University of Nebraska Foundation

Privacy and Security of Confidential Health Information

Policies and Procedures Manual

Table of Contents

PURPOSE FOR THE POLICIES AND PROCEDURES MANUAL **3**

SCOPE OF THE POLICIES AND PROCEDURES MANUAL **5**

PROTECTED HEALTH INFORMATION—DEFINED **6**

PHYSICAL SAFEGUARDS FOR PHI **8**

ADMINISTRATIVE SAFEGUARDS FOR PHI **18**

TECHNICAL SAFEGUARDS FOR PHI **36**

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION **47**

USE AND DISCLOSURE OF PHI FOR FUNDRAISING **52**

WORKFORCE PRIVACY TRAINING **60**

BREACH OF UNSECURED PHI **62**

SANCTIONING WORKFORCE MEMBERS WHO VIOLATE UNF POLICIES **68**

MINIMUM NECESSARY FOR REQUESTS FOR, OR USES OR DISCLOSURES OF, PHI **71**

DISCLOSING INFORMATION TO SUBCONTRACTOR BUSINESS ASSOCIATES ... **76**

RESPONDING TO INDIVIDUALS' REQUESTS FOR ACCESS TO THEIR DATA **81**

ACCOUNTING FOR DISCLOSURES OF PHI—TRACKING DISCLOSURES AND RESPONDING TO REQUESTS BY INDIVIDUALS **83**

RESPONDING TO INDIVIDUALS' REQUEST TO AMEND PHI OR RECORDS **86**

PURPOSE FOR THE POLICIES AND PROCEDURES MANUAL

Effective Date: May 14, 2018

I. Purpose:

To clarify the purpose, intent, and use of this Policies and Procedures Manual ("Manual") and to document the policies and procedures of University of Nebraska Foundation ("UNF") for protecting the privacy and security of protected health information.

This Manual serves as a guide for achieving compliance with the standards, implementation specifications and other requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") including the regulations on the Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164 (Subparts A and E) ("Privacy Rule"), Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Parts 160 and 164 (Subpart C) ("Security Rule"), and Notification in the Case of Breach of Unsecured Protected Health Information at 45 C.F.R. Parts 160 and 164 (Subpart D) ("Breach Rule") (referred to collectively as the "HIPAA Regulations" throughout this Manual).

II. Policy:

HIPAA controls what hospitals, clinics and other health care providers (all of which are classified as "Covered Entities") and the organizations that provide services to them may and must do with "Protected Health Information" ("PHI"). By providing services regulated under HIPAA as "fundraising" on behalf of one or more Covered Entities that involve the use and/or disclosure of PHI from or on behalf of those Covered Entities, UNF is subject to certain of the HIPAA Regulations that apply to "Business Associates". It shall be the policy of UNF to protect and safeguard the privacy and security of PHI, including any electronic PHI ("ePHI") it creates, acquires or maintains in accordance with the HIPAA Regulations.

The policies and procedures contained in this Manual, along with the policies and procedures set forth in **Information Technology Security Practices and Procedures Manual** (the "IT Manual"), document the policies and procedures of UNF for protecting the privacy and security of PHI and are intended to provide guidance to UNF personnel for complying with the HIPAA Regulations by:

A. Establishing policies and procedures regarding the use and disclosure of PHI;

B. Clarifying the rights of individuals who are the subject of PHI;

C. Specifying procedures used by UNF to ensure individuals are fully able to exercise the rights afforded them under the applicable federal and state laws and regulations; and

D. Establishing administrative procedures to assist individuals and UNF personnel to effectuate these policies and procedures.

These policies and procedures apply to all PHI and ePHI created, acquired or maintained by UNF beginning **May 14, 2018.** Policies and procedures intended to address compliance with the Security Rule are referred to collectively herein as the "Security Policies and Procedures." Policies and procedures intended to address compliance with the Privacy Rule are referred to collectively herein as the "Privacy Policies and Procedures." Policies and procedures intended to address compliance with the Breach Rule are referred to collectively herein as the "Breach Policies and Procedures."

SCOPE OF THE POLICIES AND PROCEDURES MANUAL

Effective Date: May 14, 2018

I. Policy

This Manual applies to all PHI and ePHI regardless of the form in which it is created or maintained, including but not limited to oral, written, and electronic information. UNF has two databases that contain ePHI: (1) the Grateful Patient Database; and (2) the Foundation Advancement CRM (referred to herein as the "Ali CRM Database") (collectively, the "Databases"). This Manual applies to both Databases, along with any other PHI and ePHI created, stored, maintained, or received by UNF. It applies to PHI/ePHI of living individuals and deceased individuals for a period of 50 years following the death of the individual, generally.

All UNF employees (including interns), volunteers, and vendors are required to comply with this Manual (collectively referred to as "Workforce"). Any University of Nebraska employee (or volunteer, intern or vendor) that is granted access to the Databases must also comply with this Manual and is considered part of the UNF Workforce for purposes of compliance with the HIPAA Regulations.

Terms used, but not otherwise defined, in these policies and procedures shall have the same meaning as those terms in the HIPAA Regulations.

II. Procedure

All UNF Workforce will comply with this Manual.

PROTECTED HEALTH INFORMATION—DEFINED

Effective Date: May 14, 2018

I. Policy

A. Purpose

To help UNF workforce members identify and better understand what information constitutes protected health information, including electronic protected health information (collectively, "PHI") under HIPAA, as well as what subset of PHI has been deemed "Permitted Fundraising Information" for purposes of UNF's fundraising on behalf of Nebraska Medicine.

B. PHI Defined

PHI is defined by HIPAA to include any information that:

1. Relates to:
    a. A past, present, or future physical or mental health/condition;
    b. The provision of health care to an individual; or
    c. The past, present, or future payment for health care services.
2. Is created or received by a health care provider (e.g., Nebraska Medicine) that identifies the individual (or provides a reasonable basis to believe that the information can be used to identify the individual); and
3. Is transmitted or maintained in any form or medium (i.e., verbal, written, or electronic).

This is a very broad definition. For example, the name of a patient and the fact that he or she was a Nebraska Medicine patient is PHI. Specific examples of PHI include:

- *Demographic information, including name, address, other contact information, age, gender, and date of birth*;
- *Dates of health care provided to an Individual*;
- *Clinical department where services were provided (i.e., at Oncology Center, Department of Pediatrics, Center for Social Work, etc.);*
- *Treating physician*;
- *Outcome information (e.g., information about the death of a patient or other result of treatment);*
- Nature of the health care the Individual received;
- *Health insurance status*;

- Prescriptions;
- Photographs;
- Research records;
- Date of death; and
- Any other information that may reveal the identity of the Individual or any facts about his or her health care, health condition, or health insurance.

The italicized PHI is considered "Permitted Fundraising Information" under the UNF Privacy and Security Policies and Procedures. Permitted Fundraising Information may be used or disclosed by UNF solely for the purpose of fundraising on behalf of Nebraska Medicine, as set forth in the **UNF Use and Disclosure of PHI for Fundraising Policy**. The PHI that is not italicized may not be used or disclosed for fundraising unless the individual who is the subject of the PHI has first executed an "Authorization" permitting that activity. An Authorization is a specific type of document that must comply with certain elements outlined in the HIPAA Privacy Rule at 45 C.F.R. § 164.508. Nebraska Medicine would be responsible for obtaining this Authorization to permit UNF to fundraise using the non-italicized PHI listed above.

The designation of information as "PHI" attaches at the covered entity (e.g., Nebraska Medicine) level. UNF receives data directly from Nebraska Medicine, which means that most information in the Grateful Patient Database and some information in the Ali CRM Database constitutes PHI. UNF workforce members should note that once information qualifies as PHI it holds this status indefinitely (unless Nebraska Medicine has given UNF permission to de-identify the PHI as part of the fundraising services UNF provides). Thus, UNF and its staff cannot alter the PHI designation by, for example, simply identifying an individual as a donor (as opposed to a Nebraska Medicine patient) in communications or in UNF Databases.

II. Procedure

A. UNF staff will follow this policy to identify PHI and determine whether PHI meets the definition of Permitted Fundraising Information. UNF staff that have questions as to whether information qualifies as PHI or Permitted Fundraising Information will consult with the Privacy Officer.

B. UNF, through the Privacy Officer, will only de-identify PHI as necessary to provide fundraising services to Nebraska Medicine in compliance with the **Fundraising Affiliation & Services Agreement**. UNF will not use de-identified information for its own purposes unless it obtains prior written consent from Nebraska Medicine.

C. UNF will not attempt to obtain any Authorizations for fundraising that involve the uses or disclosures of PHI.

PHYSICAL SAFEGUARDS FOR PHI

Effective Date: May 14, 2018

I. Policy:

A. Purpose

This policy establishes guidelines for having appropriate physical safeguards in place to protect the privacy and security of ePHI.

B. Policy Implementation – General Rule

UNF must reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of its policies and procedures, the HIPAA Regulations, and State law. UNF must also reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

II. Facility Access Controls—General

A. Policy

Access to ePHI will be limited to only authorized workforce members through controlling, monitoring, and denying access to physical locations where ePHI is transmitted, processed and stored.

B. Procedure

UNF compliance will be met by acting in accordance with the following policies and procedures:

i. Section III Facility Access Controls—Contingency Operations

ii. Section IV Facility Security Plan

iii. Section V Access Control and Validation

iv. Section VI Maintenance Records

v. Section VII Workstation Use and Security

III. Facility Access Controls—Contingency Operations

A. Policy

To carry out the Disaster Recovery and Emergency Mode Operations Plan in the event of an emergency, UNF has established procedures to allow controlled access by authorized workforce members to systems housing ePHI. UNF has also established a Business Continuity Plan, which sets forth emergency recovery procedures necessary to ensure efficient and effective resumption of business in the event of interruption to UNF business functions. The Business Continuity Plan applies to the ePHI referenced in the Security Policies and Procedures. Because UNF is not involved in the health care provider-patient relationship and because Covered Entities from which UNF receives ePHI have the provider-patient relationship (and have the obligation to maintain ePHI necessary for treatment and related purposes), the need for emergency access to ePHI by UNF is not as pronounced.

B. Procedure

i. In the event the Disaster Recovery and Emergency Mode Operations Plan is triggered the Security Officer will grant emergency physical access to ePHI to designated workforce members and will otherwise follow the procedure set forth in the UNF Business Continuity Plan. Such access will be limited to the amount necessary to respond to the emergency.

ii. In the interim, or when UNF's copy of the ePHI cannot be accessed, the Security Officer will obtain ePHI needed to perform necessary services from Nebraska Medicine or UNF's subcontractors.

IV. Facility Security Plan

A. Policy

Physical access to areas within UNF facilities that contain equipment hosting ePHI, and areas from which ePHI may be accessed, will be restricted to authorized workforce members and visitors. Restricting physical access will protect ePHI from tampering, destruction, or theft.

