

NEW MEXICO STATE UNIVERSITY
PROCEDURES FOR THE PROTECTION
OF
CONFIDENTIAL INFORMATION

As required by the privacy regulations created as a result of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), this document sets forth the procedures for the protection of confidential personal health information at New Mexico State University (NMSU).

The U.S. Department of Health and Human Services issued the Health Insurance Portability and Accountability Act (HIPAA) regulations to protect the confidentiality of personal health care information. Privacy standards within HIPAA (a) limit the use and disclosure of health information, (b) restrict most disclosures of health information to the minimum intended purpose, (c) establish new requirements for access to records by researchers, and (d) protect the confidentiality and integrity of health information. Covered entities are required to comply with HIPAA no later than April 14, 2003. Although New Mexico State University (NMSU) can be considered a “Hybrid Entity” (defined in the Final Rule as a Covered Entity **whose covered functions are not its primary functions**), it has been determined that all NMSU faculty, staff, and students who perform covered functions (e.g., provide health care or have access to health care information) will comply with HIPAA regulations.

HIPAA defines “health information” as any information, whether in oral or recorded form, that (a) is created or received by a Covered Entity, employer, university or school, etc.; and (b) relates to the past, present or future physical or mental health condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual. “Protected health information” (PHI) is defined as Individually Identifiable Health Information maintained or transmitted by a covered entity in any form or medium. PHI includes: (1) demographic information collected from an individual; (2) medical history; (3) information relating to the past, present or future physical or mental health or condition of an individual that is identifiable; (4) the provision of health care to an individual or the payment for the provision of health care; (5) results of physical examinations, blood tests, x-rays; and (6) results of other diagnostic and medical procedures. PHI excludes “de-identified information,” defined as health information that does not identify an individual and with respect to which there is not reasonable basis to believe that the information can be used to identify an individual.

NMSU faculty, staff, and/or students may receive health information from a third party that is protected under applicable state and/or federal law, including without limitation, protected health information (PHI) as defined in the regulations at 45 CFR Parts 160 and 164 (the Privacy Standards) promulgated pursuant to the HIPAA. This information includes such identifiers as:

1. Names;
2. Geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:

- (a) the geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people, or
 - (b) the initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000;
3. All elements of dates (except year) for events directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
 4. Telephone numbers;
 5. Fax numbers;
 6. Electronic mail addresses;
 7. Social security numbers;
 8. Medical record numbers;
 9. Health plan beneficiary numbers;
 10. Account numbers;
 11. Certificate/license numbers;
 12. Vehicle identifiers (VIN) and serial numbers, including license plate numbers;
 13. Device identifiers and serial numbers;
 14. Web universal resource locators (URLs);
 15. Internet protocol (IP) address numbers;
 16. Biometric identifiers, including fingerprints and voice-prints;
 17. Full-face photographic images and any comparable images; and
 18. Any other unique identifying numbers, characteristics, or codes, unless otherwise permitted by the Privacy Rule for re-identification.

NMSU faculty, staff, and students who handle PHI in any aspect of their work and/or instructional learning will comply with HIPAA regulations in the manner provided for in the following procedures.

Use of PHI: NMSU agrees not to use or disclose (or permit the use or disclosure of) PHI in a manner that would violate the requirements of the Privacy Standards. NMSU shall permit the use of PHI solely for the University's benefit and only (a) for the purpose of performing services for the University, and (b) as necessary to carry out its legal responsibilities, provided that such uses are permitted under federal and state law. Appropriate safeguards shall be used to prevent the use or disclosure of PHI other than as expressly permitted in writing by the appropriate individual. Individuals shall retain all rights to the PHI, unless otherwise granted to NMSU. Use and disclosure of de-identified health information is not permitted unless expressly authorized in writing by the appropriate representative. NMSU shall permit the use or disclosure of PHI for the purpose of research only in the following circumstances: (1) upon the signing of a written authorization by the individual that meets the content requirements of the Privacy Rule; (2) upon the granting of an appropriate "waiver of authorization" by its duly constituted Institutional Review Board (IRB); (3) upon receipt of appropriate representations from the researcher, for "reviews preparatory to research," and (4) upon similar representations, for research on decedent's information. The core elements of such authorizations are:

1. A description of the PHI to be used or disclosed, identifying the information in a specific and meaningful manner;

2. The names or other specific identification of the person or persons (or class of persons) authorized to make the requested use or disclosure;
3. The names or other specific identification of the person or persons (or class of persons) to whom the University may make the requested use or disclosure;
4. A description of each purpose of the requested use or disclosure;
5. Authorization expiration date or expiration event that relates to the individual or to the purpose of the use or disclosure;
6. Signature of the individual and date – if the individual’s legally authorized representative signs the authorization, a description of the representative’s authority to act for the individual must also be provided.

