Health and Human Services

Risk Management Guide

First revised 8/8/2015; Second revision, 9/2017; third revision Summer 2019

Preface

This manual has been developed as a guide for faculty, students, clinicians, and administrators. The information contained herein is intended to enhance your knowledge of risk management, provide a set of procedures to avoid or reduce your exposure to violations of regulations, and provide a set of steps for following the proper procedures should a violation occur. These Risk Management guidelines are not intended to serve as legal advice.
This Risk Management document is available to assist you and the Chairs of Health and Human Services, Deans, and administration of ENMU in the services to our students and clients.

Original Committee (2015)
Suzanne Swift, CDIS
Laura Bucknell, CDIS
Karen Copple, CDIS
Judith Piepkorn, Nursing
Delia Avilla, Social Work
Trisha Griggs, CDIS Graduate Student

2017 Review Committee
Suzanne Swift, CDIS
Laura Bucknell, CDIS
Karen Copple, CDIS
Judith Piepkorn, Nursing
Patty Saylor, Social Work
Jennifer Schlitt, CDIS Graduate Student

2019 Review Committee
Suzanne Swift, CDIS
Laura Bucknell, CDIS
Karen Copple, CDIS
Judith Piepkorn, Nursing
Melissa Hardin, Social Work

Table of Contents

OVERVIEW OF RISK MANAGEMENT

Risk management is an overall philosophy for the entire department and is no longer solely

represented by an individual Risk Manager. Faculty could double as the risk management/safety committee to discuss pertinent issues or a committee formed. The information contained in this manual is directed toward the student, faculty, and the administrative/management faculty and staff to develop a well-rounded risk management program including both proactive and reactive procedures.

Orientation and Training
To facilitate orientation and to serve as a resource for all students and faculty, this policy and procedures manual includes, but is not limited to, the following:

1. Policies and procedures
2. Confidentiality
3. FERPA
4. Policies on the release of medical records
5. What to do when a violation has occurred
6. Policies on using, distributing, and storage of Protected Health Information including client communications.
7. Procedures for responding to patients' complaints
8. Training and training updates to students, faculty, and staff in Risk Management including Privacy and Security Training (i.e., FERPA, HIPPA), CPR, First Aid, and Universal Precautions).

Students and faculty should regularly receive training and education in risk management. All personnel using the policies and procedures should sign and date their acknowledgement and understanding of the policies yearly.

These policies and procedures should be dated. When any revisions are made, the date should be changed to reflect those revision; as such (i.e., "Revised 01/01/05").

Overview of HIPPA

In 1996, the federal government established the Health Insurance Portability and Accountability Act, or HIPPA. This law provided for the protection of any and all health related records maintained by health care providers. Under this law, a patient or guardian is afforded the

opportunity to understand and agree with the manner in which their private health care information is maintained. This privacy has been extended to electronic transmission of health care reports through the Hi Tech Amendment and Omnibus Rule of 2013.

The Privacy Rule providing federal protections for individually identifiable health information applies to records held by the Speech and Hearing Rehabilitation Outreach Clinic (SHROC), the department of Social Services, and the department of Nursing at Eastern New Mexico University (ENMU). However, the Privacy Rule, also HIPPA, balances these protections with the right of the disclosure of health information needed for patient care and other important purposes.

The Privacy Rule, as well as the Administrative Simplification rule, applies to health plans, health care clearinghouses, and to any health care provider, such as SHROC that transmits health information in electronic form. The Privacy Rule protects all "individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral." The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, FERPA, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.

Using electronic technology, such as email, does not mean a health care provider is a covered entity; the transmission must be in connection with a standard transaction. The Privacy Rule covers a health care provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf. Health care providers include all "providers of services" (e.g., institutional providers such as hospitals) and "providers of medical or health services" (e.g., non-institutional providers such as physicians, dentists and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care.

There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information; either: 1) a formal determination by a qualified statistician; or 2) the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the clinic has no actual knowledge that the remaining information could be used to identify the individual.

In Summary, patients have the following rights under HIPPA. The right to:

Access their records, including inspecting and copying
Account for any non-routine disclosure; communicating the use of their PHI
Notice of Information Practices (i.e., what happens to their records)

Request restrictions on use and disclosure of their PHI
Alternate communication Methods; home versus work or cell phone contacts
Request correction/amendments to their PHI; excluding third party records, written.