B. Procedure

i. UNF workforce members are issued photo identification badges in accordance with the UNF **Employee Identification (ID) Badge Policy**. All UNF workforce members must wear and visibly display a photo identification badge at all times when in UNF offices and at staff functions (e.g., all staff meetings). Facility access will be controlled during

business hours through check-in or confirmation with front-desk personnel and after hours using keycard readers or physical keys, as required by each facility.

ii. Replacement ID badges are issued in accordance with the **Employee Identification (ID) Badge Policy**.

iii. Access to work areas where ePHI is received, processed, stored or transmitted will be limited to authorized workforce members. Access will be controlled through the ID badge system and keycard readers.

iv. All Nebraska Medicine data is housed off-site in the UNF Lincoln Datacenter. Equipment that stores Nebraska Medicine ePHI is stored in an isolated environment. Access to such equipment is restricted to only those workforce members who need access to accomplish his or her job duties. Other UNF workforce members do not have access to this equipment.

v. All workforce members are given security keycards (and in some instances physical keys) for their primary office. In some cases authorized employees may be issued security keycards for additional offices (e.g., Lincoln or Omaha offices). All security keycards and keys will be approved by the Privacy Officer and issued by Building Services.

vi. Visitors will be required to register when entering UNF facilities and will be escorted while in the facility. Visitors are required to wear a "VISITOR" badge during large meetings, events, or trainings.

vii. During non-working hours, facilities are locked and can only be accessed using an authorized keycard or physical key. Guidelines in the **IT Security Practices and Procedures Manual** (Application Service Providers (ASP) Security Standards, 3.2 Physical Security) apply to the physical locations where ePHI is stored and maintained by application service providers to UNF and includes locked environments for servers and other equipment on which ePHI is maintained. UNF-controlled facilities in which ePHI is maintained similarly have locked environments for servers and other information technology resources. The majority of UNF facilities have industry standard alarm systems by which law enforcement is alerted in the event of attempts to improperly access the facilities. UNF datacenter locations also have cameras and/or utilized security personnel for additional security.

viii. Use of paper documents that contain PHI (e.g., reports, event lists, prospect summaries, etc.) will be minimized and discouraged. Workforce members that have paper documents that contain PHI will store the documents in a locked desk drawer when not in use and will dispose of the documents using the confidential shred bins when no

longer needed. Paper documents containing PHI should generally not leave the premises, and if so the provisions of subparagraph (ix) below must be followed.

ix. Unsecured PHI or ePHI that is being physically transported within UNF (such as from one department to another) will be attended and supervised at all times.

x. Unsecured PHI or ePHI that is transported in a motor vehicle will be attended and supervised at all times. Should there be a need to leave the unsecured PHI/ePHI unattended, the equipment/unsecured PHI/ePHI will be locked in the trunk of the car. Workforce members are not permitted to transport PHI/ePHI via motor vehicles other than through these methods.

xi. The Security Officer, in conjunction with UNF management, will conduct an annual review of the current Facility Security Plan. A review will also take place any time there are major structural changes in the facility.

V. Access Control and Validation Procedures

A. Policy

Control and validation of access to UNF facilities and the specific areas within the facilities where ePHI can be accessed, including control of access to software programs for testing, will be in place, active, and restrict access appropriately.

B. Procedure

i. UNF workforce members will wear ID badges at all times in accordance with Section IV and the UNF **Employee Identification (ID) Badge Policy**. Visitors will be accompanied at all times by a UNF staff member and will be required to wear a "VISITOR" badge during large functions.

ii. Omaha and Lincoln facility records (such as keycard logs, which indicate who entered and exited the facility and date/time of access) will be reviewed periodically to validate that only authorized individuals have accessed the facilities. The Kearney Office does not currently have automatic access recording (via keycard logs) but will employ paper-based visitor logs until such time as keycard logs are implemented if UNF determines implementation of the same to be reasonable and appropriate for the Kearney Office.

iii. Visitor logs will be reviewed quarterly to validate that only appropriate visitors are being allowed into UNF's facilities. Such logs will be maintained for two (2) years or such other period of time as the Privacy Officer determines to be appropriate (and documents in writing if such period varies from the aforementioned two (2) year period).

iv. Physical access to systems hosting ePHI will be restricted to authorized workforce members in accordance with the **Workstation Use and Security Policy**. Such systems will be reviewed quarterly to validate that only authorized workforce members have obtained access.

VI. Maintenance Records

A. Policy

Security-related modifications to the physical components to UNF facilities will be documented and reviewed to safeguard the facility from unauthorized access. In addition, security ID badge management procedures will be in place to secure UNF facilities and the ePHI accessible from within UNF facilities.

B. Procedure

i. UNF Building Services has authority to authorize repairs or modifications of UNF's facilities and other components of physical security. In the event Building Services determines that facility repairs or updates are warranted, and such repairs and modifications are not routine in nature, Building Services shall notify UNF leadership. Should any repair or modification alter or in any way impact the security of ePHI or PHI, Building Services shall also notify the Privacy Officer in advance so that the Privacy Officer can plan accordingly. UNF leadership is responsible for making facility update requests to Building Services.

ii. Security-related repairs and modifications to the physical components of a facility will be recorded. These records will be reviewed by the Privacy Officer at least annually and will also be reviewed any time there are major structural changes in the facility. Maintenance records indicating modifications to a facility may necessitate updates to UNF policies and procedures, which will be led by the Privacy Officer.

iii. In accordance with the **Employee Identification (ID) Badge Policy**, workforce members must notify Building Services of any lost or stolen ID badges. Building Services, with assistance from the Privacy Officer, will investigate the situation and identify next steps to protect facility security.

VII. Workstation Use and Security

A. Policy

Access to ePHI workstations will be limited to authorized workforce members. While performing their job duties, authorized workforce members will access and process ePHI using designated procedures at their approved and designated workstations. Workforce

members will take reasonable steps so that all ePHI in their work area is accessible only by authorized workforce members. This applies to ePHI maintained at UNF facilities and at remote locations.

B. Procedure

i. Access to workstations where ePHI is received, processed, and transmitted will be limited to authorized workforce members and controlled through the UNF security ID badge system and keycard readers, along with system username and password requirements.

ii. UNF workforce members will comply with the Acceptable Use security protocol set forth on pp. 3-4 of the **IT Security Practices and Procedures Manual** for all workstations and electronic media. All workstations and electronic media will be secured with a password protected screensaver with an automatic activation feature set at ten (10) minutes or less.

iii. The Security Officer will approve the security specifications for workstation(s) used by authorized workforce members to access ePHI.

iv. Each workforce member will follow the rules below to safeguard ePHI:

- An authorized workforce member will access ePHI only as needed to perform his or her job duties.
- Mobile phones will be safeguarded in accordance with the **Mobile Device Management Policy** adopted by UNF. All other electronic media and devices (including computers, tablets, and other technology) will be password-protected in accordance with UNF's Password Management policy, set forth in Section XVII of the **Administrative Safeguards Policies**.
- ePHI will be stored only on secure network drives. ePHI will never be copied to or stored on a workforce member's desktop or local hard drive;
- ePHI is not permitted to be stored or maintained on any personally-owned devices (e.g., computers, tablets, phones, drives, etc.).
- ePHI will not be copied to or stored on UNF-sponsored portable devices (including USB/thumb drives, phones and tablets) unless the workforce member receives prior written approval from the IT Department and Security Officer. Workforce members will avoid storing PHI on portable devices unless the Security Officer has determined that storage is warranted and necessary to accomplish certain job functions. If temporary storage of ePHI on a portable device is determined to be

necessary for fundraising events, the IT Department will make available a designated UNF-sponsored Surface tablet (or other comparable device) for use by the workforce member at the event. Storage of ePHI will be limited to that device. The workforce member is required to return the device to the IT Department upon the conclusion of the job function that warranted storage. The IT Department will remove any stored ePHI and will verify that ePHI is no longer maintained on such device. Option (a) or (b) from section B.(v) of the Unique User Identification provision of the **Technical Safeguards for PHI Policies and Procedures** will be adhered to in the event that ePHI is stored on the Surface tablet during an event.

- Electronic media containing ePHI will be stored in locked filing cabinets, desk drawers or rooms to which only authorized workforce members have access;

- Any computer monitor used to access ePHI will be protected from the view of persons who are not authorized workforce members (e.g., though monitor shades, monitor positioning away from public paths of travel, etc.);

- All workforce members will log off or lock his or her computer before leaving his or her office or worksite (e.g., it is not sufficient to wait for the auto-lock to trigger; rather workforce members must affirmatively log-off or lock computers when leaving workstations);

- UNF email must not be automatically forwarded to an external destination without prior approval by the workforce member's supervisor or the IT Department, in accordance with the **IT Security and Procedures Manual**;

- PHI/ePHI will not be included in electronic calendar appointments unless the entity providing electronic calendaring services enters into a Subcontractor Business Associate Agreement in the form of its **UNF Template Subcontractor BAA** or a substantially similar agreement that meets HIPAA's business associate agreement requirements.

- PHI/ePHI will not be transmitted by text message;

- PHI/ePHI will not be transmitted by email, even when such email is sent confidentially, unless this transmission occurs via an "Approved Channel" (as defined in the **UNF Security Rule Technical Safeguards**); and

- In the event UNF elects to acquire a secure methodology for the electronic transmission of ePHI via email (i.e., one of the Approved Channels), workforce members will adhere to such guidelines as UNF may adopt related to use of that methodology.

v. Shared resources (e.g., servers) where ePHI data is stored will be protected with access restricted to authorized workforce members that need access.

vi. Workforce members must lock or log-off devices when unattended**.** All workstations and electronic devices must be secured with a password protected screensaver with an automatic activation feature set at ten (10) minutes or less.

vii. The IT Department will keep an inventory of UNF issued property and equipment, including workstations and electronic media, in accordance with Section X below. UNF utilizes Microsoft Intune to manage both UNF issued and personal property and equipment. Microsoft Intune enables UNF to set parameters to restrict access and protect data at an application level and enables UNF to remotely wipe data if necessary.

viii. Workforce members must comply with the remote access policy set forth on pp. 9-11 and the Virtual Private Network ("VPN") policy set forth on pp. 25-26 of the **IT Security and Procedures Manual**. Workforce members are only permitted to utilize remote access after first obtaining permission from his or her supervisor. All requests are reviewed by the UNF AVP of Advancement Services, or his or her designee. Workforce members are required to ensure that their remote access connection is as secure as UNF's security protocols, and that any equipment used complies with UNF's security standards, policies and procedures. Workforce members are prohibited from letting family members, friends, or any other unauthorized users access UNF systems, networks, or the Databases. Workforce members must immediately log out of any remote access system after use and secure login and password information so that others cannot access UNF systems.

VIII. Device and Media Controls—Disposal

A. Policy

The final disposition of ePHI and the electronic media hosting ePHI (including hardware, such as server hard-drives and copiers, and storage media) will be tracked and documented. The ePHI and the electronic media hosting ePHI will be disposed of as permitted by these policies and procedures.

B. Procedure

i. When ePHI is deemed to be no longer required, the original ePHI and all copies will be removed from all electronic media.

ii. When UNF electronic media hosting ePHI is no longer required or deemed to be usable, the IT Department will remove the ePHI from the device using a zero out hard drive procedure DOE-compliant three pass erase (2 passes of random data followed by a

single pass of known data over the entire disk). If removal is not possible, the ePHI will be destroyed with the physical destruction of the device. In both cases the electronic media will be disposed of in a manner that makes the media un-usable and unreadable.

iii. Prior to donating UNF-owned devices, the IT Department will remove all data from the device.

iv. Destruction and disposal of electronic media will be logged in the corresponding inventory log book.

