Eastern Kentucky University EMC Program

HIPAA Policies

Draft Policy
5/14/03

(This document is not to be duplicated or distributed without expressed permission from the EMC Program.)

Eastern Kentucky University - EMC Program
HIPAA Policies

Eastern Kentucky University
EMC Program

Remember
The "Golden Rule" of HIPAA:

What You See Here,
What You Hear Here,
When You Leave Here,
Let It Stay Here!

Eastern Kentucky University - EMC Program
HIPAA Policies

General Statement:

The Eastern Kentucky University - Emergency Medical Care program recognizes that it is NOT a covered entity as defined by the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA). However, the Program also recognizes that because of the nature of the course work involved, its students, staff members and faculty may have access to protected health information as a result of internship and work in other clinical settings. This policy was created to assure that all persons associated with the program are aware of the provisions set forth in HIPAA and that it will serve as a guide for maintaining the confidentiality of protected patient health information. It is NOT to be used in place of any stricter policies that may be in place at any clinical or internship site.

Eastern Kentucky University - EMC Program
HIPAA Policies

The EMC program wishes to assure that our students and faculty are aware of and compliant with the Health Information Portability Accountability Act (HIPAA). In order to assure these goals, the program will follow the polices as laid out in this document, based upon a nationally recognized in-service program, and the expertise of the faculty.

The EMC program (hereafter known as the "Program") recognizes that it is NOT a covered entity as described in HIPAA (also identified in this document as the *Privacy Rule*). However, since our students will be participating in both clinicals and internship at covered entities and since faculty will coordinate and instruct the clinicals and internship courses, the program will provide documented training for those students and faculty regarding the Privacy Rule. This training will be conducted for each student prior to the beginning of internship and EMT ride-time. Faculty will be trained no later than June 1, 2003. Updates to this training will be conducted when there is a material change in the policies or procedures regarding the Privacy Rule, within a reasonable period of time after the material change becomes effective.

For the purposes of this document the following definitions will be utilized:

Instructor: the faculty member or outside consultant secured by the Program to conduct HIPAA Privacy Rule training

Participant: faculty, staff members and staff who attend and complete the mandatory HIPAA Privacy Rule training

Faculty: persons serving as full-time or part-time faculty within the Program; preceptors, clinical skills instructors and any person serving in the role of "teacher"

This Privacy Rule training will consist of the following steps:

<u>Instructor</u>

1. Instructor will provide a brief introduction, emphasizing that completion of organization's required privacy training includes: a) watching the video presentation, b) reading and reviewing the Program's privacy policies, c) asking questions about the video presentation and privacy policies, and d) completing the post-test and reviewing the correct answers.

2. Instructor will show the respective HPTV video presentation(s).

3. Instructor will review organization's policies on privacy.

4. Instructor will administer the post-quiz and review the correct answers with the audience.

5. Instructor will make sure everyone has signed in and that the sign-in records and training materials are retained by the Program for at least 6 years.

Participants

1. Participants will sign in on the training log sheet.

2. Participants will receive the program objectives and slide presentation handouts for the training program (administrative personnel, faculty, students or field providers).

3. Participants will receive and complete the acknowledgement form to turn in at the end of the training session.

The specific objectives for Privacy Rule training for faculty, staff members and students are:

1. Describe the basic legal obligations of EMS, EMS educational agencies, hospital and ambulance organizations with respect to the creation, access, use and disclosure of protected health information (PHI).

2. Describe the program's policies and procedures regarding PHI and the responsibilities of students, faculty and staff members to safeguard that information.

3. Describe when information would be considered PHI under the HIPAA Privacy Rule.

4. Describe common sources of PHI.

5. Describe how and when a Notice of Privacy Practices (NPP) should be given to the patient.

6. Describe when and how to obtain the patient's acknowledgement of receipt of the NPP.

7. Describe the role of the Privacy Officer in the program as well as an EMS or hospital.

8. Describe the process for patients (or surrogates) to access PHI.

9. Describe the process by which a student and or faculty member may release PHI to other health care providers, patients, rescuers or police.

10. Identify the procedure for patients to request amendment of their protected health information, and the process for acting on those requests.

11. Describe the process patients (or surrogates) may take to express a concern about the program's, hospital's or an EMS agency's PHI policies.

12. Describe considerations for documentation of PHI that should appear on a completed patient care report (PCR) and or clinical skills sheet (paper or electronic format).

