Executive Memorandum No. 27

HIPAA Compliance Policy (effective April 14, 2003)

Purpose

It is the purpose of this Executive Memorandum to set forth the Board of Regents' and the University Administration's Policy committing the University to compliance with applicable mandates of the Administrative Simplification provisions, Title II, of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

Definitions

Compliance plan or ***plan*** means a coordinated set of policies, procedures, forms and other steps which, when taken together and applied and enforced according to their terms, will permit the University or a covered component of the University to comply with its obligations under HIPAA.

Covered component means an operating unit of the University which conducts activities that makes it subject to HIPAA. There are ***directly covered components***, such as UNMC, which engage directly in one of the three activities covered by HIPAA – provider activities, health plan activities and clearinghouse activities. There are also ***supporting components***, such as campus business offices, which may perform functions on behalf of directly covered components and create or receive and use protected health information to do so. Both are covered components under this Policy.

Group health plans sponsored by the Board of Regents are also treated as "covered components" under this Policy, even though they will require separate Compliance Plans.

Covered transaction means an electronic transaction conducted by a covered component that is subject to the HIPAA transaction standards.

Protected health information means information that relates to past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for health care to an individual, which identifies the individual or as to which there is a reasonable basis to believe could be used to identify the individual.

Safeguard means a physical, technical or administrative action which is designed to achieve or help meet a privacy or security objective.

Transaction standard means a mandatory standard for conducting covered transactions. The transaction standards are adopted as federal regulations at 45 C.F.R. Part 162.

Governing Legal Authorities

1. Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d to 1320d-8).

2. 45 C.F.R. Parts 160 and 162 – Final HIPAA standards for electronic transactions.

3. 45 C.F.R. Parts 160 and 164 – Final HIPAA privacy regulations (the "Privacy Rule").

4. Final Security Rule when adopted and effective. A Final Security Rule (the "Security Rule") is expected to be codified at 45 C.F.R. Part 142.

5. Final enforcement regulations when adopted and effective.

6. Other federal and state law to the extent that such other federal or state law conflicts with and preempts a provision of HIPAA.

Applicability

This Policy applies to all covered components of the University and all personnel who are subject to the Board of Regents' jurisdiction.

The University will appoint a privacy officer charged with overall responsibility to assure University-wide compliance as described in this Policy. Each University campus shall be responsible to assist in implementing this policy in a manner best suited to its own organization and to cooperate with the Privacy Officer.

Privacy Officer

The University Risk Manager/Privacy Officer will serve as the Privacy Officer for the University as a whole. The Privacy Officer reports to the Vice President for Business and Finance. The Privacy Officer is responsible to develop and implement or review and approve individual compliance plans for all covered components of the University.

The Privacy Officer is to have the assistance of the Chancellors, Central Administration and everyone else subject to this Policy.

The Privacy Officer will:

1. Identify and describe in a comprehensive University-wide policy all covered components of the University, including those that are covered solely as supporting components.

2. Assure that all covered components are included in a HIPAA Compliance Plan which meets the requirements of this Policy. In the case of UNMC, this will be the Plan adopted by UNMC and the other participants in the affiliated covered entity arrangement. In the case of other covered components (other than group health plans), this may be a single University Plan or a combination of Plans recommended by the covered components and approved by the Privacy Officer. In the case of group health plans, these may be individual Plans or a joint Plan if the group health plans qualify and elect to enter into an organized health care arrangement for HIPAA purposes.

3. Assist the various covered components to develop Plans fitting their activities.

4. Advise Central Administration on progress toward compliance. Current compliance dates are:

    a. Privacy Rule – April 14, 2003 (April 14, 2004 for any group health plans which qualify as small group health plans).

    b. Transaction standards – October 16, 2003.

    c. Other mandates – as specified in final federal regulations as and when adopted.

5. Serve as the designated official to receive complaints and to provide additional information about matters covered in the University's privacy notices, unless an individual Compliance Plan designates another person with that responsibility for the component or components covered by such Plan.