General Principles for Uses and Disclosures

A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed by the clinic. The clinic may not use or disclose protected health information, except either: (1) as the Privacy Rule permits

or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.

Required Disclosures.
The clinic must disclose protected health information in only two situations: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to HHS when it is undertaking a compliance investigation or review or enforcement action.

Permitted Uses and Disclosures.
The clinic is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations: (1) to the individual (unless required for access or accounting of disclosures); (2) treatment, payment, and health care operations; (3) opportunity to agree or object; (4) incident to an otherwise permitted use and disclosure; (5) public interest and benefit activities; and
(6) limited data set for the purposes of research, public health or health care operations.

Public Interest and Benefit Activities.
The Privacy Rule permits use and disclosure of protected health information, without an individual's authorization or permission under specific circumstances. These disclosures are permitted, although not required, by the Privacy Rule in recognition of the important uses made of health information outside of the health care context. Specific conditions or limitations apply to each public interest purpose, striking the balance between the individual privacy interest and the public interest need for this information.

The clinic may disclose protected health information to:

(1) public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect;
(2) entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and post-marketing surveillance;
(3) individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and

(4) employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with the Occupational Safety and Health Administration (OHSA), the Mine Safety and Health Administration (MHSA), or similar state law..
(5) law enforcement officials for law enforcement purposes under

the following six circumstances, and subject to specified conditions:

(1) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests;

(2) to identify or locate a suspect, fugitive, material witness, or missing person;

(3) in response to a law enforcement official's request for information about a victim or suspected victim of a crime;

(4) to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death;

(5) when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and

(6) by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime

(7) Workers' Compensation as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.

(8) Limited Data Set. A limited data set is protected health information from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed. A limited data set may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the protected health information within the limited data set.

Written Authorization.

The clinic must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule. The clinic may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances. An authorization must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party. Examples of disclosures that would require an individual's authorization include disclosures to a life insurer for coverage purposes, disclosures to an employer of the results of a pre-employment physical or lab test, or disclosures to a pharmaceutical firm for their own marketing purposes. All authorizations must be in plain language, and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data. The Privacy Rule contains transition provisions applicable to authorizations and other express legal permissions obtained prior to April 14, 2003.

Special cases:

Personal Representatives.

The Privacy Rule requires a covered entity to treat a "personal representative" the same as the individual, with respect to uses and disclosures of the individual's protected health information, as well as the individual's rights under the Privacy Rule. A personal representative is a person legally authorized to make health care decisions on an individual's behalf or to act for a deceased individual or the estate. The Privacy Rule permits an exception when a covered entity has a reasonable belief that the personal representative may be abusing or neglecting the individual, or that treating the person as the personal representative could otherwise endanger the individual.

Minors.
In most cases, parents are the personal representatives for their minor children. Therefore, in most cases, parents can exercise individual rights, such as access to the medical record, on behalf of their minor children. In certain exceptional cases, the parent is not considered the personal representative. In these situations, the Privacy Rule defers to State and other law to determine the rights of parents to access and control the protected health information of their minor children. If State and other law is silent concerning parental access to the minor's protected health information, a covered entity has discretion to provide or deny a parent access to the minor's health information, provided the decision is made by a licensed health care professional in the exercise of professional judgment

OVERVIEW OF FERPA

The ENMU CDIS Program and SHROC clinic not only train and educate undergraduate and graduate students for clinical practice but also include teaching, counseling, and advising students as educators. As such, the Health and Human Services Department must also adhere to the policies and regulations of the Family Educational Rights and Privacy Act (FERPA). These rights transfer to the adult student at age 18, which means that information cannot be shared

with a student's parents without the written permission of the adult student. The rights under FERPA include:

- The right to inspect and review educational records maintained by ENMU.
- The right to request, to the department chair, in written form, that ENMU correct records that they believe are inaccurate or misleading.
- Generally, ENMU CDIS must have written permission from the adult student to release any information from the student's records. FERPA does allow disclosure without consent to the following parties:
    - School officials with legitimate educational interest
    - Other schools to which a student is transferring
    - Specified officials for audit or evaluation purposes
    - Appropriate parties in connections with financial aid to an adult student
    - Organizations conducting certain studies for or on behalf of ENMU CDIS
    - Accrediting organizations
    - To comply with a judicial order or lawfully issued subpoena
    - Appropriate officials in cases of health and safety emergencies, and
    - State and local authorities within a juvenile justice system, pursuant to specific State law.
- ENMU CDIS can also release "directory" information such the adult student's name, address, phone number, date and place of birth, honors and awards, and dates of attendance.
- ENMU CDIS will notify the adult students, annually, concerning their rights under FERPA.
- Old Daily Therapy logs with identifiable student information will be stored by the Clinic Director. These logs will be shredded at the end of each academic year.