Objectives based upon information in: Copyright 2003 by Page, Wolfberg & Wirth, LLC

Eastern Kentucky University - EMC Program

Privacy Rule Training Outline

Purpose

To ensure that all faculty, staff members and students of the Eastern Kentucky University - Emergency Medical Care program (hereafter known as the "Program") who have access to confidential patient health information (PHI) understand the organization's concern for the respect of patient privacy and are trained in the Program's policies and procedures regarding PHI.

Policy

1. All current faculty, staff members and students who may have access with PHI will be required to undergo privacy training in accordance with the HIPAA Privacy Rule prior to June 1, 2003 or their next participation in a direct patient care setting (whichever comes first).

2. All new faculty, staff members and students who may have access with PHI will be required to undergo privacy training in accordance with the HIPAA Privacy Rule within a reasonable time upon association with the Program, as scheduled by the Privacy Officer.

3. All faculty, staff members and students who may have access with PHI will be required to undergo privacy training in accordance with the HIPAA Privacy Rule within a reasonable time after there is a material change to the Program's policies and procedures on privacy practices.

Procedure

1. The Privacy Officer or his or her designee will conduct the Privacy Training.

2. All attendees must attend the training in person and verify attendance and agreement to adhere to the Program's policies and procedures on privacy practices.

3. All attendees will receive copies of the Program's policies and procedures regarding privacy.

4. Training will be conducted in the following manner:

    a. Introduction
    b. Sign-in and verification
    c. Distribution of policies
    d. Video presentation

e. Discussion and questions
f. Post-test
g. Discussion and questions

5. Topics of the training will include a complete review of the Program's Policy on Privacy Practices and will include other information concerning the HIPAA Privacy Rule, such as, but not limited to, the following topic areas:

a. Overview of the federal and state laws concerning patient privacy including the Privacy Regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
b. Description of protected health information (PHI)
c. Patient rights under the HIPAA Privacy Rule
d. Staff member responsibilities under the Privacy Rule
e. Role of the Privacy Officer and reporting employee and patient concerns regarding privacy issues
f. Importance and benefits of privacy compliance
g. Consequences of failure to follow established privacy policies
h. Use of agency (i.e., clinical and internship site) specific privacy forms

Eastern Kentucky University - EMC Program
Medical Records of Students

Policy

To provide guidance to faculty, staff members and students concerning the privacy of medical records of students of the Program.

Procedure

The Eastern Kentucky University - EMC program (hereafter known as the "Program") will, to the extent required by law, protect medical records it receives about students in a confidential manner. Generally, only those with a need to know the information will have access to it, and, even then, will only have access to as much information as is minimally necessary for the legitimate use of the medical records.

Students' records that are not considered to be protected health information, or PHI, subject to HIPAA safeguards, include certain medical records that are related to the student activities. These records not covered under HIPAA include, but are not limited to: information obtained to determine suitability to perform the teaching-learning duties (such as physical examination reports), drug and alcohol tests obtained in the course of class work, doctor's excuses provided in accordance with the attendance policy, work-related injury and occupational exposure reports, and medical and laboratory reports related to such injuries or exposures, especially to the extent necessary to determine workers' compensation coverage.

Nonetheless, despite the fact that such records are not considered HIPAA protected, the Program will limit the use and disclosure of these records to only those with a need to have access to them, such as certain faculty, staff, the Program's and or University's designated physician or officials, and state (and federal) agencies as allowed by law.

If you have any questions about how medical information about you is used and disclosed by the Program, please contact the Privacy Officer.

Eastern Kentucky University - EMC Program
Patient Care Reports

Policy

To ensure that all faculty, staff members and students of the Program properly manage all materials used in the preparation of a patient care report (PCR) and to secure and restrict PCR accessibility.

Procedure

The Eastern Kentucky University - EMC program (hereafter known as the "Program") maintains strict requirements on the security and access of all PCRs as well as the initial documentation created by the field providers and students in their preparation of a PCR.

1. All preliminary documentation used by a student, faculty and or staff member to assist in the creation or modification of a PCR is the sole property of the Program.

2. A PCR may be amended by a student, faculty and or staff member upon approval by the Privacy Officer or Faculty member of record for the applicable course.

3. Completed PCRs are to go immediately to a person designated by the Program. Typically this will be the instructor of record for the applicable course. PCRs must be either hand delivered or placed in a lock box.

4. All scratch paper used by a student in the preparation of a PCR must be shredded immediately.

5. Inappropriate access or retention of PHI may result in disciplinary action, including warnings, suspensions and termination (i.e., assigned a failing grade).

Eastern Kentucky University - EMC Program
Clinical Skill Forms

Policy

To ensure that all students of the Program properly manage all materials used in the preparation of a clinical skill form (CSF) and to secure and restrict CSF accessibility.