6. Promptly investigate or assist legal counsel to investigate patient, workforce or other complaints alleging noncompliance with HIPAA or with a Plan, unless that function is delegated to another person in an individual Compliance Plan.

7. Initiate efforts to mitigate the adverse effects of improper disclosure of protected health information, through direct action or in collaboration with others, unless that function is delegated to another person in an individual Plan.

8. Carry out other HIPAA-related responsibilities as are assigned from time to time.

Affiliated Covered Entity Arrangement

In its Resolution, the Board authorized entering into an affiliated covered entity arrangement with Nebraska Health System, University Medical Associates and University Dental Associates for the purpose of assuring a coordinated campus-specific HIPAA Compliance Plan for the UNMC campus. Upon approval of the affiliated covered entity arrangement by all parties, the University will enter into an affiliated covered entity agreement under which the parties will:

1. Jointly develop and implement a HIPAA Compliance Plan specific to their operations;

2. Designate individuals to serve as the HIPAA Privacy Officer and security official under their joint HIPAA Compliance Plan;

3. Bear their respective costs of compliance; and

4. Agree to be individually responsible for their respective breaches of the HIPAA Compliance Plan.

Covered Entities and Covered Components

HIPAA directly regulates four types of entities based on the activities they perform.

1. Covered Health Care Providers

   A covered health care provider is a provider of health care which transmits any health information electronically in connection with a standard transaction. Terms are broadly defined and inclusive. A health care provider includes any person or organization "who furnishes, bills or is paid for health care in the normal course of business." Health care includes:

   "(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment or procedure with respect to the physical or mental condition, or functional status of an individual or that affects the structure or function of the body; and

   (2) Sale or dispensing of a drug, device, equipment, or other items in accordance with the prescription."

   Applying these broad definitions, there are *many* health care provider activities conducted on University campuses, although relatively few will be *covered* health care provider functions because

they do not couple the provider activity with the second part of the test – transmitting health information electronically in connection with a standard transaction.

An early goal of this Policy is to identify all covered health care provider components of the University so that they can be appropriately included in compliance planning.

2. Health Plans

Health plans are individual and group plans that provide or pay the cost of medical care. Various University departments deal regularly with health plans, such as Blue Cross, Medicare and CHAMPUS.

Health plans also include "group health plans" covering medical benefits on behalf of University employees and their dependents. The Board of Regents sponsors several group health plans providing medical, dental, vision, pharmacy, and long-term care benefits. These group health plans are treated as separate covered entities under HIPAA and need their own approach to the transactional standards, privacy and security.

3. Health Care Clearinghouses

Health care clearinghouses are entities (or internal departments) which convert or facilitate converting data from non-standard-to-standard data elements or vice versa. For example, a covered student health center may not prepare claims according to the transaction standards, but a campus department or a third-party vendor may do so on its behalf in order to bill a health plan. This is a clearinghouse function.

4. Hybrid Entities

A hybrid entity is a covered entity that engages in both covered and non-covered functions. The University of Nebraska is a hybrid entity.

The University must designate its covered components (its covered health care provider, health plan and health care clearinghouse components). The University will do this by separate policy adopted by the President or the Privacy Officer once all covered components have been identified through the campus-specific and Central Administration planning process.

How the University is affected by HIPPA

HIPAA imposes three broad rules on covered entities. These rules must be converted into operating policies and safeguards.

1. Transaction Standards

Effective October 16, 2003 (unless an extension is granted), all covered entities transmitting health information electronically in connection with a standard transaction must follow uniform transaction standards. The transactions for which transaction standards have been adopted are:

- Health care claims or equivalent encounter information transaction.
- Eligibility for a health plan transaction.
- Referral certification and authorization transaction.
- Health care claim status transaction.
- Enrollment and disenrollment in a health plan transaction.
- Health care payment and remittance advice transaction.
- Health plan premium payment transaction.

- Coordination of benefits transaction
- Health claim attachment transaction (proposed).

The government is working to develop and publish other transaction standards as well.