The following statements are required on all authorizations:

1. A statement of the individual’s right to revoke his/her Authorization and how to do so, and, if applicable, the exceptions to the right to revoke his/her Authorization or reference to the corresponding section of the covered entity’s notice of privacy practices;
2. Whether treatment, payment, enrollment, or eligibility of benefits can be conditioned on the Authorization, including research-related treatment and consequences of refusing to sign the Authorization, if applicable; and
3. A statement of the potential risk that PHI will be re-disclosed by the recipient – this may be a general statement that the Privacy Rule may no longer protect health information disclosed to the recipient.

Authorizations to use and disclose PHI must be written in plain language so that it is understood by all appropriate parties and must contain the core elements and required statements. A signed copy must be provided to the individual signing it.

The IRB may grant a “waiver of authorization” permitting the disclosure of PHI to, and use of PHI by, a researcher. In order to do so, the IRB must first find that certain conditions are satisfied:

1. The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:
 - (a) an adequate plan to protect the identifiers from improper use and disclosure;
 - (b) an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or a legal requirement to retain them; and
 - (c) adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of PHI would be permitted under the Privacy Rule;
2. The research could not practicably be conducted without the waiver or alteration; and
3. The research could not practicably be conducted without access to and use of the PHI.

The IRB will not grant waivers for disclosures of psychotherapy notes. Such disclosures shall require the appropriate individual’s and/or legal representative’s authorization.

When a research project is conducted at multiple sites and/or requires the use and disclosure of PHI created or maintained by more than one entity, the University will rely on a waiver or an alteration of authorization approved by any IRB or Privacy Board, without regard to the location of the IRB or Privacy Board approving it, provided the researcher notifies the IRB of such prior review of the research protocol. The researcher will provide the IRB with copies of the appropriate documentation.

Disclosure of PHI: NMSU may disclose PHI as necessary to perform its obligations as an educational institution of higher education and as permitted by law, provided that it has (a) obtained reasonable assurances from any person to whom the information is disclosed that the information will be held confidential and further used and disclosed only as required by law (including by statute, regulation, or court orders) or for purposes for which it was disclosed to the person or entity; (b) been assured that NMSU will be immediately notified of any instances of which the receiving party is aware that PHI is being used or disclosed for a purpose other than that for which it was provided or for a purpose not expressly permitted by the Privacy Standards; and (c) ensured that all disclosures of PHI are subject to the principle of “minimum necessary use and disclosure,” i.e., only the minimum PHI that is necessary to accomplish the intended purpose will be disclosed. If NMSU discloses PHI received from a third party, or created or received by NMSU on behalf of a third party, to individuals external to NMSU, the NMSU shall require Recipients to agree, in writing, to the same restrictions and conditions that apply to NMSU. In certain circumstances, NMSU may disclose PHI: (a) to appropriate government authorities regarding victims of abuse, neglect, or domestic violence; (b) to comply with workers’ compensation laws and other similar programs providing benefits for work-related injuries or illnesses; or (c) to law enforcement entities if the information is believed necessary to prevent or lessen a serious and imminent threat to a person or the public.

Use of De-Identified Data: The IRB shall consider data to be de-identified data if (a) all of the identifiers specified above (i.e., name, address, phone number, dates of service, social security number, medical record numbers, etc.) have been removed from the relevant data set; or (b) a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable certifies that there is a “very small” risk that the information could be used by the recipient to identify the individual who is the subject of the information, alone or in combination with other reasonably available information. The person certifying statistical de-identification must document the methods used and the result of the analysis that justifies the determination. This certification shall be provided, in written or electronic format, to the Compliance Office in the Office of the Vice Provost for Research at NMSU, where it will be retained for at least six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

Rights Regarding Designated Records Sets: If NMSU maintains a designated record set on behalf of a Covered Entity, NMSU shall permit the Covered Entity to inspect or copy PHI contained in that set under the conditions and limitations required under 45 CFR 164.524, as it may be amended from time to time. The Covered Entity must specify in a business associate contract issued to NMSU when (1) NMSU must make such PHI available if and when needed by the Covered Entity to provide an individual with access to the information; (2) NMSU is to provide access to individuals, as may be appropriate where NMSU is the only holder of the designated record set, or part of the designated record set; and (3) NMSU is to amend the PHI about an individual in a designated record set, including any designated record sets (or copies thereof) held by NMSU.