PROCEDURES FOR CDIS CLINIC

All CDIS student clinicians are required to receive training in HIPPA, FERPA, PBP, Universal Health Precautions, AED, and Confidentiality. Students will follow HIPPA regulations in handling PHI in written, electronic, and oral form. A client or parent of a client may not contact individual clinicians by any means. They should instead phone the clinic, supervisor, or the clinical director. Student clinicians should not have contact with clients or their families outside of the clinic without supervisor approval or with the supervisor present.

Security Procedures:

To reduce the Risk of Access by unauthorized parties, all client PHI will be entered into the ClinicNote system. ClinicNote is a password protected healthcare data base. All client PHI, including but not limited to, personally identifying and demographic information, SOAP notes, and evaluation data. A second, student clinician "work folder," will be kept under the clinician's name in a locked file cabinet in the SHROC Library. This folder will only hold session data regarding ongoing therapy performance . Following each therapy session, the clinician will return the folder to the SHROC library where is will, again, be locked up. Any client correspondence between clinicians and their supervisors outside of the ClinicNote system, will be conducted via google docs or email with only the clincian's name. Google docs and ENMU email are both protected ways for the supervisor to provide corrective feedback and EBP to the clinician. Clinicians may only access ClinicNote in the "clean lab." No client PHI will be saved to a clinician's computer, iPad, iPhone, or any other portable storage system.
Other clinical concerns include clinician clinic hours. Therapy hours are logged and saved in an electronic, password protected, electronic system called Calipso. Calipso is FERPA compliant. Faculty reusing paper in their office printers must be cognizant of PHI and FERPA protected information and protect any of that information from general view.

Medically Fragile Clients:
Supervisors and clients need to be aware of the following:

- No clinician, at any time, may administer medication to a client.
- If a client is in eminent danger, in the case of a chronic medical condition, the parent (s) or other identified person(s) with written permission to act on behalf of the client, **MUST remain in the observation area in order to administer medication, if needed.**
- Examples of these conditions may include but are not limited to:
    - Seizures
    - Asthma
    - Allergies
    - Other, non-specified compromising neurological or respiratory conditions.

Access to AED Cardiac Defibrillator (pending):
The acronym AED stands for Automated External Defibrillator. The SHROC AED will be provided in the hallway, second floor, with signs posted. All students and faculty will be provided with training and updates every year or when first given a client.

In Case of Emergency:
Evacuations maps and instructions are placed in every therapy suite. In addition, each therapy room also has a radio electronic notification for active shooter alerts. The SHROC at ENMU has

fire warning alarms with flashing lights. Please, familiarize yourself, clients, and/or your client's parent(s) with the emergency exit map placed in each therapy room. DO NOT use the elevator during an emergency evacuation of the building.

Tornado Warnings:
Active Shooter
Fire Alarm: The SHROC at ENMU has fire warning alarms with flashing lights.
DO NOT use the elevator during an emergency evacuation of the building.

Fax Use:
The fax machine is housed in the ENMU CDIS office behind the secretary's desk out of the view of persons doing business or obtaining client files for treatment or evaluation purposes. Any fax communications must use the clinic cover page with HIPPA disclaimer. Copiers and Fax machines must be wiped and cleaned regularly

Universal Health Precautions:
All materials checked out for clinical use must be washed prior to their being returned to the library. NO unmarked or unlabeled bottles are allowed in the clinic.

What to do with a violation
If you have violated a procedure cited in the Student Handbook regarding inappropriate conversations or communications with you client that is prohibited due to the lack of student licensure, faculty have the option of discussing non-PHI or non-HIPPA violations before a student is written up for violating clinic policy.
If you have violated a HIPPA regulation or you observed someone committing a violation, you are ethically and legally bound to report that violation first to your immediate supervisor and the clinic director. The violation must also be submitted to the clinical director in writing so a permanent record of the incident and how the incident was corrected can be made by the clinic (See Appendix 2). Please, do not wait or delay communication of a violation to your immediate clinic supervisor and/or the clinical director. The clinic does not want to hear about a violation from the client or their family. Although we need to be proactive, we need to be responsive and reactive to any incidence(s) of violations (See attachment concerning Reporting HIPPA Violations).

