Executive Memorandum No. 27

HIPAA Compliance Policy

Purpose

It is the purpose of this Executive Memorandum to set forth the Board of Regents' and the University'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"), as amended.

Definitions

Covered component means an operating unit of the University that conducts activities that make it subject to HIPAA. There are ***directly covered components***, such as the University of Nebraska Medical Center ("UNMC"), which engage directly in covered 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.

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

Hybrid entity means a covered entity that is a single legal entity that conducts both covered and non-covered functions.

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.

Workforce means any individual, whether employed by, leased to, or a volunteer of, the University whose assigned responsibilities are to support a covered component of the University.

Governing Legal Authorities

1. Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d to 1320d-8), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, Public Law 104-191.

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

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

4. 45 C.F.R. Part 142 – Security Rule (the "Security Rule").

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 Workforce as defined herein.

Group health plans sponsored by the Board of Regents are considered separate covered entities under HIPAA and will be governed by separate HIPAA compliance policies.

Hybrid Entity and Covered Components

By Resolution, the University has declared itself a Hybrid Entity. The President of the University of Nebraska is authorized to and shall be responsible for designating and documenting the covered and non-covered components of the University and such designation shall be effective without further action on the part of the Board of Regents. References herein to the University shall mean the covered components of the University as so designated.

Affiliated Covered Entity Arrangement

By Resolution, the University of Nebraska Medical Center (a covered component of the University) participates in an Affiliated Covered Entity arrangement with The Nebraska Medical Center (formerly known as Nebraska Health System), UNMC Physicians (formerly known as University Medical Associates), University Dental Associates, Bellevue Medical Center, LLC, and Nebraska Pediatric Practice, Inc. for the purpose of assuring coordinated HIPAA compliance across these affiliated entities. Affiliated Covered Entity participation is solely for the purposes stated above and shall not have the effect of creating a new legal entity, merging or consolidating existing entities, merging or consolidating their operations, or in any way impairing the corporate and organizational separateness between the covered entities participating in the Affiliated Covered Entity.

Privacy Officer and Security Officer

The University has appointed a Privacy Officer and a Security Officer each charged with overall responsibility to assure University-wide compliance as described in this Policy, respectively, as

applicable to their roles. Each covered component shall be responsible to assist in implementing this Policy in a manner best suited to its covered activities and to cooperate with the Privacy Officer and Security Officer. The University Chief Compliance Officer/Privacy Officer serves as the Privacy Officer, and the University Chief Information Security Officer serves as the Security Officer, for all covered components of the University that are not included in the Affiliated Covered Entity. The members of the Affiliated Covered Entity separately appoint a Privacy Officer and Security Officer for Affiliated Covered Entity activities.

The Privacy Officer will:

1. Periodically review and approve, and ensure implementation of, policies and procedures in support of this HIPAA Compliance Policy for all covered components of the University.

2. Serve as the designated official to receive complaints and to provide additional information about matters covered in the University's privacy notices, unless delegated by policy to another person with that responsibility for a particular covered component.

3. Promptly investigate or assist legal counsel to investigate patient, Workforce or other complaints alleging noncompliance with HIPAA or with a policy or procedure implemented under this HIPAA Compliance Policy, unless delegated by policy to another person with that responsibility for a particular covered component.

4. 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 by policy to another person with that responsibility for a particular covered component.

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

The Security Officer will:

1. Ensure a sufficient and appropriate level of training is provided to all members of the Workforce regarding their responsibilities with respect to the security of protected health information.

2. Assist with contingency planning efforts and categorizing information (or specific application systems) according to a criticality scale.

3. Understand the permissible uses and disclosures, and potential risks associated with, protected health information.

4. Protect the protected health information in the University's possession from unauthorized access, alteration, destruction or usage.

5. Identify and administer general controls such as back-up and recovery systems consistent with the University's policies and standards.

6. Establish, monitor and operate information systems in a manner that is consistent with the University's policies and standards.

Additional Core Elements of this HIPAA Compliance Policy and Supporting Policies

In addition to the above elements, the University will adopt supporting policies and procedures to implement the following core elements of a comprehensive HIPAA compliance program. All such policies and procedures shall become a part of this HIPAA Compliance Policy.

1. **Compliance with Minimum Necessary Standard (§ 164.502(b), § 164.514(d))**. The University will implement appropriate technical safeguards, policies and training to limit access and use to the minimum amount of information necessary to carry out the function requiring access or use of protected health information.