Procedure

The Eastern Kentucky University - EMC program (hereafter known as the "Program") maintains strict requirements on the security and access of all CSFs as well as the initial documentation created by the field providers in their preparation of a CSF.

1. All preliminary documentation used by a student, faculty and or staff member to assist in the creation or modification of a CSF is the sole property of Program.

2. A CSF may be amended by a student, faculty and or staff member upon approval by the Privacy Officer or Faculty member of record for the applicable course.

3. Completed CSFs are to go immediately to a person designated by the Program. Typically this will be the instructor of record for the applicable course. CSFs must be either hand delivered or placed in a lock box.

4. All scratch paper used by a student in the preparation of a CSF must be shredded immediately.

5. Inappropriate access or retention of PHI may result in disciplinary action, including warnings, suspensions and termination (i.e., assigned a failing grade).

Eastern Kentucky University - EMC Program
Access, Security and Disclosure of PHI

Purpose

To outline levels of access to Protected Health Information (PHI) for faculty, staff members and students of the Eastern Kentucky University - Emergency Medical Care program (hereafter known as the "Program") and to provide a policy and procedure on limiting access, disclosure, and use of PHI. To provide policies outlining patient rights and Program's responsibilities in fulfilling patient requests related to PHI.

Policy

The Program retains strict requirements on the security, access, disclosure and use of PHI. Access, disclosure and use of PHI will be based on the role of the individual faculty, staff members and student in the organization, and should be only to the extent that the person needs access to PHI to complete necessary job functions.

When PHI is accessed, disclosed and used, the individuals involved will make every effort, **except in patient care situations**, to only access, disclose and use PHI to the extent that only the minimum necessary information is used to accomplish the intended purpose.

Persons whose PHI has been collected may exercise their rights to access, amend, restrict, and request an accounting, as well as lodge a complaint with either the Program, the clinical/internship site or the Secretary of the Department of Health and Human Services. Students should direct any patient requests to the applicable Privacy Officer for the clinical/internship site. *As the Program is not a covered entity as defined by the Privacy Rules, and it does not collect information that is specifically identifiable to individual patients, it is not expected to receive these requests.*

Procedure

Course Related Collection

Students are specifically forbidden to record any protected patient health information (PHI) that may lead to the identification of a specific patient on any patient care report or clinical skills form. Students MAY collect such information as needed by the clinical/internship site or the Program for the purposes of treatment, payment or operations (as defined in HIPAA) and or incident report. It is the responsibility of the person recording PHI to utilize the minimum amount of information that is necessary in order to complete the task at hand.

Role Based Access

Access to PHI will be limited to those who need such access to that information to carry out their duties. The following describes the specific categories or types of PHI to which persons need access and the conditions, as appropriate, that would apply to such access.

Job Title	Description of PHI to Be Accessed	Conditions of Access to PHI
Student	Dispatch information, intake forms from dispatch, patient care records, clinical skills forms and incident reports	May access only as part of completion of a patient event and post-event activities and only while actually on duty
Faculty	Dispatch information, intake forms from dispatch, patient care records, clinical skills forms and incident reports	May access only as part of completion of a patient event and post-event activities, teaching, data entry and analysis and quality assurance
Staff	Clinical Skill Forms	May access only as part of completion of post-event activities, data entry and analysis

Access to PHI is limited to the above-identified persons only, and to the identified PHI only, based on the Program's reasonable determination of the persons or classes of persons who require PHI, and the nature of the health information they require, consistent with their job responsibilities.

Access to PHI will not be allowed except when expressly permitted by Program policy or s approved by the Privacy Officer.

Disclosures to and Authorizations from the Patient

Students are NOT required to limit disclosure to the minimum amount of information necessary when disclosing PHI to other health care providers for treatment of the patient. This includes (but is not limited to) preceptors, doctors, nurses, etc. at the receiving hospital, any mutual aid provider, fellow crewmembers involved in the call, and any other person involved in the treatment of the patient who has a need to know that patient's PHI. In addition, disclosures authorized by the patient are exempt from the minimum necessary requirements unless the authorization to disclose PHI is requested by the clinical/internship site.

For all other uses and disclosures of PHI, the minimum necessary rule is likely to apply. A good example of when the minimum necessary rule applies is when the clinical/internship site or the Program conducts quality assurance activities. In most situations it is not necessary to disclose certain patient information such as the patient's name, address, social security number, and or certain portions of the PHI of the treated patient, in order to conduct a call review. This sensitive information should be left out of

or redacted (blacked out) from the patient care report and or clinical skills form being used as a quality-assurance/quality-assessment example or classroom activity.