IX. Media Re-Use

A. Policy

ePHI will be removed from all UNF electronic media before the media is made available for re-use.

B. Procedure

i. Electronic media will be sanitized in accordance with a DOE-compliant hard drive sanitation process.

ii. Sanitization of electronic will be logged by the IT Department.

iii. The Security Officer will ensure the sanitizing procedures used by UNF are adequate prior to re-using any electronic media that previously hosted ePHI.

X. Accountability for Hardware and Media Containing ePHI

A. Policy

An inventory record log will be maintained for the acquisition, movement and disposal of electronic media hosting ePHI to ensure that ePHI is not accidentally lost, exposed, or destroyed. An inventory will be maintained of all electronic media used to store ePHI and all devices used to gain access to ePHI. Each electronic media/device in this inventory will include the location of the electronic media/device (both inside and outside of UNF facilities) and a record of what ePHI is store on electronic media, or accessible via the device, in sufficient detail to comply with the breach notification requirements set forth in the **UNF Breach Policy**.

B. Procedure

i. UNF-owned electronic media that contain ePHI will be inventoried and tracked by the IT Department during its useful life. This includes hardware under repair, under warranty, or handled by third parties.

ii. Because the Ali CRM Database is a web-based application, workforce members are able to access limited ePHI using their personal devices. Workforce may also access ePHI that may be available in email through personal devices. UNF employs Microsoft Intune to manage and protect data that is accessible on personal devices. For example, Microsoft Intune allows UNF to set parameters to restrict access and protect data at an application level, enables UNF to remotely wipe data if necessary, and enables UNF to force encryption of personal devices. Further, regardless of the technical access capabilities described above, workforce members' supervisors are responsible for determining whether access by workforce to the Ali CRM Database or ePHI available through email is appropriate and workforce members shall not engage in any such access until such approval has been granted by their supervisor. In no event is ePHI is permitted to be stored or maintained on personal owned devices/media (e.g., computers, tablets, phones drives, etc.).

iii. Electronic media used for ePHI will always be under the control of an authorized workforce member or vendor designated by UNF.

iv. The IT Department will review this inventory log on a bi-weekly basis.

v. Any electronic media that cannot be accounted for will be reported to, and investigated by, the Security Officer.

XI. Data Backup and Storage

A. Policy

A retrievable exact copy of ePHI will be created before movement of any critical systems containing ePHI.

B. Procedure

UNF has identified critical applications and systems that contain ePHI. These critical applications and systems are operated and stored in a secured environment that is segmented away from other UNF systems, and access to the data on such systems is limited. UNF will make a backup copy of these systems and data, which will facilitate restoring ePHI if necessary.

ADMINISTRATIVE SAFEGUARDS FOR PHI

Effective Date: May 14, 2018

I. General Policy:

A. Purpose

This policy establishes guidelines for having appropriate administrative safeguards in place to protect the privacy and security of ePHI.

B. Policy Implementation – General Rule

UNF must reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of its Security and/or Privacy Policies and Procedures, the HIPAA Regulations, and State law.

UNF must also reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

II. Security Management Process Standard

A. Policy

UNF will implement policies and procedures to prevent, detect, contain and correct security violations.

B. Procedure

i. UNF will implement the policies and procedures as set forth in this Manual, along with the policies and procedures in the **IT Security Practices and Procedures Manual**. All ePHI is considered "confidential information" within the parameters of the **IT Security Practices and Procedures Manual**.

ii. The Security and Privacy Policies and Procedures will be updated to account for any legal, operational, or environmental changes.

III. Risk Analysis and Risk Management

A. Policy

UNF conducted a thorough and accurate assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI ("ePHI") held by UNF. The risk analysis addressed the current level of risk, helped determine an acceptable level of risk, and identified solutions. The current risk analysis is maintained

in UNF's records and is saved as **UNF Risk Analysis Feb. 1, 2018** and is subject to the Security Officer's oversight and control. Based on the analysis documented in the **UNF Risk Analysis Feb. 1, 2018**, UNF has implemented security measures to reduce risks and vulnerabilities to a reasonable and appropriate level. The process of risk analysis and risk management will be conducted on an on-going basis to maintain the confidentiality, integrity and availability of ePHI.

B. Procedure

i. Each year UNF's Security Officer, with the assistance of the IT Department, shall conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI maintained by UNF. In addition, the Security Officer will monitor any developments related to new categories or volumes of ePHI created, received, maintained or transmitted by UNF; new technology; Security Incidents and changes in the law and use such information to make recommendations to UNF related to any potential corrections of identified security gaps or changes in reasonable and appropriate security measures at UNF.

ii. UNF's Security Officer shall implement policies and procedures that record, examine, and reduce risks and vulnerabilities relating to ePHI maintained by UNF.

iii. UNF's Security Officer shall consult with in-house counsel or external resources as necessary to meet the Officer's obligations as outlined in the Manual.

IV. Workforce Sanctions

A. Policy

UNF workforce members are prohibited from violating Security Policies and Procedures as well as the HIPAA Regulations. The Privacy Officer will apply appropriate sanctions against workforce who violates the Security Policies and Procedures or the HIPAA Regulations.

B. Procedure

UNF will implement this policy through the UNF **Security and Privacy Rule Sanction Policy**.

V. Information System Activity Review

A. Policy

UNF will conduct periodic reviews of system and program activity that contain ePHI to verify that only authorized workforce members have access to ePHI and that such authorized workforce members are properly accessing the data.

B. Procedure

i. UNF will perform regular internal audits using industry standard methods. UNF has systems in place to record events that occur on its networks and systems, and such logs are utilized during UNF audits. UNF employs the National Institute of Standards and Technology (NIST) publication pertaining to computer security log management (available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf). In addition, UNF will periodically engage the assistance of UNL-IT Enterprise and use an audit tool to monitor network activity.

ii. If UNF discovers that there has been inappropriate use by workforce members, such access will be immediately terminated and the incident(s) will be further investigated by the UNF Security Officer. Accounts will be locked for thirty (30) minutes upon five (5) unsuccessful attempts to log-in. Reasonable steps will be taken thereafter to address any issues or vulnerabilities identified, including subjecting UNF workforce members to disciplinary action in accordance with the **Security and Privacy Rule Sanction Policy**.

iii. UNF will document and track all audit results.

VI. Security Officer Designation

A. Policy

UNF will designate a Security Officer so that workforce know who is responsible for overseeing UNF's compliance with the HIPAA Security Rule and for the development and implementation of UNF's Security Policies and Procedures, the HIPAA Regulations, and other applicable laws.

UNF must document the Security Officer designation in its Security Policies and Procedures. The Security Officer may delegate responsibilities to an office or a designee provided that the Security Officer maintains responsibility for directing the office or designee's activities. UNF must maintain documentation regarding the designation of the Security Officer and his/her contact information for at least six (6) years from the date when it was last in effect.

B. Procedure

i. UNF has designated Ben Storck as its Security Officer. Ben Storck can be contacted by either phone, email, mail, or in-person:

Ben Storck
Assistant Vice President, Advancement Services
1010 Lincoln Mall, Suite 300
Lincoln, NE 68508
(402)-458-1197
ben.storck@nufoundation.org

ii. In the event the individual serving as Security Officer changes, UNF will document such change either via an amendment to the Security Officer Designation of this Policy and Procedure or through such other documentation that it determines to be appropriate.

iii. The Security Officer is responsible for the following tasks:

- Initiating, facilitating, and promoting activities to foster information security awareness within UNF;
- Leading a culture of cyber security within UNF;
- Developing, monitoring, amending, and overseeing the implementation of UNF's Security Policies and Procedures;
- Performing those tasks specifically assigned to the Security Officer in UNF policies (e.g., performing periodic risk assessments);
- Overseeing UNF compliance with HIPAA's administrative, technical and physical safeguards and monitoring changes in the Security Rule that may affect UNF policies and procedures;
- Overseeing, developing and/or delivering initial and ongoing security training to the workforce;
- Serving as point of contact for questions from workforce;
- Periodically evaluating security trends, evolving threats, risks and vulnerabilities and apply tools to mitigate risk as necessary;

- Assisting the Privacy Officer as needed with HIPAA breach determinations and notification processes under HIPAA and applicable State breach rules and requirements; and

- Serving as an information security consultant to all departments for all data security related issues.

iv. UNF will maintain documentation regarding its Security Officer designation and the necessary contact information for at least six (6) years.

VII. Workforce Security

A. Policy

UNF only permits authorized workforce members to access ePHI, and such access will be supervised and reviewed to ensure that access is appropriate. Unauthorized workforce will be prevented from obtaining access to ePHI.

B. Procedure

The UNF Security Officer will implement, and UNF workforce will comply with, the following policies and procedures:

- Section VIII. Authorization and Supervision of Workforce

- Section IX. Workforce Clearance Procedures

- Section X. Termination of Access

- Section XI. Information Access Management—Access Authorization

- Section XII. Information Access Management—Access Establishment and Modification

VIII. Authorization and Supervision of Workforce

A. Policy

UNF will review and specifically authorize access to ePHI for each member of its workforce. UNF will supervise such workforce member's access to ensure it is appropriate.

B. Procedure

i. UNF has two databases that contain ePHI: (1) the Grateful Patient Database; and (2) the Foundation Advancement CRM (referred to herein as the "Ali CRM Database") (collectively, the "Databases"). Both Databases are hosted and maintained by UNF. These are the only databases where ePHI resides at UNF.

ii. As described more fully in UNF's **Privacy Policies and Procedures**, most ePHI will generally be contained within the Grateful Patient Database. Limited amounts of ePHI may be contained within the Ali CRM Database.

iii. UNF will authorize workforce access to the Grateful Patient Database based on the workforce member's position and job duties, in accordance with the **Access to Grateful Patient Database** policy. All UNF workforce need access to the Ali CRM Database to perform their job responsibilities. Any University of Nebraska staff needing access to the Ali CRM Database will first be required to submit a request for access to UNF and documentation (including recommendation from their supervisor, if applicable) of why such access is necessary for their responsibilities. The Security Officer and/or Privacy Officer will review any such requests for access to the Ali CRM Database and make determinations of whether such access will be permitted. Any UNF workforce who are granted such access shall be required to complete the **HIPAA Education Program**, will be subject to all UNF Security and Privacy Policies and Procedures and will be considered part of the UNF workforce for purposes of compliance with the HIPAA Regulations; provided, however, that interim HIPAA training will occur (in accordance with paragraph (v), below) for workforce members who will initially only have access to the Ali CRM Database; access to the Grateful Patient Database will not be available until the full **HIPAA Education Program** is completed. Any UNF or University of Nebraska staff who improperly access ePHI in the Ali CRM Database will be subject to all applicable workforce or employment sanction policies and procedures.

iv. For each workforce member, the designated UNF supervisor will make a recommendation to the Security Officer regarding the workforce member's access to ePHI through workstations, networks, programs, or systems. Such recommendation will include the level of access that is appropriate. This requirement also applies to any University of Nebraska staff who are intended to have access to ePHI in both the Grateful Patient and Ali CRM Databases. UNF supervisors may make these determinations on the basis of categories of workforce at UNF who perform comparable services within those categories (as opposed with respect to each individual within the category); provided, however, that all workforce members with access to ePHI shall be subject to these policies and procedures.

v. The Security Officer will review the recommendation and, if he/she approves, will direct the IT department to grant such access. Prior to any access being granted to the Ali CRM Database, workforce members shall be required to undergo an initial training session on HIPAA. All workforce members are required to complete UNF's full **HIPAA Education Program** before access to the Grateful Patient Database is granted, which shall be led by the Privacy Officer or the Officer's designee.

vi. UNF supervisors will oversee workforce access to ensure that ePHI is being used and disclosed correctly and that access levels remain appropriate.

vii. If UNF supervisors or the Security Officer determine that access is no longer warranted, such access will be terminated or adjusted in accordance with the procedure set forth in this Manual.