The impact of the transaction standards on the University can be illustrated as follows:

a. If a student health center electronically queries a health plan's data base to determine whether a student receiving services is enrolled in the health plan, it is conducting a standard transaction electronically and the transaction must meet the published transaction standards.

b. If a student health center turns over encounter information to a campus business office and the business office files claims electronically with a payer, the transaction is a covered transaction and must meet the published transaction standards. Moreover, in this case, *both* the student health center and the supporting campus business office are *covered* components when it comes to implementing the HIPAA Privacy Rule and Security Rule.

2. Privacy Rule

Effective April 14, 2003 (unless an extension is granted), the University must have deployed reasonable and appropriate physical, technical and administrative safeguards (i) to ensure the confidentiality of protected health information; (ii) to protect against reasonably anticipated unauthorized uses or disclosures of protected health information; and (iii) to otherwise ensure compliance with the HIPAA Privacy Rule by all members of its workforce.

The Privacy Rule applies to *covered entities*, rather than *covered transactions*. Once a component of the University becomes a covered component (for example, because it is a provider component and it transmits health information electronically in connection with one or more standard transactions), the component becomes subject to the mandates of the Privacy Rule. This applies both to the directly-covered component (the student health center that is a provider component) and the supporting component (the business office that files the claim or audits its operations).

The Privacy Rule includes rigorous privacy standards and affords individuals new rights to access, control and know how their information is used and disclosed.

3. Security Rule

Based on the statute itself, the Security Rule, when final, will require the University to deploy reasonable and appropriate administrative, technical and physical safeguards (i) to ensure the integrity of health information; (ii) to protect against any reasonably anticipated threats or hazards to the security or integrity of health information; and (iii) to otherwise ensure compliance with a Final Security Rule by the workforce.

Many elements of the proposed Security Rule are already in place at the University because they represent something of industry standards or best practices. Also, even though final compliance with the Security Rule will not be required until a Final Security Rule and a final compliance date are published, many security steps are essential in order to support privacy. Therefore, initial HIPAA Compliance Plans which are targeted *mainly* at meeting applicable transaction standards and the Privacy Rule will be expected to incorporate and build upon supporting security principles.

Standards for Adoptions of Compliance

Compliance Plans should be developed and implemented within the following parameters:

1. Plans should be effective. The Board and the University's administration are committed to compliance. The most important criterion in judging safeguards and elements of a Plan will be effectiveness.

2. Plans should be reasonable, affordable and workable in light of our resources and experience.

3. Plans should address foreseeable threats to privacy and integrity of health information.

4. Plans should use common sense and experience and draw on the experience of our workforce in assessing threats and implementing safeguards.

5. Plans should be understandable. Everyone subject to a Plan should be able to understand the rules that apply to his or her job.

6. Plans should be enforceable. They should contain appropriate sanctions for violators and the sanctions should be enforced.

7. Plans should be dynamic. They should evolve with our organizational experience and understanding of the law and with changes in the law.

8. Plans should address the applicable transactional standards and the privacy and security requirements, with the understanding that Plans will need to be amended following adoption of final security regulations and thereafter, from time to time, as necessary, to remain current and effective.

Elements of HIPAA Compliance Plans

1. **Governing Policy**. The Plan will govern all access to, and use and disclosure of, protected health information. Policy and training will distinguish these functions and emphasize everyone's need to tailor access, use or disclosure to appropriate authority and permitted functions.

2. **Privacy Official; Security Official; Reporting**. Each Plan will designate a Privacy Officer and a security official. The Privacy Officer's responsibilities will include serving as a resource on HIPAA, answering questions, processing complaints and helping with non-routine matters. Anyone uncertain as to the application of HIPAA or the Plan to a given situation should contact the Privacy Officer for assistance. Anyone knowing or suspecting violation of this Policy or the supporting policies and procedures of the HIPAA Compliance Plan must immediately report the known facts and concerns to the Privacy Officer. Failure to immediately report a known or suspected violation is grounds for discipline.

3. **Compliance with Minimum Necessary Standard (§ 164.502(b), § 164.514(d))**. The Plan should emphasize appropriate technical safeguards, policies and training to limit access and use and to remind everyone that HIPAA formally imposes a "needs to know" rule and that there are severe enforcement consequences to the organization if it is not followed.