Program Requests for PHI

If the Program needs to request PHI from a health care provider, it must limit its requests to only the reasonably necessary information needed for the intended purpose, as described below. For requests not covered below, the Program must make this determination individually for each request. For example, if the request is non-recurring or non-routine, like making a request for documents via a subpoena, we must review the request to make sure it covers only the minimum necessary PHI to accomplish the purpose of the request. The agency serving the subpoena must satisfy the HIPAA rules for such a request (i.e., assurance that the information will be destroyed following the closure of the matter at hand or that the patient has been notified of this request).

Holder of PHI	**Purpose of Request**	**Information Reasonably Necessary to Accomplish Purpose**
Health Care Agencies	• To assist in identifying potential health risks related to occupational exposures • To investigate patient and or faculty/agency complaints	Patient care reports, incident reports

Incidental Disclosures

The Program understands that there will be times when there are incidental disclosures of PHI in the context of caring for a patient. The HIPAA privacy rules were not intended to impede common health care practices that are essential in providing health care to the individual. Incidental disclosures are inevitable; these will typically occur in radio or face-to-face conversation between health care providers, or when patient care information in written or computer form is left out in the open for others to access or see.

The fundamental principle is that all faculty, staff members and students need to be sensitive about the importance of maintaining the confidence and security of all material created or used that contains patient care information. Coworkers, other staff members, students, members of other agencies and the general public should not have access to information that is not necessary to complete their job. *For example, it is generally not appropriate for field personnel to have access to billing claim forms of the patient nor is it appropriate for student workers to review patient care reports.*

All personnel must be sensitive to avoiding incidental disclosures to other health care providers and others who do not have a need to know the confidential patient health

information. Pay attention to who is within earshot when making verbal statements about a patient's health information, and follow some of these common sense procedures for avoiding accidental or inadvertent disclosures:

A) Verbal Security

Waiting or Public Areas: If patients are in waiting areas to discuss the service provided to them or to have billing questions answered, make sure that there are no other persons in the waiting area, or if so, bring the patient into a screened area before engaging in discussion. The patient (or their representative) should be directed to the preceptor or the privacy officer of the agency.

Station and Hospital Areas: Faculty, staff members and students should be sensitive to that fact that members of the public and other agencies may be present in these and other easily accessible areas. Conversations about patients and their health care should not take place in areas where those without a need to know are present. This includes avoiding allowing law enforcement officers from overhearing protected health information without either:

1. the officer being an active participant in the care of the patient (even then the release of information should be related to the actual care)
2. being presented with a subpoena or other legal mandate (and the approval of the privacy officer)

Other Areas: Faculty, staff members and students should only discuss patient care information with those who are involved in the care of the patient, regardless of their physical location. Faculty, staff members and students should be sensitive to their level of voice and to the fact that others may be in the area when speaking. This approach is not meant to impede anyone's ability to speak with other health care providers freely when engaged in the care of the patient. When it comes to treatment of the patient, faculty, staff members and students should be free to discuss all aspects of the patient's medical condition, treatment provided, and any of their health information they may have in their possession with others involved in the care of the patient.

B) Physical Security

Patient Care and Other Patient or Billing Records: Patient care reports and clinical skill sheets should be stored in safe and secure areas. When any paper records concerning a patient are completed, they should not be left in open bins or on desktops or other surfaces. Only those with a need to have the information for the completion of their job duties should have access to any paper records.

Billing records, including all notes, remittance advices, charge slips or claim forms should be stored according to the policies of the agency. In general they should not be left out in the open and should be stored in files or boxes that are secure and in an area with access limited to those who need access to the information for the completion of their job duties.

Computers and Entry Devices: Computer access terminals and other remote entry devices such as PDAs and laptops should be kept secure. Access to any computer device that contains patient care information should be stored according to the policies of the agency. In general they should be accessible by password only. Persons using these devices should be sensitive to who may be in viewing range of the monitor screen and take simple steps to shield viewing of the screen by unauthorized persons. All remote devices such as laptops and PDAs should remain in the physical possession of the individual to whom it is assigned at all times. *See the Program's Policy on Use of Computer Equipment and Information Systems for further details*.

Penalties for Violation

The Program takes its responsibility to safeguard patient information very seriously. There are significant legal penalties against companies and individuals that do not adhere to the laws that protect patient privacy.

Faculty, staff members and students who do not follow our policies on patient privacy will be subject to disciplinary action, up to and including verbal and written warnings, suspension and or termination of their association with the Program.