IX. Workforce Clearance Procedures

A. Policy

UNF will implement procedures in the hiring and termination process to determine whether access to ePHI is appropriate. These procedures will also apply to all workforce members who have access to ePHI, regardless of whether they are employees, independent contractors, volunteers, trainees or individuals affiliated with the University of Nebraska who require access to ePHI for their job responsibilities.

B. Procedure

i. UNF will evaluate each workforce member's position upon hire (or other commencement of the workforce relationship) to determine whether access to ePHI and the Databases are necessary and warranted.

ii. UNF supervisors will make access determinations prior to such workforce member's start date and will reevaluate workforce access annually.

iii. Prior to clearing access, UNF will ensure that the workforce member has completed a background check in accordance with UNF's contractual obligations. Prior to any access being granted to the Ali CRM Database, workforce members shall be required to undergo an initial HIPAA training session. Workforce must complete both the initial HIPAA training session and UNF's full **HIPAA Education Program**, which shall be led by the Privacy Officer or the Officer's designee, prior to access being granted to the Grateful Patient Database.

iv. The Security Officer will assess all other requests for access, including those made by University of Nebraska staff.

v. The Security Officer will maintain and update a record of all individuals who have access to ePHI in the Databases.

X. Termination of Access

A. Policy

UNF will implement procedures for terminating access to ePHI when employment ends, the workforce relationship concludes or termination of access is otherwise warranted.

B. Procedure

i. Workforce member access to the ePHI will be terminated if the workforce member:

- Fails to follow UNF policies and procedures, including but not limited to the Security and/or Privacy Policies and Procedures, and UNF determines that the workforce member cannot be rehabilitated through additional trainings, sanctions, or other appropriate methods;
- No longer needs access to perform their job duties; or
- Is no longer employed by UNF.

ii. The workforce member's supervisor is responsible for facilitating termination of access rights.

iii. Upon access termination, UNF supervisors will immediately retrieve from such workforce member any keys or access cards to any area where ePHI is stored. The Security Officer will also facilitate the immediate deactivation of the workforce member's network and password access to ePHI.

iv. The Security Officer will secure from the workforce member any UNF-sponsored electronic media stored in home offices, on mobile devices, or in other remote locations. The Security Officer will also verify that all appropriate on-site electronic media is secured. No UNF-sponsored computer or other electronic media containing ePHI will remain in the possession of, or accessible by, any workforce with unauthorized access. Workforce members are not permitted to store or maintain ePHI on personal devices (e.g., computers, tablets, phones, thumb drives, etc.). Termination procedures will ensure that no access to UNF ePHI or Databases is permitted via portable devices at termination. The Security Officer (or Privacy Officer as UNF determines to be appropriate) will lead periodic trainings as a way of reminding staff not to store ePHI on personal devices and/or will send out periodic email reminders to work force with privacy and security tips.

v. Any ePHI/PHI in the possession of any workforce members must be returned immediately upon access termination. The IT Department will properly dispose of ePHI/PHI, as necessary and appropriate.

vi. Any human resources exit checklists, exit interview guidelines or letters of termination will be updated as appropriate by UNF to ensure that termination of access to ePHI is appropriately included as an element on such materials to be confirmed as completed.

XI. Information Access Management—Access Authorization

A. Policy

Access to ePHI through workstations, networks, programs and systems will be restricted and will be granted only to authorized workforce members that require access to accomplish their job duties. Remote access to ePHI will be granted when necessary and appropriate.

B. Procedure

i. Internal access to ePHI through workstations, networks, programs or systems will be identity based, using a unique user ID and password for each authorized workforce member.

ii. Remote access to ePHI through a virtual private network ("VPN"), remote access service ("RAS") or other forms of connection will be identity based, using a unique user ID and password for each authorized workforce member. UNF will adhere to the guidelines on Remote Access set forth on pp. 9-10, Virtual Private Network (pp. 25-26) and other applicable provisions of the **IT Security Practices and Procedures Manual** in authorizing access.

iii. UNF will implement, and workforce must follow, the access procedures set forth in Sections VIII-X above.

XII. Information Access Management—Access Establishment and Modification

A. Policy

UNF will implement procedures that establish, review, or modify workforce members' right of access to ePHI through workstations, networks, programs or systems, through internal or remote access, to ensure proper access has been granted.

B. Procedure

i. UNF supervisors will make recommendations to the Security Officer regarding workforce access to ePHI through workstations, networks, programs, or systems. Such recommendation will include the level of access that is appropriate.

ii. The Security Officer will review the recommendation and, if he/she approves, will direct the IT Department to grant such access.

iii. The IT Department will facilitate the establishment of unique user IDs and passwords for each workforce member.

iv. UNF supervisors and/or the Security Officer can and will modify access at any time in accordance with the Security Policies and Procedures.

v. An annual review will be conducted to re-validate workforce member access and make any necessary modifications.

vi. UNF guidelines from the **IT Security Practices and Procedures Manual** on Remote Access (pp. 9-10), Audit (pp. 16-17), Extranet (pp. 18-19), Internet DMZ Equipment (pp. 19-21), Virtual Private Network (pp. 25-26) and Wireless Communication (pp. 26) apply.

XIII. Security Awareness and Training

A. Policy

The Privacy Officer, in conjunction with the Security Officer, will train UNF workforce with respect to the UNF Privacy and Security Policies and Procedures. The level of training will depend upon the workforce member's access to ePHI.

B. Procedure

i. All UNF workforce members must complete the **HIPAA Education Program**. All new workforce members must complete the **HIPAA Education Program** within thirty (30) days of commencing their workforce relationship at UNF or assuming such new roles or responsibilities. Additional HIPAA training will be provided to workforce depending on their level of access to PHI and their job duties. Workforce members must complete an initial HIPAA training program prior to receiving credentials that permit access to the Ali CRM Database, and must complete the full **HIPAA Education Program**, and any other required training, prior to receiving credentials that permit access to the Grateful Patient Database.

ii. The Security Officer and Privacy Officer will oversee the training of each workforce member on UNF's Privacy and Security Policies and Procedures.

iii. The Security Officer and Privacy Officer will conduct refresher training sessions annually. Additional trainings will be provided throughout the year with respect to any legal, operational, or environmental changes or updates.

iv. The Privacy Officer will ensure that each workforce member with access to ePHI receives sufficient training to carry out his or her job duties and responsibilities in compliance with the UNF Security Policies and Procedures.

v. The Security Officer and Privacy Officer will document all training provided and monitor attendance and successful completion by UNF workforce. The **HIPAA Overview & Privacy Training Sign In Sheet** (or a substantially similar document) will be tracked and maintained by the Privacy Officer.

XIV. Security Reminders

A. Policy

The Security Officer will provide periodic (as needed) security updates and reminders to UNF workforce. Periodic security updates will reinforce the formal training processes and keep workforce up-to-date on security issues.

B. Procedure

i. The Security Officer will take into account Security Incidents and other identified events that reflect potential risks and vulnerabilities to ePHI in determining whether security reminders to UNF workforce are necessary.

ii. The Security Officer will provide security reminders to workforce using a variety of communication forms, including e-mail, formal letters/memos, screen savers, training modules, organizational-wide listservs, eNUF Weekly (weekly e-publication that provides staff with organizational updates), classroom instruction and updated training materials.

XV. Protection from Malicious Software

A. Policy

The Security Officer will ensure that security measures are in place to guard against, detect and report malicious software thereby ensuring the confidentiality, integrity and availability of ePHI.

B. Procedure

i. The Security Officer will implement UNF's policies set forth in the **IT Security Practices and Procedures Manual**, which identifies and implements UNF network and program security measures, including but not limited to anti-virus software and physical, network, and web security standards. UNF guidelines on anti-virus protection are included on pp. 12-13 and pp. 21 of the UNF **IT Security Practices and Procedures Manual** and address the following: running UNF standard, supported software; managing files or macros that were sent by unknown or suspicious sources; downloading of suspicious files; the sharing/using of disks; and the anti-virus standards for UNF computers.

ii. UNF workforce will receive training on these security measures as part of the **HIPAA Education Program.**

iii. UNF workforce will be reminded annually to: (a) not download unauthorized software, and (b) not open email attachments from unknown senders. The annual reminder will ask workforce members to report suspicious activity or unknown software they find to the Service Desk. Service Desk staff members will notify the Security Officer, as appropriate, and work to resolve the potential issue.

iv. In the event of a phishing scam, the IT Department will send out an email to all UNF workforce to identify the scam, warn of its suspicious message, and provide education on the proper protocol.

v. The Security Officer will evaluate these security measures at least annually.

XVI. Log-in Monitoring

A. Policy

UNF will monitor all log-in attempts through its syslog tools and Solarwinds software and will report discrepancies.

B. Procedure

i. UNF will block unauthorized access to ePHI through workstations, programs, and systems.

ii. User accounts will be automatically disabled after five (5) successive unsuccessful log-in attempts. User accounts will remain locked for thirty (30) minutes and can only be re-enabled after user identification has been verified through a successful password change or upon approval by the Service Desk.

iii. To the extent practicable using UNF's information technology resources, an alert will be automatically generated if an excessive number of inappropriate log-in attempts are programmatically detected in a server log.

iv. Unsuccessful attempts will be logged and reviewed to identify potential security threats.

v. UNF workforce will be informed of this procedure during the **HIPAA Education Program** or through other methods, as appropriate.

XVII. Password Management

A. Policy

Passwords used by UNF workforce to gain access to ePHI will be created, changed, and safeguarded in a manner that protects ePHI from unauthorized access.