2. **Disclosures to Business Associates (§ 164.502(e), § 164.504(e))**. All business associate relationships will be memorialized in business associate contracts. 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.

3. **Privacy Notice (§ 164.520)**. Individuals have the right under HIPAA to know how the covered components of the University will use and disclose their protected health information. The University will distribute a Notice of Privacy Practices ("Privacy Notice") in accordance with the requirements of the Privacy Rule. The Privacy Notice for the members of the Affiliated Covered Entity will be specific to the Notice adopted by the Affiliated Covered Entity. Protected health information should be used and disclosed only in accordance with the applicable Privacy Notice.

4. **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 Privacy Rule and applicable Privacy Notice and policies.

5. **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) University uses and disclosures of protected health information for treatment, payment and health care operations; and (ii) University 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.

6. **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. Such requests must be processed in accordance with specific procedures, to include the steps following the denial or approval of such request.

7. **Access by Individuals to Their Own Protected Health Information (§ 164.524)**. Individuals have the right, subject to certain exceptions, to inspect and copy their protected health information maintained by the University in designated record sets and to direct the University to send a copy of their protected health information to a third party. The procedures, fees, timeframes, exceptions and process for individuals to request access shall be set forth in policies and shall be consistent with HIPAA. Policies will define designated record sets for each covered component.

8. **Amending Protected Health Information (§ 164.526)**. Individuals have the right to request amendment of their protected health information maintained by the University 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. The procedures, timeframes, exceptions and process for individuals to request access, and persons authorized to make the final decision, shall be set forth in policies and shall be consistent with HIPAA. Such policies will set forth obligations of the University for handling the request and related actions, including but not limited to and any notification to third parties, including business associates, as may be required.

9. **Accounting for Disclosures of Protected Health Information (§ 164.528)**. Upon request, the University will provide individuals with an accounting of certain disclosures made by the University or University business associates. The procedures, fees, timeframes, exceptions process for individuals to request an accounting shall be set forth in policies and shall be consistent with HIPAA.

10. **Personnel Designations (§ 164.530)**. The Privacy Officer and Security Officer appointed by the University will be responsible to develop and implement the policies and procedures of the organization and to oversee HIPAA compliance.

11. **Education and Training (§ 164.530(b))**. All Workforce will be required to 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.

12. **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.

13. **Complaints (§ 164.530(d))**. The University will maintain procedures for individuals to complain regarding the University's information practices or its compliance with HIPAA. The procedures will be described in the Privacy Notice. Complaints or questions about filing and pursuing complaints should be directed to an appropriate person as designated in policy. The complaint policy and the Privacy Notice describe how to file complaints directly with the Secretary or the Office for Civil Rights of the United States Department of Health and Human Services.

14. **Sanctions (§ 164.530(e))**. The University will appropriately sanction anyone subject to this Policy who fails to comply with this Policy or 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 policy or of known threats to the privacy or security of protected health information in the University's control.

15. **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.

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

17. **Changes to Privacy Practices Stated in the Privacy Notice (§ 164.530(i)(4))**. The University reserves the right to change its privacy practices and Privacy Notice and will describe this reserved right in the Privacy Notice. In the case of change, the University will comply with notice and posting requirements.

18. **Policies and Procedures (§ 164.530(i)(1))**. The University or the covered component has implemented supporting policies and procedures, as needed, to make this Policy an effective HIPAA Compliance Policy. The University will review and revise its policies and procedures as necessary and appropriate from time to time to maintain their effectiveness.

19. **Documentation and Record Retention (§ 164.530(j))**. All records identified as HIPAA records must be retained for the minimum period set by regulation, currently six years from the date last in effect, in either written or electronic form.

20. **Transaction Standards**. The University will identify all covered transactions conducted by the components covered by this HIPAA Compliance Policy. All covered transactions conducted electronically must meet published and effective transaction standards.

21. **Information Security**. The University is committed to protecting the security of all protected health information entrusted to it. The University has adopted information security policies that are necessary to ensure continuity of operations; protect and ensure the confidentiality, integrity and availability of protected health information in its control; prevent unauthorized access to protected health information; protect against potential threats to the privacy and security of protected health information; and ensure Workforce members are committed to following the University's information security requirements. The University will review and revise its information security policies and procedures as necessary and appropriate from time to time to maintain their effectiveness.

Reference: August 21, 2003
Amended April 2, 2021