Questions About This Policy or Any Privacy Issues

The Program has appointed a Privacy Officer to oversee its policies and procedures on patient privacy and to monitor compliance. The Privacy Officer is also available to all faculty, staff members and students for consultation on any issues or concerns they may have about how the Program deals with protected health information. Faculty, staff members and students should feel free to contact the Privacy Officer at any time with any questions or concerns.

The Program will not retaliate against any faculty, staff members and students who express a good faith concern or complaint about any policy or practice related to the safeguarding of patient information and the Program's legal obligations to protect patient privacy.

Patient Access, Amendment or Restriction to PHI

Faculty, staff members and students may receive patient requests to access, amend and or restrict access to PHI. If the request is made in regards to the documentation completed at a clinical/internship site (i.e., hospital records or EMS run forms), those requests should be directed to that agency's Privacy Officer. If the request is made in regard to Program related forms (i.e., PCRs, and CSFs), those requests should be directed to the Program's Privacy Officer. Under no circumstances should the faculty, staff members or students release any patient health information without the specific approval of the applicable Privacy Officer.

Policy - Accounting

Purpose

To provide guidance to faculty, staff members and students concerning the patient's right to an Accounting and the types of uses and disclosures of PHI for which the Program is required to document. *As the Program does not allow students to include protected patient health information on its records, it is not expected that such requests will be made to the Program.*

Procedure

1. All patient records will be kept by the Program for a period of six (6) years from the date of service.

2. All patient accounting requests should be received directly from a patient or legal representative.

3. The Program will provide a list of uses and disclosures of the patient's PHI, for the last six (6) years or to the extent that the Program has maintained that patient's information if less than six (6) years.

4. All uses and disclosures of a patient's PHI, made by the Program, must be documented for accounting purposes except:

    a. Disclosures to carry out treatment, payment and health care operations;
    b. For national security or intelligence purposes;
    c. Uses and disclosures incident to an unaccountable use or disclosure;
    d. That occurred prior to the compliance date.

5. A common use or disclosure that must be accounted for and information provided upon a request for accounting is the disclosure of PHI in response to a subpoena, summons or warrant.

<u>Policy - Patient Complaints</u>

Patients have the right to complain to the Program about any concerns they may have concerning patient privacy. Any patient or family member who expresses a concern or complaint to the Program (including faculty, staff members and or students) should be directed to contact the Privacy Officer. The Privacy Officer is responsible for receiving, investigating, and documenting all complaints from patients concerning patient privacy issues.

Eastern Kentucky University - EMC Program
Use of Computer and Information Systems and Equipment

Purpose

The Eastern Kentucky University Emergency Medical Care program (hereafter known as "Program") is committed to protecting the protected health information (PHI) of the patients we serve, and the Program from illegal or damaging actions by individuals and the improper release of PHI and other confidential or proprietary information.

The purpose of this policy is to outline the acceptable use of computer equipment by faculty, staff and students associated with the Program. These rules are in place to protect the PHI encountered during the activities of the Program. Inappropriate use exposes the Program to risks including virus attacks, compromise of network systems and services, breach of patient confidentiality and other legal claims.

Scope

This policy applies to employees, volunteers, members, contractors, consultants (e.g., preceptors), temporary employees, students, and others at the Program who have access to computer equipment, including all personnel affiliated with third parties. This policy applies to all equipment that is owned, or leased or used by the Program.

Procedure

Use and Ownership of Computer Equipment

1. All patient related data created or recorded using any computer equipment owned, controlled or used for the benefit of the Program is at all times the property of the Program. The Program will take all steps necessary to secure the privacy of all protected health information in accordance with all applicable laws.

2. Faculty, staff members and students are responsible for exercising good judgment regarding the reasonableness of personal use and must follow operational guidelines for personal use of Internet/Intranet/Extranet systems and any computer equipment.

Security and Proprietary Information

1. Confidential information should be protected at all times, regardless of the medium by which it is stored. Faculty, staff members and students should take all necessary steps to prevent unauthorized access to patient health information.

2. All PCs, laptops, workstations and remote devices (e.g., PDAs) containing patient health information should be secured with a password-protected screensaver, wherever possible, and set to deactivate after being left unattended for ten (10)

minutes or more, or by logging-off when the equipment will be unattended for an extended period.

   a. The loss of any electronic device that contains patient health information must be immediately reported to the Privacy Officers of the clinical/internship site and the Program.