B. Procedure

i. UNF workforce will comply with the password protocol set forth in the **IT Security Practices and Procedures Manual**. It is the policy of UNF to require workforce to use passwords that conform to the guidelines on "Strong" passwords as outlined in the **IT Security Practices and Procedures Manual**. Passwords will be required to have characters from three of the following four categories: (1) English uppercase characters (A through Z); English lowercase characters (a through z); (3) Base ten digits (0 through 9) and (4) Non-alphabetic characters (e.g., !, $, #, %). Additional Password protocol requirements are set forth on pp. 7-9 of the **IT Security Practices and Procedures Manual**.

ii. As described in the **IT Security Practices and Procedures Manual**, all passwords must be changed every ninety (90) days and cannot be shared with other individuals. Group accounts and passwords are prohibited. UNF workforce are required to keep passwords confidential and adhere to the password protection standards on pp. 8-9 of the **IT Security Practices and Procedures Manual.**

iii. Following five (5) successive unsuccessful log-in attempts, user accounts will be disabled for thirty (30) minutes. Workforce are required to complete a successful identification verification process, or work with the Security Desk, to re-enable access to their account.

iv. UNF workforce will be trained on these password protocols during the **HIPAA Education Program**.

XVIII. Security Incident Procedures—Response and Reporting

A. Policy

The Security Officer will identify and respond to suspected or known Security Incidents. The Security Officer will mitigate known Security Incidents to the extent practicable, along with any known harmful effects of the Security Incidents. The Security Officer will document the Security Incidents and outcomes and will work with the Privacy Officer to provide notifications of any Breach of Unsecured PHI when required.

A "Security Incident" is defined as an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with a UNF system (including but not limited to hardware, software, and data applications). All incidents, threats, or violations that affect or may affect the confidentiality, integrity, or availability of ePHI are considered Security Incidents.

B. Procedure

i. UNF workforce must report any actual or suspected Security Incident to the Security Officer. UNF workforce are to be familiarized with the reporting obligations outlined in the **IT Security Practices and Procedures Manual** and are expected to make such reports as required thereunder.

ii. UNF's guidelines on reporting unsuccessful Security Incidents to Nebraska Medicine are set forth in Section 2.15 of the Business Associate Agreement between UNF and Nebraska Medicine.

iii. The Security Officer will investigate suspected material Security Incidents directed at ePHI or impacting ePHI. If his or her investigation confirms that a material Security Incident has occurred, the Security Officer will, in consultation with the Privacy Officer, determine what action to take, which may include remotely removing data from equipment that has been determined to be lost or stolen. All equipment on which ePHI is created, maintained, accessed or transmitted that leaves the physical confines of UNF will be encrypted as well as configured to permit remote wiping of data.

iv. The Security Officer will work with the Privacy Officer to provide notifications of Breaches of Unsecured PHI as may be required by the HIPAA Regulations, the UNF Breach Policy and Section 2.18 of the Business Associate Agreement between UNF and Nebraska Medicine.

v. If determined necessary by the Security Officer and Privacy Officer, action will be taken to minimize the harmful effects of the Security Incidents. Mitigation may include, but is not limited to:

- Revising UNF Security and/or Privacy Policies and Procedures to prevent future similar violations;
- Altering UNF security measures;
- Restoring ePHI that has been altered or modified to its original state; or
- Retention of qualified data forensics firm to evaluate the Security Incident, assist with resolution, providing guidance and recommendations for remedial steps, revising UNF Security and/or Privacy Policies and Procedures to address identified risks and vulnerabilities, assisting with updated training materials and related advice and consultation.

vi. The Security Officer will document the investigation of material Security Incidents directed at ePHI or impacting ePHI and the action taken to correct or mitigate the Security Incident.

vii. UNF workforce will receive training on Security Incidents during the **HIPAA Education Program**.

XIX. Contingency Plan

A. Policy

UNF will implement procedures for responding to an emergency that damages systems containing ePHI (e.g., fires, vandalism, system failure, natural disasters, etc.). Because UNF is not involved in the health care provider-patient relationship and because Covered Entities from which UNF receives ePHI have the provider-patient relationship (and have the obligation to maintain ePHI necessary for treatment and related purposes), the need for emergency access to ePHI by UNF is not as pronounced.

B. Procedure

i. *Data Backup Plan*: Server systems that contain ePHI are located in a protected datacenter that is monitored 24/7. The backup periods outlined on p. 24 of the **IT Security Practices and Procedures Manual** apply to ePHI. Electronic backups of this data are performed daily and on a set schedule and are maintained in off-site storage. UNF employs periodic backups on a set schedule for equipment that has been segmented off for Nebraska Medicine, in accordance with UNF IT best practices. In

addition, UNF identifies critical applications, data, and operations on an annual basis, and such data is stored on a highly secured environment and is segmented away from general UNF systems for greater protection.

ii. *Disaster Recovery Plan*: UNF is in the process of upgrading its existing disaster recovery plan. UNF will continue to implement its current disaster recovery plan until a cloud-based solution is finalized. UNF will require the provider of a cloud-based solution to enter into a Subcontractor Business Associate Agreement in the form of its **UNF Template Subcontractor BAA** (as defined below) or a substantially similar agreement that meets HIPAA's business associate agreement requirements. UNF will either update these Security Policies and Procedures to reflect the operation of the disaster recovery plan or will document the same in a separate document that is subject to the oversight of the Security Officer and is considered a component of these Security Policies and Procedures.

iii. *Emergency Mode Operation Plan*: UNF has identified those systems that are critical to its operations and has established the necessary resources to support those systems during a disaster. ePHI will be accessible pursuant to the Data Backup Plan provisions outlined in Section XII.B.1 (above). ePHI that cannot be accessed pursuant to the Data Backup Plan but that is necessary to perform business services will be obtained from Nebraska Medicine or UNF subcontractors.

iv. *Testing and Revision Procedure:* UNF will perform periodic testing to verify that its contingency plan is valid and operational and will revise the plan if necessary. In consultation with UNF management, the Security Officer and UNF IT department will identify critical IT systems and perform targeted testing to determine whether such systems function as expected during and after a disaster. UNF will work in collaboration with Nebraska Medicine to confirm that Nebraska Medicine retains retrievable copies of ePHI.

v. *Applications and Data Criticality Analysis*: UNF will periodically assess the criticality of specific applications and data in support of other contingency plan components. UNF will include a list of systems that are determined critical for maintaining the security of ePHI as outlined in these safeguards. UNF will address the ongoing availability of these applications through the protections implemented under the **IT Security Practices and Procedures Manual** (e.g., Application Service Providers (pp. 13-16), Internet DMZ Equipment (pp. 19-21), Risk Assessment (p. 23) and Server Security (pp. 24-25)).

XX. Evaluation

A. Policy

UNF will perform a periodic technical and non-technical evaluation of its compliance with the HIPAA Security Rule, considering environmental and/or operational changes affecting the security of ePHI. The analysis of "technical" compliance will address information systems containing ePHI (and compliance with the Security Rule's "technical safeguards" at 45 C.F.R. § 164.312) and the analysis of "non-technical" compliance will focus on administrative and physical safeguards beyond information systems (and compliance with the Security Rule's "administrative safeguards" at 45 C.F.R. § 164.308 and "physical safeguards" at 45 C.F.R. § 164.310).

B. Procedure

i. The initial evaluation performed by UNF is documented on the **UNF Risk Analysis Feb. 1, 2018.**

ii. The Security Officer will, on an annual basis, perform an evaluation of UNF's compliance with the HIPAA Security Rule and the Security Policies and Procedures.

iii. The Security Officer will document his/her review, including any findings and recommendations. Any identified deficiencies will be remediated to ensure compliance. This evaluation may be performed in conjunction with other annual compliance reviews.

iv. This review will be documented through updates to the **UNF Risk Analysis Feb. 1, 2018**.

XXI. Subcontractor Business Associate Agreements

A. Policy

UNF will enter into Subcontractor Business Associate Agreements ("Subcontractor BAAs") with each subcontractor that will use, disclose, or create, receive, maintain or transmit PHI or ePHI. The Subcontractor BAAs will include the provisions required by the HIPAA Regulations.

B. Procedure

i. The Privacy Officer is responsible for determining whether a Subcontractor BAA is required. The Privacy Officer will refer to UNF's policies on business associates and

subcontractor business associates, and the HIPAA Regulations, to make this determination and will consult with legal counsel when necessary.

ii. If a Subcontractor BAA is required, UNF will enter into a Subcontractor BAA in accordance with this policy and the HIPAA Regulations prior to disclosing any PHI or ePHI to a subcontractor or otherwise permitting the commencement of a subcontractor business associate relationship to occur between UNF and the subcontractor. UNF will use the **UNF Template Subcontractor BAA** with subcontractors to the extent possible. UNF will also use the **Business Associate Checklist** when reviewing and evaluating third party BAAs or subcontractor BAAs (i.e., form BAAs or subcontractor BAAs proposed for use between UNF and a third party).

iii. The Privacy Officer will oversee the execution of the Subcontractor BAA to ensure that it complies with the HIPAA Regulations and the Business Associate Agreement with Nebraska Medicine (or any other relevant Business Associate Agreements).

iv. The Privacy Officer will maintain a list of subcontractors that are subcontractor business associates as defined in the HIPAA Regulations. The Privacy Officer will maintain copies of executed Subcontractor BAAs with each such subcontractor.

TECHNICAL SAFEGUARDS FOR PHI

Effective Date: May 14, 2018

I. Policy:

A. Purpose

This policy establishes guidelines for having appropriate technical safeguards in place to protect the privacy and security of ePHI.

B. Policy Implementation – General Rule

UNF must reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of its policies and procedures, the HIPAA Regulations, and State law. UNF must also reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

II. Access Control

A. Policy

Procedures will be in place for electronic information systems that host ePHI to allow access only to those persons or software programs that have been granted access rights in accordance with the Information Access Management Standard under the Administrative Safeguard provisions of the HIPAA Security Rule.

B. Procedure

UNF will implement this policy through the following policies and procedures:

i. Section III Unique User Identification

ii. Section IV Automatic Logoff

iii. Section V Audit Controls

iv. Section VI Person or Entity Authentication

III. Unique User Identification

A. Policy

UNF will assign a unique user ID to each workforce member and system for identifying and tracking user identity in networks, programs, and systems hosting ePHI. UNF will select the specific options to achieve this goal within the parameters of its existing

capabilities, but at a minimum each workforce member will have a unique user ID and password as defined below. Employee numbers or other pre-existing individual designations may be used as a substitute for user IDs if UNF systems are only to facilitate the use of existing employee designations.