4. **Disclosures to Business Associates (§ 164.502(e), § 164.504(e))**. All business associate relationships will be memorialized in business associate contracts in the form specified in detailed business associate policies. Business associates should be properly identified and should have access to protected health information only after giving satisfactory written contractual assurances that they will use, safeguard and disclose protected health information in accordance with their assurances.

5. **Privacy Notice (§ 164.520)**. Individuals have the right under HIPAA to know how the University will use and disclose their protected health information. Everyone subject to this Policy will receive training and is expected to be familiar with the content of the Privacy Notice applicable to them. Separate covered components with separate Compliance Plans may have separate Privacy Notices.

The Privacy Notice for the parties participating in the affiliated covered entity arrangement will be specific to the Compliance Plan adopted by them. Privacy Notices for group health plans will be separate from Privacy Notices for other covered components. Group health plans which qualify and elect to participate in an organized health care arrangement may adopt a joint Privacy Notice. Protected health information should be used and disclosed only in accordance with the applicable Privacy Notice.

6. **Uses and Disclosures of Protected Health Information for Marketing and Fundraising (§ 164.508(a), § 164.514(f))**. The University will use or disclose protected health information for marketing and fundraising activities only in accordance with the final Privacy Rule and applicable Privacy Notice.

7. **Right to Request Restriction on Use or Disclosure of Protected Health Information (§ 164.522(a))**. Individuals have the right to request specific restrictions on (i) our uses and disclosures of protected health information for treatment, payment and health care operations; and (ii) our disclosures to individuals involved in the individual's care. Such requests must be processed in accordance with specific procedures, to include the steps following the denial or approval of such request. Each Plan should state that restrictions can only be approved if (i) approval will not breach any assurances given to others (such as in an affiliated covered entity arrangement, under an organized health care arrangement, to business associates, or as a business associate); (ii) the University has an effective means to assure that all personnel and departments will know of and can practically comply with the restriction; and (iii) agreeing to the restriction will not be contrary to another policy. Only limited persons to be specified in the individual Plans may agree to a restriction.

8. **Confidential Communications (§ 164.522(b))**. Individuals have the right to request to receive communications of protected health information by alternative means or at an alternative address. Each Plan should require the affected components to accommodate these requests where feasible. Only persons specified in Plans may agree to special arrangements. When considering or agreeing to special arrangements, personnel must determine if and how the arrangements can be effectively communicated to all personnel and departments covered by the Plan who may be subject to the arrangement.

9. **Access by Individuals to Their Own Protected Health Information (§ 164.524)**. Individuals have the right, subject to limited exceptions, to inspect and copy their protected health information maintained by the University in designated record sets. The procedures, fees, timeframes, exceptions and personnel authorized to handle requests shall be set forth in policies and shall be consistent with HIPAA. Plans will define designated record sets for each covered component. All requests for access and copies must be referred for processing to personnel designated in the Plans.

10. **Amending Protected Health Information (§ 164.526)**. Individuals have the right to request amendment of their protected health information maintained by us in designated record sets. In many circumstances, the University is not obligated to agree to the amendment, such as when the information is accurate and complete. However, our goal should be to try to make certain that our protected health information is accurate. The procedures, timeframes, exceptions and personnel authorized to handle requests, and persons authorized to make the final decision, should be set forth in detailed policies as part of individual Plans. Special care must be taken to make certain that all personnel and departments, and all business associates, who maintain, use or disclose the protected health information which is the subject of the request to amend, are notified of any amendments which are adopted, and are furnished with information which should accompany any further disclosures of protected health information by them (whether or not the amendment is adopted).

11. **Accounting for Disclosures of Protected Health Information (§ 164.528)**. Upon request, the University will provide individuals with an accounting of certain disclosures made by us or our business associates. The procedures, fees, timeframes, exceptions and personnel authorized to handle

requests shall be set forth in individual Plans. All requests for an accounting must be referred for processing to personnel designated in the Plans.