3. All computer equipment used by Faculty, staff, and students whether owned by the individual staff member or the Program shall regularly run approved virus-scanning software with a current virus database in accordance with Program and or University policy.

4. Faculty, staff members and students must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses.

Unacceptable Use

1. Under no circumstances is a faculty, staff member or student of the Program authorized to disclose any patient health information to any person, agency or entity that is not specifically approved to receive that information by the policies of the Program and applicable state and or federal laws or without the approval of the applicable Privacy Officer.

Enforcement

Any faculty, staff member or student found to have violated this policy may be subject to disciplinary action, up to and including suspension and termination (e.g., receiving a failing grade for the applicable course).

Eastern Kentucky University - EMC Program

Confidentiality of Patient Information: Verification for Faculty, Staff and Students

Given the nature of the program, it is imperative that it maintains the confidence of patient information that is received in the course of activities involving students and faculty and staff members. The Eastern Kentucky University - Emergency Medical Care program (hereafter known as "Program") prohibits the release of any patient information to anyone not involved in the treatment, billing and or operations related to the care of the patient in question unless required to do so by law. Discussion of patient health information is acceptable when it is required for purposes of treatment, payment, or health care operations but even then such discussions of Protected Health Information (PHI) should be limited. Acceptable uses of PHI by faculty, staff members and students include, but are not limited to, exchange of patient information needed for the treatment of the patient, billing, and other essential health care operations, classroom activities, peer review, internal audits, and quality assurance activities. In all cases of disclosure, this agency will only disclose what is necessary and only to persons with a legitimate need for that information.

I understand that as faculty, staff member or student of the Program, I may provide services to patients or I may have access to documentation of services provided to patients that are private and confidential and that I am a crucial step in respecting the privacy rights of patients. I understand that it is necessary, in the rendering of services, that patients provide personal information and that such information may exist in a variety of forms such as electronic, oral, written or photographic and that all such information is strictly confidential and protected by federal and state laws.

I agree that I will comply with all confidentiality policies and procedures set in place by the Program as well as any clinical and or internship site at which I am associated during my entire employment (and or clinical/internship) or association with the Program. If I, at any time, knowingly or inadvertently breach these patient confidentiality policies and procedures, I agree to immediately notify the Privacy Officers of the clinical or internship site and the Program. In addition, I understand that a breach of patient confidentiality may result in punishment, including but not limited to suspension or termination of my employment or association with Program. Upon termination of my employment or association with the Program for any reason, or at any time upon request, I agree to return any and all patient confidential information (originals and or copies, regardless of its format) in my possession to the Program's Privacy Officer within 24 hours. I also understand that I will still be bound by the terms of this agreement despite no longer being employed by or associated with the Program.

I have read and understand all privacy policies and procedures that have been provided to me by the Program. I agree to abide by all policies or be subject to disciplinary action as noted above. This is not a contract of employment and does not alter the nature of the existing relationship between the Program and me.

Signature:_____ Date:_____

Printed Name:_____

Eastern Kentucky University - EMC Program

Contact information for Privacy Officer

Name: Sandy Hunter

Title: Associate Professor

Address: Emergency Medical Care Program

Dizney 225

Eastern Kentucky University

225 Lancaster Avenue

Richmond, KY 40475

Telephone: (859) 622 - 1028

E-mail: Sandy.Hunter@eku.edu

Appendix 1

Job Description: Privacy Officer

JOB DESCRIPTION

Job Title: Privacy Officer

Program: Emergency Medical Care
Reports to: Program Director

JOB PURPOSE AND SUMMARY

The Privacy Officer oversees all activities related to the development, implementation, and maintenance of the Program's policies and procedures covering the privacy of patient health information. This person serves as the key compliance officer for all federal and state laws that apply to the privacy of patient information, including the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA). This individual is tasked with the responsibility of ensuring that all of the organization's patient information privacy policies and procedures related to the privacy of, and access to, patient health information are followed.

DUTIES AND RESPONSIBILITIES

Principle Responsibilities

a. Develop policies and procedures on faculty, staff member and student training related to the privacy of patient health information and protected health information;
b. Develop policies on the security of health care information including computer and password security and patient data integrity;
c. Define levels of staff access to PHI and minimum necessary requirement for staff based on the required job responsibilities;
d. Oversee, direct, deliver, and ensure the delivery of initial and ongoing privacy training and orientation to all faculty, staff members, employees, volunteers, students and trainees.
e. Serve as the contact person for the dissemination of PHI are required by law;
f. Serve as the contact person for patient complaints and requests;
g. Process patient requests for access to and amendment of health information and consent forms;
h. Process all patient accounting requests;
i. Ensure the capture and storage of patient PHI for the minimum period required by law;
j. Ensure the Program's compliance with all applicable Privacy Rule requirements and work with legal counsel and other managers to ensure the Program maintains appropriate privacy and confidentiality notices, forms, and materials.
k. Cooperate with the state and federal government agencies charged with compliance reviews, audits and investigations.