B. Procedure

i. A unique user ID will be assigned to each individual workforce member. The user ID will identify the workforce member for authentication and granting access. Workforce members are prohibited from sharing user IDs and passwords/passphrases, as set forth on pp. 3 (ITR Acceptable Use) of the **IT Security Practices and Procedures Manual.**

ii. Workforce member activity will be tracked using user IDs. UNF employs the National Institute of Standards and Technology (NIST) publication pertaining to computer security log management (available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf). In addition, UNF will monitor all events within UNF server systems through periodic internal audits of user activity and through use of an UNL-IT Enterprise auditing/tracking tool.

iii. Pursuant to pp. 17 of the **IT Security Practices and Procedures Manual**, access by software programs will be granted only after authentication with valid credentials. The credentials used must not reside in the main, executing body of the software program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server. Database passwords/passphrases will adhere to UNF guidelines on Password/Passphrases (p. 7-8) of the **IT Security Practices and Procedures Manual.** System access will comply with the additional storage, retrieval, and access requirements set forth on pp. 17-18 (Database Password) of the **IT Security Practices and Procedures Manual.**

iv. Shared user IDs are not permitted (other than in the limited circumstance described in paragraph (v)). In the event programs or systems are under consideration for use at UNF that involve the use of shared IDs, the IT Department and Security Officer will evaluate the potential advantages and disadvantages of using such programs/systems that do not have the capability of using unique user IDs. Such evaluation will occur prior to any acquisition or procurement of such systems/programs. In the event the Security Officer and IT Department conclude that such programs/systems are warranted for use at UNF, the Security Officer and IT Department will be required to develop guidelines for use of shared IDs such that access to shared user IDs will be limited, monitored, and changed as needed to restrict and control access in compliance with the HIPAA Regulations.

v. A limited exception to the policy described in paragraph (iv) (above) shall exist pursuant to one of the two following options: (a) event staff at UNF functions will use one mobile computer (maintained by the IT Department), access to which is only available through shared events staff log-in (individual log-ins remain required for access to emails or a Database via the mobile computer). The IT department will establish a protected folder on the mobile computer that is only accessible by designated event staff and event staff may use that folder to save ePHI in use at the event (that would otherwise be on printed materials) in such folder. Such ePHI will reside in such folder until the conclusion of the event and the folder will then be erased by the IT department from the mobile computer. (b) Alternatively, the mobile computer will be maintained by the IT Department, will be checked out only for certain events, and will be returned to the IT Department when the event is over (for removal of stored ePHI). The Privacy Officer will designate one workforce member that is responsible for checking out and maintaining the mobile computer during the event and it shall be UNF's policy that that individual is the only individual permitted to save the events list to the mobile computer, to access ePHI from the mobile computer and is otherwise in charge of managing such list during the event. The designated individual is further charged with returning the mobile computer to the IT Department upon conclusion of the event for removal of stored ePHI.

vi. The basis for paragraph (v), options (a) and (b), is that UNF has concluded that it is more protective of ePHI/PHI for such information to remain on the mobile computer during the event at issue then it is for such information to be maintained in paper format, which would be more susceptible to being lost or misplaced.

IV. Emergency Access of ePHI

A. Policy

UNF will be able to obtain necessary ePHI during an emergency, while conforming to UNF's ePHI access requirements. Because UNF is not involved in the health care provider-patient relationship and because Covered Entities from which UNF receives ePHI have the provider-patient relationship (and have the obligation to maintain ePHI necessary for treatment and related purposes), the need for emergency access to ePHI by UNF is not as pronounced.

B. Procedure

i. The Security Officer (in consultation with the Privacy Officer) is responsible for implementation of UNF's emergency access procedures.

ii. The Security Officer will initiate UNF's emergency access procedures and guidelines, as set forth on pp. 15-16 of the **Administrative Safeguards Policy** and will ensure that selected UNF workforce members have appropriate qualifications and have been trained on these emergency procedures.

iii. ePHI that is necessary to perform UNF services but cannot be accessed by UNF due to an emergency will be obtained from Nebraska Medicine or UNF's subcontractors as necessary and appropriate.

V. Automatic Locking

A. Policy

Workstations and electronic devices that are used to access ePHI, including those with remote access, will be locked out after a predetermined time of inactivity.

B. Procedure

i. Workstations from which ePHI can be accessed will be automatically locked after ten (10) minutes of inactivity, as set forth on pp. 3 (ITR Acceptable Use) of the **IT Security Practices and Procedures Manual**.

ii. Remote access sessions operated through UNF devices will be automatically locked after ten (10) minutes of inactivity, as set forth on pp. 3 (ITR Acceptable Use) of the **IT Security Practices and Procedures Manual**.

iii. Workforce members are not permitted to modify or terminate UNF's automatic logoff functions. All workforce members will be informed of these guidelines during the **HIPAA Education Program**.

iv. Workforce members will be discouraged from using personal devices to remotely access ePHI. UNF will make UNF devices available to staff who need access to work remotely to minimize the use of personal devices to access UNF information. UNF will also train staff regarding the importance of accessing work-related information remotely through UNF devices. UNF has implemented a Mobile Device Management Policy to address risks associated with personal devices.

v. The basis for paragraph (iv) is that UNF has concluded it is unable to control UNF staff from using personal devices to access its web-based applications. It has limited the amount of ePHI accessible through web-based applications and believes it is appropriately safeguarding ePHI through the additional safeguards it is taking regarding personal devices.

VI. Encryption and Decryption of ePHI

A. Policy

ePHI that is "at rest" (not being transmitted) will be encrypted. At rest ePHI will be decrypted only when accessed by authorized workforce members. UNF will encrypt all devices that host ePHI that leave UNF facilities, along with ePHI that is being transmitted.

B. Procedure

i. At rest ePHI will be encrypted using an industry standard encryption process.

ii. All passwords/passphrases saved on UNF information technology resources will be encrypted as provided in the **IT Security Practices and Procedures Manual** (Password/Passphrase, pp. 7-9).

iii. The Security Officer will develop and maintain an inventory of information system components and electronic devices with data encryption capabilities.

iv. The IT Department will encrypt all UNF-sponsored portable devices that go into the field. The encryption will be performed on the hard drive level and use industry standard encryption processes. UNF will also implement remote wipe processes, through Microsoft Intune, when deemed appropriate by the Privacy or Security Officer.

v. ePHI that that is transmitted between UNF and Nebraska Medicine will occur pursuant to one of the "Approved Channels" outlined in Section X.B, below.

vi. The UNF IT Department will evaluate application service providers' encryption standards as part of its overall review and determination of whether UNF should use such application service providers. Standards to be used by the IT Department in making this determination are found in the **IT Security Practices and Procedures Manual** (Application Service Providers, pp. 16). This supports the use of role-based access control policies that define service providers and controls their access based upon UNF's determination of their roles.

vii. Pursuant to the **IT Security Practices and Procedures Manual** (Internet DMZ Equipment, pp. 16), (Router Security, pp. 23-24), Server Security (pp. 24-25) and (Wireless Communication (pp. 26), the IT Department has adopted guidelines for use of encryption technologies to protect UNF information technology resources.

viii. On an ongoing basis, the Security Officer (in consultation with the IT Department) will:

- Assess and measure the risk of ePHI being either unintentionally or maliciously disclosed or modified during preparation for transmission or during reception;
- Consider implementation of added cryptographic mechanisms to prevent unauthorized disclosure of ePHI and detect changes to information during transmission unless otherwise protected by physical security control; and
- Document, and disseminate to workforce members systems and communication protection policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

VII. Audit Controls

A. Policy

Hardware, software and procedural mechanisms that record, store and examine activity in information systems that host or access ePHI will be in place to identify security threats. Audit logs, access reports and security incident reports will be properly protected from tampering, destruction or manipulation.

B. Procedure

i. The **IT Security Practices and Procedures Manual** (pp. 3, ITR Acceptable Use) (pp. 16-17, Audit) provide for UNF's authority to conduct audits of any information technology resources at use and provides of examples of the circumstances in which audits may occur. All workforce members will receive training on UNF's policy of engaging in periodic audits to determine workforce members' compliance with UNF Security and/or Privacy Policies and Procedures.

ii. Scope and frequency of audits are intended to be scalable based on factors such as key audit events (e.g., new or repeated security incidents; increase in volume or type of ePHI maintained by UNF such as use of PHI that is more extensive than "Permitted Fundraising Information"; use of new systems or technologies with which IT Department is not as familiar; disciplinary action against workforce members that requires additional verification of compliance for future activities, etc.).

iii. Scope of issues to be identified in audits are intended to be flexible but may include issues such as the following: (a) are workforce members accessing ePHI through the Ali CRM Database without having completed the initial HIPAA training, and/or accessing ePHI through the Grateful Patient Database without having completed the **HIPAA Education Program**; (b) are workforce members included on the list of

personnel with access to ePHI; (c) does workforce members' access appear to coincide with ongoing fundraising initiatives; (d) are there anomalies in workforce members incidents of successful access (e.g., multiple requests involving the same patient, access involving prominent individuals, etc.); (e) have there been violations of UNF guidelines on fundraising using PHI (e.g., failure to track opt-outs); and (f) has PHI been disclosed to a subcontractor business associate prior to execution of a valid subcontractor business associate agreement.. Other examples of issues subject to audit (and audit guidelines and retention procedures and policies) include those listed in the **IT Security Practices and Procedures Manual** (Internet DMZ Equipment, pp. 19-21) (Audit, pp. 16-17) (Server Security, pp. 24-25).

iv. UNF server logs will automatically record successful and failed access attempts for servers hosting ePHI.

v. Server logs for server hosting ePHI will be periodically reviewed by the Security Officer to ensure that ePHI is being appropriately accessed only by authorized workforce members.

vi. An alert will be automatically generated if an excessive number of inappropriate logon attempts are programmatically detected in a server log.

vii. On an ongoing basis, the Security Officer will document and disseminate to workforce members an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. Issues or problems identified in auditing will be addressed through security reminders or other forms of communications to workforce with the goal of minimizing the likelihood of reoccurrence.

VIII. Integrity of ePHI

A. Policy

ePHI will be safeguarded from unauthorized alteration or destruction by implementation of appropriate procedures.

B. Procedure

i. UNF will implement the system access control procedures set forth in Sections VII-XII of the **Administrative Safeguard Policy** and Sections II-VII of the **Physical Safeguards Policy** to prevent unauthorized workforce members from accessing (and improperly altering or destroying) ePHI.

ii. Remote access to UNF's information technology resources requires execution of a Third Party Connection Agreement (**IT Security Practices and Procedures Manual** (Remote Access, pp. 9-11). The Third Party Connection Agreement requires contractual commitments from parties accessing UNF IT that they will protect against improper alteration, loss, destruction, etc. UNF workforce members with authority to seek execution of the Third Party Connection Agreement will receive training and instruction on the importance of obtaining an executed Third Party Connection Agreement and will be instructed to direct any questions regarding the same to the Security Officer.

iii. Workforce members are prohibited from improperly altering ePHI as part of the guidelines on Unacceptable Use in the **IT Security Practices and Procedures Manual** (ITR Acceptable Use, pp. 3-4). Workforce members will receive training during the **HIPAA Education Program** on not improperly modifying or destroying ePHI. In addition, only designated workforce members that have a need to alter ePHI as part of his or her job duties will be granted access to equipment and systems that house ePHI. Most workforce members will not be granted the permissions necessary to alter ePHI.

iv. Current systems capabilities provide that the only ePHI in the Ali CRM Database that can be updated is biographical information consisting of names and contact information. Risks of more substantial changes to ePHI in the Grateful Patient Database will be addressed through the guidelines discussed above.

v. UNF will perform periodic audits of its systems and data to ensure that ePHI was not improperly altered or destroyed.

IX. Person or Entity Authentication

A. Policy

The identity of a person or entity seeking access to ePHI will be confirmed prior to allowing ePHI access.