Researcher's Responsibilities: Once the IRB has authorized a researcher to use and/or disclose PHI, the researcher (a) may only use or disclose the PHI in the manner and for the purposes expressly permitted by the approved human subjects application, and (b) must abide by all limitations, safeguards, and prohibitions expressly included or incorporated by reference in the human subjects application. PHI in research records cannot be re-used or re-disclosed for any other research study in the future without a new approval from the IRB. The researcher will keep all records containing PHI in a secure area, in locked files available only to authorized research personnel. Electronic records will be kept in a special password-protected database and made available only to legally authorized individuals. Oral communications will be held in private areas that minimize the chances of being overheard. All authorized research personnel will be informed about the policies and procedures that apply to the disclosure of confidential PHI. Telephone answering machines should never be used to transmit PHI. If the intended recipient of a telephone call is not available, the researcher must request a callback or a telephone appointment. If information is to be transmitted by e-mail, an attempt must be made to de-identify all confidential information. E-mails containing confidential information must have the prominent notice that the information is confidential. The following notice is acceptable: "CONFIDENTIALITY NOTICE: This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, and/or privileged information protected by law. If you are not the intended recipient, you may not use, copy, or distribute this e-mail message or its attachments. If you believe you have received this e-mail message in error, please contact the sender by reply e-mail and destroy all copies of the original message." All facsimile transmissions must be sent with both a cover sheet and a tail sheet that are both prominently marked "CONFIDENTIAL." All sensitive documents must be removed from fax machines (and printers) as soon as practicable.

Accounting of PHI Disclosures: The researcher will not make an individual's study-related PHI available to anyone in the future, unless authorized to do so in writing by the affected individual and/or a legally authorized representative. Upon written notice to the researcher, individuals will have the right to inspect and obtain copies of their research records, and to request amendments to those records. The researcher shall keep an accounting of all disclosures of PHI from the research files. All accounting records must include the following information for each disclosure: the date the disclosure was made; the name and address of the person or entity receiving the PHI; a brief description of the PHI disclosed; a brief statement of the reason for the disclosure; the accounting contact person; and the number of requests and accountings provided to the individual. The accounting records must be retained for a period of six (6) years, regardless of whether the disclosure was made orally, by telephone, or in writing. An accounting of the records of such disclosures shall be made available to the appropriate individuals upon their or their legally authorized representative's written request.

Disposal of PHI Records: All documents containing PHI data will be either cross-cut shredded on site or stored in secure bags or containers until off-site shredding can be completed. If PHI data are kept on CDs, diskettes, or recording audiotapes/videotapes, all CDs will be broken into multiple pieces; all diskettes will have their magnetic media cut into multiple pieces or "scrubbed" with a data destruction utility; and all audiotapes and/or videotapes will be removed from the case and shredded for disposal.

Violation of Use or Disclosure of PHI: The IRB and/or individuals shall report to the Director of Compliance and/or Vice Provost for Research at NMSU any harmful effect of the impermissible use or disclosure of PHI of which they become aware. Such reporting must be done within five (5) working days of the discovery of such impermissible use or disclosure. All complaints will be sent to the Director of

Compliance at the following address:

Director of Compliance
Office of the Vice Provost for Research, MSC 3RES
New Mexico State University
Box 30001
Las Cruces, New Mexico 88003-8001

NMSU shall make every reasonable effort to mitigate, to the extent practical and unless otherwise requested in writing, any harmful effect that is known and is the result of the violation in the use or disclosure of PHI within 30 days of the violation's discovery. If NMSU is not able to mitigate the harmful effect, the violation will be reported to the U.S. Department of Health and Human Services (DHHS), Office for Civil Rights. An individual who knowingly obtains or discloses individually identifiable health information in violation of HIPAA faces a fine of \$50,000 and up to 1 year of imprisonment. The criminal penalties increase to \$100,000 and up to 5 years of imprisonment if the wrongful conduct involves false pretenses, and to \$250,000 and up to 10 years of imprisonment if the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. Criminal sanctions will be enforced by the Department of Justice. DHHS may impose civil money penalties on the University of \$100 per failure to comply with a Privacy Rule requirement. That penalty may not exceed \$25,000 per year for multiple violations of the identical Privacy Rule requirement in a calendar year.