Students in Off-Campus Placements
When a student is placed at an off-campus practicum site, the student remains bound ethically and legally to follow all HIPPA, FERPA, and ADA regulations. All students should obtain a copy of the Risk Management policies and regulations specific to their off-campus practicum site. Any violations of HIPPA, FERPA, or ADA regulations by the student clinician or any violations observed by the student must be reported to their immediate supervisor and the SHROC ENMU clinic director both orally and in writing so that a permanent record can be kept (See Appendix 2).

PROCEDURES FOR NURSING

Basic Requirements

Students enrolled in the online BSN Completion Program at ENMU conduct their practicums in clinical or educational facilities that are off campus. Students enrolled in nursing practicum courses are required to provide the following credentials to the nursing program as verification:

- Active RN licensure which must be kept current throughout the program
- Immunity to rubella (titer) and to hepatitis B
- Freedom from active tuberculosis: Proof will vary and may include PPD or chest x-ray

- Individual Professional liability insurance
- Current CPR certification

Behavioral expectations from RN's in the workplace include:

- HIPPA compliance
- Avoidance of conflict of interest as pertains to: preceptors, clinical sites and job responsibility
- Dress appropriately for professional presentation by wearing ENMU BSN/MSN identification with uniform, laboratory coat and street attire, or scrubs when representing the BSN Completion program. (no shorts, flip-flops or jeans)
- Punctual attendance for meetings, completing mutually agreed upon activities and initiating communication as necessary with instructor/preceptor/supervisor
- Practice during practicums within the scope of the student role
- Compliance with ID verification using ENMU BSN student badge.
- Adherence to Affiliation Agreements with sites where practicum is performed

24 March 2015

Procedures for reporting violations

If you have violated a HIPPA regulation or you observed someone committing a violation, you are ethically and legally bound to report that violation, first, to your immediate supervisor and second, to the clinic director. The violation must also be submitted to the clinical director in writing so a permanent record of the incident and how the incident was corrected can be made. In addition, once a violation has been reported, the department chair must also be advised orally, via face-to-face or phone call. Do not communicate any violation(s) via electronic means. The department chair must also receive a written copy of the incident. Please, do not wait or delay communication of a violation to your immediate clinic supervisor

and/or the clinical director. The clinic does not want to hear about a violation from the client or their family. We need to be responsive and reactive to any incidence(s) of violations.

The client or parents of a minor client must receive a certified letter describing the violation and whether or not personally identifiable health information was simply available for someone to observe or whether the health information was actually read by or received by another person. Incidents and adverse occurrences that may arise out of the office or practice setting may include but are not limited to leaving client PHI on a desktop display and leaving the room, not protecting files being checked in or out of the file cabinet, or leaving report on printers in general access area. The certified letter must include:

Addressing the violation
Your supervisor and the clinic director in communication under the advisement of the department chair will follow one of the following procedures when a violation occurs.

Student Sanctions:

First Violation (Depending on the seriousness of the violation).
- Write-up detailing how to avoid future violations
- KASA remediation
- Re-take HIPPA training
- Possible fine according to Federal Regulations

Second Violation (Depending on the seriousness of the violation).
- Loss of clinic privileges and hours
- KASA remediation
- Possible program expulsion
- Possible fine according to Federal Regulations

Faculty Sanctions:

First Violation (Depending on the seriousness of the violation).
- Written up
- Probationary status
- Possible fine according to Federal Regulations

Second Violation (Depending on the seriousness of the violation).
- Dismissal
- Possible fine according to Federal Regulations

HIPPA Criminal Penalties

1. Knowingly obtaining or disclosing individually identifiable Health information.
    - $50,000 fine and imprisonment for 1 year
2. Obtaining or disclosing individually identifiable Health information under false pretenses.
    - $100,000 fine and imprisonment for 5 years
3. Knowingly obtaining or disclosing individually identifiable Health information with the intent to sell, transfer, or use the information for commercial advantage, personal gain, or malicious harm.
    - $250,000 fine and/or up to 10 years in prison

Non-compliance with security standards

1. $100.00 per violation up to $25,000.00 per person for all identical violations in a calendar year.
    - This $100.00 amount, up to $1,000.00 per violation due to "reasonable cause and not willful neglect."
2. $10,000.00 for each violation due to willful neglect that is corrected.
3. $50.000.00 for each violation if the violation is not properly corrected.