B. Procedure

i. User ID and passwords will be used to verify the identity of workforce members and University staff seeking to access ePHI.

ii. All other persons or entities seeking access to ePHI will only be given access after verification and approval by the Privacy Officer.

iii. If UNF staff have questions about whether a person or entity should be allowed to access ePHI, staff must consult with the Privacy Officer.

iv. UNF's IT Department is in the process of implementing multi-factor authentication through a DUO product. Multi-factor authentication will generally involve three forms of authentication by the individual seeking access to ePHI, including; (1) passwords/passphrases; (2) unique user ID; and (3) token code (available over phone or other device). Any default passwords/token codes will be changed when systems for accessing ePHI are initially implemented. UNF is in the process of implementing multi-factor authentication to a test group and has set June 30, 2018, as its target roll out date for full implementation with workforce members. The Security Officer will update these Security Policies and Procedures to the extent necessary to facilitate compliance with multi-factor authentication.

v. All workforce members will receive training on multi-factor authentication as part of the **HIPAA Education Program** or through other appropriate means.

X. Transmission Security and Encryption

A. Policy

ePHI will be protected from unauthorized access when being transmitted over an electronic communications network.

B. Procedure

i. UNF does not permit ePHI to be transmitted by email or text message over any unencrypted network or means of transmission**.** UNF will use Proofpoint to facilitate encrypted communications of ePHI. Guidelines on the improper use of electronic communications, monitoring of electronic communications, auditing of electronic communications and related prohibitions in the **IT Security Practices and Procedures Manual** (ITR Acceptable Use, pp. 3-4; Automatically Forwarded Email, pp. 5; Email Use, pp. 6; Password/Passphrase, pp. 7-9; and Anti-Virus, pp. 12-13) apply to all communications of ePHI. In addition, workforce will receive training and instruction on the use of Proofpoint. The only methodologies by which ePHI may be transmitted are included in Section X.B.ii, below.

ii. Any electronic transmission of ePHI will only occur using the following approved channels: encrypted emails and secure file transfer protocol (the "Approved Channels"). In no event shall communications of ePHI occur through any unapproved channels (e.g., via personal email accounts (Yahoo, Gmail, Hotmail, etc.) or text message). In the event the roster of Approved Channels at UNF changes, the Security Officer will update these Security Policies and Procedures to reflect the same and will ensure that communication of such changes is made to all workforce members.

iii. To the extent access to an Approved Channel for purposes of electronic communication of ePHI is permitted to occur via a personal device, personal devices shall be required to use a screen lock feature with an access code consisting of at least four characters. In no event shall ePHI be stored or maintained on a personally owned device.

iv. Pursuant to the **IT Security Practices and Procedures Manual** (Internet DMZ Equipment, pp. 16), (Router Security, pp. 23-24), (Server Security pp. 24-25) and (Wireless Communication pp. 26), the IT Department has adopted guidelines for use of encryption technologies to protect UNF information technology resources.

v. On an ongoing basis, the Security Officer (in consultation with the IT Department) will:

- Assess and measure the risk of ePHI being either unintentionally or maliciously disclosed or modified during preparation for transmission or during reception;
- Consider implementation of added cryptographic mechanisms to prevent unauthorized disclosure of ePHI and detect changes to information during transmission unless otherwise protected by physical security control; and
- Document, and disseminate to workforce members systems and communication protection policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

XI. Documentation Requirements

A. Policy

UNF has implemented policies and procedures to comply with the standards, implementation specifications, and other requirements of the HIPAA Security Rule. UNF has documented, and will maintain, these policies and procedures in compliance with the HIPAA Regulations.

B. Procedure

i. UNF has implemented policies and procedures to comply with HIPAA Security Rule requirements. These policies and procedure have been documented, and are maintained, in its **Administrative Safeguard Policies and Procedures**, **Physical Safeguard Policies and Procedures**, and **Technical Safeguard Policies and Procedures**.

ii. UNF will retain for six years, in written or electronic form, all documents required to be retained by the HIPAA Regulations. A document will be retained for six years after the date of creation, or six years after the document ceases to be effective, whichever is later. UNF workforce members will be trained on these documentation requirements as part of the **HIPAA Education Program** or through other means, as appropriate.

iii. The Security Officer will make UNF's policies and procedures available to workforce members. UNF's HIPAA Privacy and Security Policies and Procedure Manual can be found on the UNF Intranet site, which can be accessed on the General Counsel Department's page at: https://intranet.nufoundation.org/. If workforce members have questions or are not able to access these policies and procedures, workforce members can request a copy from their supervisor.

iv. The Security Officer will review and update UNF's **Administrative, Physical, and Technical Policies and Procedures** and other security documentation on an annual basis, and as needed in response to environmental or operational changes affecting the security of ePHI.

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

Effective Date: May 14, 2018

I. Policy

A. Purpose

This policy establishes general requirements that must be met by UNF workforce members regarding the use and disclosure of PHI. Guidelines related to UNF's use and disclosure of PHI that is Permitted Fundraising Information for fundraising is addressed more specifically in the **Use and Disclosure of PHI for Fundraising Policy and Procedure**.

B. General Rule

UNF and its subcontractors will not use or disclose PHI except as permitted by the HIPAA Regulations, the **Fundraising Affiliation & Services Agreement** between UNF and Nebraska Medicine (the "Fundraising Agreement"), and these policies and procedures.

C. Use of PHI by UNF

Pursuant to the Business Associate Agreement that was executed as part of the **Fundraising Agreement**, UNF may use and disclose PHI for the following purposes:

1. As necessary to perform the fundraising services on behalf of Nebraska Medicine. The fundraising services are set forth on **Exhibit A** of the **Fundraising Agreement**; Guidelines on UNF's use and disclosure of PHI that is Permitted Fundraising Information for fundraising is addressed more specifically in the **Use and Disclosure of PHI for Fundraising Policy and Procedure**.

2. For UNF's proper management and administration; and

3. To carry out UNF's legal responsibilities.

D. Disclosure of PHI by UNF

UNF may disclose PHI only as necessary to perform the fundraising services on behalf of Nebraska Medicine, for the proper management and administration of UNF, or to carry out UNF's legal responsibilities.

1. Disclosure to Perform Fundraising Services on Behalf of Nebraska Medicine

UNF may disclose PHI to perform the fundraising services set forth in **Exhibit A** of the **Fundraising Agreement**. Guidelines on UNF's use and disclosure of PHI that is Permitted Fundraising Information for fundraising is addressed more specifically in the **Use and Disclosure of PHI for Fundraising Policy and Procedure**.

2. **Disclosures Required by Law**

UNF may disclose PHI when such disclosure is required by law, provided that UNF notifies Nebraska Medicine no less than five (5) business days prior to any such disclosure and provides Nebraska Medicine with an opportunity to seek confidential treatment for any PHI disclosed. UNF will cooperate with Nebraska Medicine if it should seek confidential treatment.

3. **Disclosures for UNF's Own Proper Management and Administration**

UNF may disclose PHI for its own management and administration provided that, prior to the disclosure, UNF obtains reasonable written assurances from the person or entity to whom the PHI is disclosed that:

a. It will be held confidentially and used or further disclosed only as Required by Law or for the lawful purpose for which it was disclosed to the person or entity;

b. The person or entity will notify UNF within two (2) days of any instances of which it is aware in which the confidentiality of the PHI has been breached.

E. **Uses and Disclosures for which an authorization or opportunity to object is not required**

The HIPAA Regulations identify a number of other uses and disclosures of PHI in which covered entities are permitted to engage without obtaining Authorization from the Individual or giving the Individual the opportunity to object. These include:

1. Uses and disclosures for public health activities (45 C.F.R. § 164.512(b));

2. Disclosures about victims of abuse, neglect or domestic violence (45 C.F.R. § 164.512(c));

3. Uses and disclosures for health oversight activities (45 C.F.R. § 164.512(d));

4. Disclosures for judicial and administrative proceedings (45 C.F.R. § 164.512(e));

5. Disclosures for law enforcement purposes (45 C.F.R. § 164.512(f));

6. Uses and disclosures about decedents (45 C.F.R. § 164.512(g));

7. Uses and disclosures for cadaveric organ, eye or tissue donation purposes (45 C.F.R. § 164.512(h));

8. Uses and disclosures for research purposes (45 C.F.R. § 164.512(i));

9. Uses and disclosures to avert a serious threat to health or safety (45 C.F.R. § 164.512(j));

10. Uses and disclosures for specialized government functions (45 C.F.R. § 164.512(k)); and

11. Disclosures for workers' compensation (45 C.F.R. § 164.512(l)).

Under the **Fundraising Affiliation & Services Agreement**, UNF is only permitted to use and disclose PHI for the limited purposes described in sections I.D.1, I.D.2 and I.D.3, above. Accordingly, UNF, as Nebraska Medicine's business associate, will notify Nebraska Medicine prior to using or disclosing PHI for any of the additional purposes described in this section E and will act in accordance with Nebraska Medicine's direction with respect to these uses and disclosures.

F. **Disclosure of PHI to UNF Volunteers**

Access to PHI is typically granted only to UNF employees. At times, however, volunteers may aid in fundraising activities of UNF and it may sometimes be necessary to share PHI with volunteers to assist in those fundraising efforts.

1. **Responsibilities of UNF Workforce Members When Working with Volunteers**

UNF workforce members must comply with the following when disclosing PHI to volunteers:

a. Understand and follow UNF's **Privacy and Security Policies and Procedures**;

b. If there are questions about the ability of volunteers to access PHI, UNF workforce members should contact the Privacy Officer immediately and prior to facilitating any access by volunteers to PHI;

c. Read and sign UNF's **Volunteer Confidentiality Agreement**, providing a signed copy to the Privacy Officer (signatures will be renewed annually);

d. Ensure that volunteers to whom PHI will be disclosed have read the applicable portions of UNF's **Privacy and Security Policies and Procedures**;

e. Disclose PHI to volunteers only as necessary for the perform of his or her job duties, in accordance with the **Minimum Necessary for Requests For, or Uses or Disclosures of, PHI**;

f. Require volunteers to return all materials containing PHI to UNF once the volunteer's fundraising purpose has been fulfilled.

2. **Responsibilities of Volunteers**

Volunteers to whom PHI is disclosed must:

a. Read and follow the applicable parts of UNF's **Privacy and Security Policies and Procedures**;

b. Read, sign, and follow the **Volunteer Confidentiality Agreement**;

c. Protect PHI to ensure there is no unauthorized use or disclosure, in accordance with UNF's **Privacy and Security Policies and Procedures**;

d. Return all PHI to UNF once the volunteer's fundraising role has been completed.

G. **Public Acknowledgment of Gifts**

A gift from a grateful patient who volunteers their own health information (i.e., an individual who is not solicited using PHI (including Permitted Fundraising Information) provided by Nebraska Medicine) may be publicly acknowledged. However, to publicly acknowledge gifts solicited using PHI (including Permitted Fundraising Information) received from Nebraska Medicine, UNF must obtain an Authorization that complies with HIPAA Privacy Rule requirements at 45 C.F.R. § 164.508. In addition, UNF must confirm with Nebraska Medicine that UNF is permitted to seek Authorization from the patient for the public acknowledgement.