12. **Personnel Designations (§ 164.530)**. The Privacy Officer identified in each Plan will be responsible to develop and implement the policies and procedures of the organization and to oversee HIPAA compliance. Individual Plans will also designate a contact person for receiving complaints to the University, if other than the Privacy Officer, and for providing additional information regarding our privacy practices.

13. **Education and Training (§ 164.530(b))**. Each Plan will require a commitment to initial and ongoing training. It is to be a condition of continued employment or assignment that all individuals covered by a Plan participate in and successfully complete initial and periodic HIPAA training appropriate to their responsibilities and their need for access to and use of protected health information.

14. **Safeguards (§ 164.530(c))**. The University has taken and will continue to take appropriate steps to identify threats to the privacy (and security) of protected health information and to identify and implement reasonable and appropriate physical, technical and administrative safeguards to deal with foreseeable threats. Physical safeguards will be designed to assure that the University's physical surroundings are conducive to maximum privacy. Technical safeguards and systems will be designed to secure protected health information from unauthorized use or disclosure and to support the privacy policies described and referred to herein.

15. **Complaints (§ 164.530(d))**. Each Plan will define the procedures for individuals to complain regarding information practices. The procedures will be described in the Privacy Notice. Complaints or questions about filing and pursuing complaints should be directed to an appropriate person. The complaint policy and the Privacy Notice should also describe how to file complaints directly with the Secretary or the Office of Civil Rights of the United States Department of Health and Human Services.

16. **Sanctions (§ 164.530(e))**. The University will appropriately sanction anyone subject to this Policy who fails to comply with a Plan and the related policies and procedures applicable to them. Sanctions may be imposed not only for improper use and disclosure of protected health information, but also for failure to immediately notify the designated official of known or suspected violations of a Plan or of known threats to the privacy or security of protected health information in the University's control.

17. **Refraining from Intimidating or Retaliatory Acts (§ 164.530(g)**. The University will not intimidate, threaten, coerce, discriminate or retaliate against an individual who exercises any right described in this Policy, including the filing of a complaint, testifying, assisting with or participating in an investigation or providing information in connection with a compliance review or hearing.

18. **Waiver of Rights (§ 164.530(h))**. The University will not require an individual to waive his or her right to file a complaint with the Secretary of Health and Human Services as a condition to providing treatment.

19. **Changes to Privacy Practices Stated in the Privacy Notice (§ 164.530(i)(4))**. Under a Plan and in each Privacy Notice itself, the University shall reserve the right to change its privacy practices and Privacy Notice. In the case of change, the University will comply with notice and posting requirements. The Privacy Notice must reference this reserved right.

20. **Policies and Procedures (§ 164.530(i)(1))**. The University or the individual covered component will develop and implement supporting policies and procedures, as needed, to make each Plan an effective Compliance Plan. The University will review and revise its policies and procedures, as necessary, and appropriate, from time to time, to maintain their effectiveness. The University will adopt

additional compliance policies with supporting policies and procedures, as needed, to implement the other parts of HIPAA, such as HIPAA security, when finalized, that directly apply to the University.

21. **Documentation and Record Retention (§ 164.530(j))**. HIPAA records will be identified and retained according to a detailed HIPAA records policy. All records identified as HIPAA records must be retained for the minimum period set by regulation, currently six years, in either written or electronic form, and may be retained for longer periods if provided in a Plan. An effort must be made to identify and retain indefinitely the records documenting the selection and development of individual HIPAA policies and safeguards.

22. **FERPA. (§ 164.501 "*protected health information*")**. Plans will appropriately identify student education records which are not subject to the HIPAA Privacy Rule because they are governed by privacy mandates under the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g *et seq*. Privacy safeguards adopted for records covered by HIPAA may be applied to records covered by FERPA, so long as not in conflict with FERPA. Covered components whose records are not subject to the HIPAA Privacy Rule because of FERPA will separately determine if they are subject to the HIPAA transactional standards for their covered transactions or to the Security Rule when adopted.

23. **Transaction Standards**. Plans will identify all covered transactions conducted by the components covered by the Plan. All covered transactions conducted electronically after the compliance date must meet published and effective transaction standards.

Reference: August 21, 2003