QUALIFICATIONS:

a. Full time faculty member
b. Maintains current knowledge of applicable federal and state privacy laws and monitors changes in privacy practices for the educational institutions, hospitals and the ambulance industry to ensure current organizational compliance.

Mental Requirements of the Job

a. Reading and writing skills required. Experience working with the public is essential.
b. Demonstrated organizational, facilitation, communication and presentation skills.

Disclaimer

The information provided in this description has been designed to indicate the general nature and level of work performed by incumbents within this job. It is not designed to be interpreted, as a comprehensive inventory of all duties, responsibilities, qualifications and working conditions required of employees, assigned to this job. The Program Director and or Chair have discretion to add or modify duties of the job and to designate other functions as essential at any time. This job description is not an employment agreement or contract.

Appendix 2

Sample Notice of Privacy Practices

Sample Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

ABC Ambulance Service, Inc. [or ABC Hospital, Inc.] ("ABC Company") is required by law to maintain the privacy of certain confidential health care information, known as Protected Health Information or PHI, and to provide you with a notice of our legal duties and privacy practices with respect to your PHI. ABC Company is also required to abide by the terms of the version of this Notice currently in effect.

Uses and Disclosures of PHI: ABC Company may use PHI for the purposes of treatment, payment, and health care operations, in most cases without your written permission. In all cases of disclosure, this agency will only disclose what is necessary and only to persons with a legitimate need for that information. Examples of our use of your PHI:

For treatment. This includes such things as obtaining verbal and written information about your medical condition and treatment from you as well as from others, such as doctors who give orders to allow us to provide treatment to you and nurses that receive you at the hospital. We may give your PHI to other health care providers involved in your treatment, and may transfer your PHI via radio or telephone.

For payment. This includes any activities we must undertake in order to obtain reimbursement for the services we provide to you, including such things as submitting bills to insurance companies, making medical necessity determinations and collecting outstanding accounts.

For health care operations. This includes quality assurance activities, licensing, and training programs to ensure that our personnel meet our standards of care and follow established policies and procedures, as well as certain other management functions.

Reminders for Scheduled Transports and Information on Other Services. We may also contact you to provide you with a reminder of any scheduled appointments for non-emergency ambulance and medical transportation, or to provide information about other services we render.

Use and Disclosure of PHI Without Your Authorization. ABC Company is permitted to use PHI *without* your written authorization, or opportunity to object, in certain situations, and unless prohibited by a more stringent state law, including:

- For the treatment, payment or health care operations activities of another health care provider who treats you;
- For health care and legal compliance activities;
- To a family member, other relative, or close personal friend or other individual involved in your care if we obtain your verbal agreement to do so or if we give

you an opportunity to object to such a disclosure and you do not raise an objection, and in certain other circumstances where we are unable to obtain your agreement and believe the disclosure is in your best interests;

- To a public health authority in certain situations as required by law (such as to report abuse [i.e., KRS 620.030 - 620.050], neglect or domestic violence;
- For health oversight activities including audits or government investigations, inspections, disciplinary proceedings, and other administrative or judicial actions undertaken by the government (or their contractors) by law to oversee the health care system;
- For judicial and administrative proceedings as required by a court or administrative order, or in some cases in response to a subpoena or other legal process;
- For law enforcement activities in limited situations, such as when responding to a warrant;
- For military, national defense and security and other special government functions;
- To avert a serious threat to the health and safety of a person or the public at large;
- For workers' compensation purposes, and in compliance with workers' compensation laws;
- To coroners, medical examiners, and funeral directors for identifying a deceased person, determining cause of death, or carrying on their duties as authorized by law;
- If you are an organ donor, we may release health information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ donation and transplantation;
- For research projects, but this will be subject to strict oversight and approvals;
- We may also use or disclose health information about you in a way that does not personally identify you or reveal who you are.

Any other use or disclosure of PHI, other than those listed above will only be made with your written authorization. You may revoke your authorization at any time, in writing, except to the extent that we have already used or disclosed medical information in reliance on that authorization.

