User) is requested to sign below acknowledging the receipt of HIPAA confidentiality education and this document. It will be kept by the UMHS Compliance Office to show compliance with HIPAA's education and mitigation requirements. Two copies are provided. Return one to the UMHS Compliance Office and give one copy to the User.

WHAT IS HIPAA? The Health Information Portability & Accountability Act (HIPAA) Privacy Rule is a Federal law that establishes national standards to protect individuals' medical records and other personal health information. HIPAA applies to health care providers and members of its workforce, including those who have access to the health care provider's electronic medical record (EMR) system.

Penalties for HIPAA Violations: Individuals who violate HIPAA can be subject to both *civil and criminal penalties,* which can include significant fines (up to $1.5 Million per HIPAA violation per year) *and imprisonment up to 10 years.* These penalties can be applied for individuals who have "knowingly" obtained or disclose individually identifiable health information, who committed offenses under false pretenses and/or who committed offenses with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm.

Inappropriate Access to the EMR violates HIPAA: HIPAA sets rules and limits on who can look at a patient's EMR. Inappropriate access to one/more patient's EMR is a violation. Any confirmed inappropriate access to one/more patient's EMR is a HIPAA violation.

Auditing EMR Access & Discussion with User: Audits of access to the EMR system are conducted by the UMHS Compliance Office. Sometimes, it is not clear whether one or more accesses to one or more patient records are appropriate. When this happens, a discussion with the User is conducted to determine if the User can explain the accesses to those records. The User is expected to be truthful about his/her accesses.

We also use this discussion as an opportunity to further educate the User about appropriate and inappropriate accesses to the EMR System.

If There Is Inappropriate Access: If inappropriate access is believed to have occurred, mitigation steps are taken to prevent further potential HIPAA violations. The User is asked whether the patient information was disclosed by the User to any other person(s) and the circumstances of such disclosure. For example: If the User accessed a patient's record and subsequently told a friend or a family member about that patient's information, the User is expected to inform his/her Supervisor about that disclosure and the circumstances of that disclosure.

The User is also be informed that while sanctions may be issued under the UMHS Disciplinary Action policy for Privacy and Security Violations and any applicable collective bargaining agreement, the User continues to be subject to HIPAA and is required to maintain the confidentiality of all patient information and not inappropriately access, inappropriately use and/or inappropriately disclose any patient information in the future.

ACKNOWLEDGEMENT: The UMHS Compliance Office requests the User to sign this as an Acknowledgement that any information accessed is confidential and subject to the protections under the Health Information Portability & Accountability Act.

By signing this document, the User acknowledges that this document has been discussed with the User and the User has been given a copy of this document.

_____	_____	_____
User Signature	User Name (printed)	Date