Procedures for Accountability

Risk Analysis (RA) has been included in the initial writing of this document. A Risk Analysis will be completed every other year or when new rules covering HIPPA are added. The Risk Analysis will include a review of how PHI is handled and by whom. A RA committee or team will be chosen each year to comply with this review requirement. Any finding of problems during a Risk Analysis will be reported to the clinic and department directors for immediate inclusion in an updated copy of this document.

The Risk Analysis Committee will be charged with identifying any problems involving safeguarding patient records, including:

1. To ensure integrity and confidentiality of patient records
2. To protect against reasonably anticipated threats and hazards
3. To protect against unauthorized uses or disclosures of PHI.

Risk Analysis Procedures:

1. Identify PHI for Security of information
2. Identify PHI for Privacy of information
3. Determine what risks exist; describe the risk, causes, and consequences.

Score	Category	Likelihood
1	mild	Unlikely or rare
2	moderate	Likely to occur; risk analysis needed
3	serious	Violation likely; immediate changes needed

4. Determine the likelihood of a breach occurring and any harm that would result
5. What are the new security or privacy measures as a result of #3?
6. Test the new procedures and/or revise this document.

Relevant Terms and Definitions

EHR-Electronic Health Record includes billing by electronic mean, FAX; billing by email, email typed to email equals an electronic transmission. NOT included: paper FAX billing, email with attachment, like paper FAX; ALSO, INCLUDED: internet, movement of electronic media (i.e. flash drive moved between computers equals an electronic record).

HEALTH INFORMATION-Past, present, or future physical or mental health or condition or an individual; provision of health care to an individual; or past, present, or future payment for the provision of health care to an individual.

HEALTH CARE OPERATIONS-are any of the following activities: (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities of the entity, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.

HIPPA-Health Insurance Portability and Accountability Act of 1996; concerned with transmission of medical information

HIPPA SECURITY RULE- specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information.

HITECH ACT-the 2009 amendment to HIPPA to improve patient rights and enforcement

OMNIBUS RULE-established on January 23, 2013

PAYMENT-encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.

PHI-Protected Health Information, The Privacy Rule protects all "individually identifiable health information" including demographic information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

PRIVACY RULE-The patient's right to access records and request copies; to receive Notice of Privacy Practices, Disclosure to family members and other providers, and Notification of breaches of PHI.

TREATMENT-is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.

References

Texas Medical Liability Trust (2005) Risk Management Guidelines for Physician Practices. www.tmlt.org

Tomes, J. P. (2013). HIPPA: Protect your client and yourself. *American Speech Language Hearing Association,* Rockford, MA: ASHA.

Unknown (n.d.*). Family Educational Rights and Privacy Act* (FERPA). ED.gov http://www.2.ed.gov/print/policy/gen/guid/fpco/ferpa/index.html

Appendices

1. Notice of HIPPA Privacy Practices
2. HIPPA violation report and remediation plan
3. Client Letter for Breach Notification
4. Risk Analysis Committee
5. Authorization For Release of a Child
6. Authorization To Release or Obtain Information
7. Permission for Use of Edibles and Other Tactile Items in Therapy
8. Permission to Record and Use Video Excerpts
9. Authorization for Evaluation and Therapy Use of Clinical and Scientific Material and Observation
10. ENMU/CDIS Classroom Confidentiality/Security Policy
11. ENMU/CDIS SHROC Clinical Practicum Confidentiality/Security Policy

Appendix 1

Speech and Hearing Rehabilitation Outreach Center
Eastern New Mexico University
Notice of Privacy Practices

In accordance with the Health Insurance and Portability Act of 1996, I understand that my health care records are Protected Health Information (PHI). This means that all of my ENMU SHROC records are:

1. Confidential and will not be released without my written consent, except under the following, legal, exceptions:

   a. the records are required by the courts,
   b. the records are required by my insurance company, or any third party payee,
   c. no third party records marked as " no discloser" will be released.
2. Afforded anonymity. I understand that my records will be kept using an alphanumeric code that does not contain any personally identifiable information (See Below);
3. Subject to inter-facility communication in order to provide for Best Practices in my care or the care of a minor or disabled person in my care;
4. Protected by the Hi Tech Act. This means that no records will be electronically transmitted either by phone, text, fax or email unless I sign a specific request/release asking you to do so. Requests for records should be addressed to the Clinical Director, Ms. Laura Bucknell and must be made in writing.
5. My health information will be kept in the ENMU Clinic indefinitely as by ENMU policy. Any request for past records needs to be addressed to the Department Chair, Dr. Suzanne Swift.

I understand that I have the right to request that the ENMU SHROC not release my health information to certain parties. This notice is subject to change and/or updates at any time. Updated notices will be distributed to active clinic clients.

My Private Health Information (PHI) and Electronic Records (EHR), or those of a minor or disabled person in my care, may include but not be limited to: personally identifiable information (i.e., date of birth, name, age, social security number, etc.), outside medical or school reports, evaluations, speech therapy session notes, progress reports, and/or any information released to this clinic by a third party or parent/guardian for the purpose of improved patient services.

I understand that I am allowed access to my records and/or copies of my PHI. I may contact the clinic in writing to challenge or correct my PHI. If I know or suspect that my PHI has been handled improperly, I have the right to contact the Clinical Director, Laura Bucknell, verbally and in written form describing the breach of confidentiality.

If you wish to designate a family member or friend to be given access to my PHI please identify them below. You may reverse this decision at any time by informing the clinic in writing.

I hereby designate _____ to have access to my PHI until such time that I withdraw this permission in writing.

I understand and agree to these rights and safeguards or that of a minor or disabled person under my legal guardianship.

_____ _____

Signature of patient/Parent or Guardian of minor or disabled person in my care

Date

Appendix 2

HIPPA Violations
Incidence Report and Risk Assessment

This report details the events related to a reported HIPPA violations in the SHROC Clinic on _____, 20___. _____, clinical supervisor for _____ was told by the student clinician of the following breech: (You must include the nature and extent of PHI involved, whether breach involved security or privacy, type of PHI disclosed and the likelihood of identifying the person, and whether the PHI was acquired or simply viewed).

_____

_____

_____

_____

_____
_____
_____
_____
_____
_____
_____

The following SHROC faculty and staff were advised of the above violation on _____:

_____ _____
Name Title

_____ _____
Name Title

The following corrective action was taken:

_____
_____
_____
_____
_____
_____
_____
_____

The following SHOC faculty and staff were responsible for overseeing the completion of the above corrective action which took place on _____:

_____ _____
Name Title

_____ _____
Name Title

Training for the entire faculty and staff regarding this violation and corrective procedures taken to ensure that the violation does not reoccur was completed on _____,

20___. All faculty and staff signed that they had received this updated training, see attached documentation.

Appendix 3

Breach of Protected Health Information

Dear _____,

This letter is to inform you that on _____ there was a Security or Privacy breach involving your protected health information (PHI). The type of unsecured PHI included _____.

The clinic investigated the breach and as a result took the following action to mitigate the violation and protect against further breaches. _____
_____
_____.

We apologize for any unnecessary distress this may cause you. If you have further questions, please, contact.

Laura Bucknell
SHROC
1500 Ave. K
Lea Hall/ENMU
Portales, NM 88130
575.562.4232

Or

Dr. Suzanne Swift
1500 Ave. K.
Lea Hall/ENMU
Portales, NM
575.562.2724

Appendix 4

Risk Analysis Form

Annually, or as situations demand, SHROC and ENMU HHS/CDIS will perform a Risk Analysis of the procedures applied to a person's PHI under HIPPA. A representative from CDIS, Social Services, Nursing, and one graduate student will constitute a committee for the purpose of Risk Analysis. The following information will be reviewed to assess the adequacy of privacy and security compliance:

Compliance with Security Procedures:

Level of Risk for Security Violations:

Compliance with possible/anticipated Privacy Policies:

Level of Risk for Privacy violations:

Follow through with Implementation of possible/anticipated violation breeches and remediation:

Signatures of Risk Management Committee and completed date of review

_____ _____

Signature Date

_____

Signature

_____

Signature

_____

Signature