Patient Rights: As a patient, you have a number of rights with respect to your PHI, including:

The right to access, copy or inspect your PHI. This means you may inspect and copy most of the medical information about you that we maintain. We will normally provide you with access to this information within 30 days of your request. We may also charge you a reasonable fee for you to copy any medical information that you have the right to access. In limited circumstances, we may deny you access to your medical information, and you may appeal certain types of denials. We have available forms to request access to your PHI and we will provide a written response if we deny you access and let you know your appeal rights. You also have the right to receive confidential communications

of your PHI. If you wish to inspect and copy your medical information, you should contact our privacy officer at 859 - 000 - 0000.

The right to amend your PHI. You have the right to ask us to amend written medical information that we may have about you. We will generally amend your information within 60 days of your request and will notify you when we have amended the information. We are permitted by law to deny your request to amend your medical information only in certain circumstances, like when we believe the information you have asked us to amend is correct. You still have a right to submit an amendment to your PHI describing the information you wish to include and or dispute. If you wish to request that we amend the medical information that we have about you, you should contact our privacy officer 859 - 000 - 0000.

The right to request an accounting. You may request an accounting from us of certain disclosures of your medical information that we have made in the six years prior to the date of your request. We are not required to give you an accounting of information we have used or disclosed for purposes of treatment, payment or health care operations, or when we share your health information with our business associates, like our billing company or a medical facility from/to which we have transported you. We are also not required to give you an accounting of our uses of protected health information for which you have already given us written authorization. If you wish to request an accounting, contact our privacy officer 859 - 000 - 0000.

The right to request that we restrict the uses and disclosures of your PHI. You have the right to request that we restrict how we use and disclose your medical information that we have about you. ABC Company is not required to agree to any restrictions you request, but any restrictions agreed to by ABC Company in writing are binding on ABC Company.

Internet, Electronic Mail, and the Right to Obtain Copy of Paper Notice on Request. If we maintain a web site, we will prominently post a copy of this Notice on our web site. If you allow us, we will forward you this Notice by electronic mail instead of on paper and you may always request a paper copy of the Notice.

Revisions to the Notice: ABC Company reserves the right to change the terms of this Notice at any time, and the changes will be effective immediately and will apply to all protected health information that we maintain. Any material changes to the Notice will be promptly posted in our facilities and posted to our web site, if we maintain one. You can get a copy of the latest version of this Notice by contacting our privacy officer at 859 - 000 - 0000.

Your Legal Rights and Complaints: You also have the right to complain to us, or to the Secretary of the United States Department of Health and Human Services if you believe your privacy rights have been violated. You will not be retaliated against in any way for filing a complaint with us or to the government. You may contact the Department of Health and Human Services at: (*Toll Free*) 1-877-696-6775. Should you have any

questions, comments or complaints you may direct all inquiries to our privacy officer at 859 - 000 - 0000.

Privacy Officer Contact Information:

Privacy Officer
ABC Ambulance Corporation
ADDRESS
TELEPHONE NUMBER
FAX NUMBER (if desired)/E-MAIL (if desired)

Effective Date of the Notice: April 14, 2003

I hereby acknowledge that I have been provided with a copy of ABC Ambulance Service, Inc.'s Notice of Privacy Practices on this date.

_____ _____
Date Signature

_____
Print Patient's Name

_____
Street Address

_____
City, State and Zip Code

Witnessed by: _____

Appendix 3

HIPAA PRIVACY TRAINING PROGRAM

PARTICIPANT ATTENDANCE LOG

HIPAA PRIVACY TRAINING PROGRAM
PARTICIPANT ATTENDANCE LOG

Topic: "HIPAA Privacy Training Video for EMS"

Date of Training: _____

Time Training - Began: _____ Ended: _____

Instructor: _____

IMPORTANT! SIGN IN AND VERIFICATION REQUIRED*

By my signature below, I verify that I have attended the training session described above and that I will adhere to the Program's policies and procedures related to privacy practices, a copy of which I received as part of the training materials for this session:

Date	Name (Please Print)	Job Title	Signature Verification of Attendance

* Attach a copy of the program handouts and materials and keep on file for a minimum of six (6) years.

Appendix 4

HIPAA PRIVACY TRAINING PROGRAM

Student Post-Test

HIPAA PRIVACY TRAINING VIDEO PROGRAM – POST TEST
FOR STUDENTS AND FIELD PROVIDERS

NOT AVAILABLE VIA THE WEB

Appendix 5

HIPAA PRIVACY TRAINING PROGRAM

Faculty - Administrator Post-Test

HIPAA PRIVACY TRAINING VIDEO PROGRAM – POST TEST
FOR FACULTY AND ADMINISTRATORS

NOT AVAILABLE VIA THE WEB