H. **Responding to Compliance Reviews and Investigations**

The U.S. Department of Health and Human Services ("HHS") and Office for Civil Rights ("OCR") has the authority to conduct compliance reviews of Nebraska Medicine and/or UNF to determine whether each is complying with HIPAA. HHS/OCR also has the authority to conduct investigations of potential HIPAA violations. It is UNF's policy to fully cooperate and comply with complaint investigations and compliance reviews of Nebraska Medicine or UNF by HHS/OCR. UNF must keep such records and submit such compliance reports, as HHS/OCR may determine to be necessary, to enable HHS/OCR to ascertain whether Nebraska Medicine and/or UNF has complied with applicable HIPAA Regulations. UNF also must permit access by HHS/OCR during normal business hours to its facilities, books, records, accounts, and other sources of information, including PHI, that are pertinent to ascertaining compliance with the applicable HIPAA Regulations.

I. **Uses and Disclosures that UNF will Not Engage In**

UNF and its staff are not permitted to use or disclose PHI for the following purposes, unless UNF obtains written permission from Nebraska Medicine; develops (or receives from Nebraska Medicine) template Authorization form that complies with Privacy Rule requirements at 45 C.F.R. § 164.508; and otherwise complies with all applicable requirements under the HIPAA Regulations.

1. Marketing (45 C.F.R. § 164.508(a)(3)); and

2. Sale of PHI (45 C.F.R. § 164.502(a)(5)(ii)).

II. Procedure

A. UNF and its workforce will use and disclose PHI in accordance with this Policy.

B. Whenever PHI needs to be used for reasons other than those permitted by this Policy, UNF workforce members must address such use or disclosure with the Privacy Officer, who will investigate and determine the appropriate course of action.

USE AND DISCLOSURE OF PHI FOR FUNDRAISING

Effective Date: May 14, 2018

I. Policy:

A. Purpose

The purpose of this policy is to establish guidelines for workforce members to follow to address compliance with HIPAA and the **Fundraising Affiliation & Services Agreement** with respect to using or disclosing PHI for fundraising purposes. This policy also outlines the proper procedures to follow when an Individual opts outs of receiving fundraising communications.

B. Policy Implementation

UNF provides fundraising services to Nebraska Medicine pursuant to the **Fundraising Affiliation & Services Agreement**, and such services require UNF to use and disclose PHI on behalf of Nebraska Medicine. UNF may use and disclose PHI for these fundraising purposes only in accordance with the HIPAA Regulations and this Policy.

Examples of common fundraising communications made on behalf of Nebraska Medicine include annual mailings and sponsorship of events that make an appeal for money; phone calls or emails to solicit donations; and organizing "reunions" where development officers are present. However, the Privacy Rule regulates many other activities as "fundraising" even if they do not directly involve a communication to a potential donor. Examples of uses and disclosures of PHI that are treated as fundraising are listed in section I.B.1.5. **Fundraising without an Authorization**.

UNF may use and disclose certain PHI consisting of Permitted Fundraising Information for fundraising without a HIPAA "Authorization" (defined below), if UNF complies with the requirements stated in section I.B.2 below, and the following circumstances are met:

a. The fundraising is for the benefit of Nebraska Medicine;

b. Any disclosures to a subcontractor business associate are addressed in a business associate agreement (or otherwise permitted under HIPAA) and complies with UNF's **Disclosing Information to Subcontractor Business Associates Policy**;

c. Nebraska Medicine provides its Notice of Privacy Practices to all patients at registration. The Notice of Privacy Practices must continue to state that Nebraska Medicine and/or UNF, as Nebraska Medicine's business associate, may contact the Individual to raise funds for Nebraska Medicine and the Individual has a right to opt out of receiving such communications;

d. The uses and disclosures of PHI are limited to the following subset of PHI (the "Permitted Fundraising Information"):

i. Demographic information related to the Individual, including name, address, other contact information, age, gender, and date of birth;

ii. Dates of health care provided to an Individual;

iii. Clinical department where services were provided (i.e., at Oncology Center, Department of Pediatrics, Center for Social Work, etc.);

iv. Treating physician;

v. Outcome information (e.g., information about the death of a patient or other result of treatment); and

vi. Health insurance status.

2. **Other requirements**

If pursuant to section I.B.1, if UNF uses or discloses Permitted Fundraising Information for fundraising purposes without the Individual's "Authorization" (as defined at 45 C.F.R. § 164.508 and discussed in more detail in section I.B.3, below), UNF shall satisfy the following requirements:

a. With each fundraising communication made to an Individual, UNF must provide the Individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an Individual to elect not to receive further fundraising communications may not cause the Individual to incur an undue burden or more than a nominal cost;

b. UNF and Nebraska Medicine may not condition treatment or payment on the Individual's choice with respect to the receipt of fundraising communications;

c. UNF may not make fundraising communications to an Individual where the Individual has elected not to receive such communications; and

d. UNF may provide an Individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.

3. **Authorization required**

HIPAA requires UNF to obtain a valid Authorization in compliance with the Privacy Rule prior to using or disclosing PHI for the purpose of fundraising if any of the requirements in sections I.B.1 or I.B.2 are not met. Pursuant to the **Fundraising Affiliation & Services Agreement**, Nebraska Medicine will provide PHI to UNF that is not Permitted Fundraising Information only if Nebraska Medicine has first received written Authorization from the Individual permitting Nebraska Medicine and UNF to contact the Individual with solicitations. The Individual may revoke this Authorization in writing at any time. For example, Nebraska Medicine and UNF would need to get authorization for any fundraising that:

a. Is for the benefit of an entity other than Nebraska Medicine, even if the information at issue would otherwise be Permitted Fundraising Information;

b. Involves activities that are more extensive than fundraising and instead meet the definition of "Marketing" under the Privacy Rule. Additional guidance on "Marketing" is discussed in section I.B.4, below;

c. The PHI used or disclosed includes information other than the Permitted Fundraising Information listed in section I.B.1(d) above. For example, this would include UNF using information about a specific illness, diagnosis or disease of recipients to raise funds (instead of only using department of service information) or UNF targeting families of pediatric patients who received treatment for particular conditions (e.g., sarcoma, Von Willebrand's disease) within the department.

A valid authorization must be written in plain language and contain all of the elements set forth at 45 C.F.R. § 164.508, including but not limited to a clear description of the information to be disclosed, the purpose of the disclosure, and name of the individual to whom Nebraska Medicine and/or UNF is making the disclosure. Additional required elements can be found at 45 C.F.R. § 164.508.

4. **Regulation of Marketing under the Privacy Rule**

"Marketing" is defined as a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. There are limited exceptions to this definition under 45 C.F.R. § 164.501, including communications made for certain treatment and health care operations purposes.

UNF is not permitted to engage in Marketing communications on behalf of Nebraska Medicine under the **Fundraising Affiliation & Services Agreement**. In addition, should Nebraska Medicine request that UNF engage in Marketing on its behalf under another arrangement, Nebraska Medicine and UNF must obtain HIPAA authorization prior to making the Marketing communication, unless the communication is:

I. A face-to-face communication made by Nebraska Medicine or its workforce to an individual; or

II. A promotional gift of nominal value.

If the Marketing involves any direct or indirect payments to Nebraska Medicine or UNF from or on behalf of a third party whose product or service is being described in the communication ("Financial Remuneration"), Nebraska Medicine and UNF must include language in the authorization form that clearly states remuneration in involved. Direct or indirect payments do not include any payments for treatment of an individual.

5. **Examples of Fundraising Activities**

In addition to the examples of communications that are considered "fundraising" uses and disclosures described in section I.B (Policy Implementation), the following uses and disclosures of PHI are also treated as "fundraising" and are therefore subject to this policy:

a. UNF uses Permitted Fundraising Information to compile a list of patients who were treated by oncologists (or in the oncology department) and then contacts patients to ask for contributions to help fund cancer research.

b. UNF uses Permitted Fundraising Information first from a department of service at Nebraska Medicine (e.g., cardiology) and then narrows based on treating physician within the cardiology department and then contacts patients to ask for contributions to support the physician's department of service (i.e., cardiology department).

c. UNF uses Permitted Fundraising Information from Nebraska Medicine to contact patients treated at the kidney clinic to ask for contributions to fund the development of a kidney transplant program to train medical students.

d. UNF uses outcome information to exclude from the grateful patient program any patients that had sub-optimum outcomes.

e. UNF engages a wealth screening vendor to assist in identifying patients or a printing house to assist in mailings of solicitations to patients/potential donors.

f. UNF uses any category of Permitted Fundraising Information to exclude patients from a fundraising initiative (e.g., insurance status).

g. UNF uses Permitted Fundraising Information to contact patients to invite them to an educational seminar on weight management and UNF development officers are fundraising at the seminar.

h. UNF organizes a "transplant reunion" component to a fundraising event based on the identities of treating physicians at Nebraska Medicine.

These are only examples and are not intended to be a complete list of uses and disclosures of PHI that would be treated as fundraising. UNF workforce members who are not sure whether a particular type of use or disclosure of PHI would be considered "fundraising" should contact the Privacy Officer prior to engaging in the use or disclosure.

6. **Public Acknowledgement of Gifts**

Public acknowledgement of gifts is not considered a fundraising use or disclosure. It is subject to the **UNF Use and Disclosure of Protected Health Information** policy.

II. Procedure:

A. Information in the Grateful Patient Database is PHI (including Permitted Fundraising Information) and is subject to the Privacy Rule and this policy. UNF has implemented a procedure to flag information that is Permitted Fundraising Information in the Ali CRM Database so that permitted uses and disclosures of that information can occur pursuant to the Privacy Rule and this policy while information in the Ali CRM Database that is not PHI/Permitted Fundraising Information can continue to be used and disclosed in accordance with other UNF guidelines related to fundraising that does not involve PHI.

B. Information that is derived from sources other than Nebraska Medicine (or another Covered Entity or Business Associate, to the extent UNF has additional relationships in the future with other Covered Entities/Business Associates) is not PHI and is not subject to HIPAA. For example, mailings to all local residents, purchased mailing lists, alumni uploads or based on some other criteria not involving the use and disclose of PHI from Nebraska Medicine is not subject to HIPAA.

C. If UNF receives information directly from individuals (or via one of the other examples discussed in section II.B), that information is not PHI. However, if UNF has a record of the same Individual in either Database that includes PHI, the production of information directly from the Individual would not modify the status of information in the Database from PHI into non-PHI.

D. Information that is PHI and is maintained by UNF in either Database remains PHI subject to HIPAA. If a Database includes only PHI (i.e., they are maintained separately from other donor databases that do not include PHI), the HIPAA Regulations only apply to the Databases that maintain PHI. If PHI is combined or mixed with other information into the same Database, the PHI does not lose status as such but remains PHI that can only be used and disclosed for fundraising as permitted under the Privacy Rule and this policy.

E. The status of any information that is PHI (including Permitted Fundraising Information) can only be modified in the event the information is de-identified in accordance with 45 C.F.R. § 164.514(b). UNF may not de-identify PHI except as necessary to provide services under the **Fundraising Affiliation & Services Agreement**. UNF may not use or disclose any such de-identified information for its own purposes without the prior written consent of Nebraska Medicine. In addition, UNF may not disclose such de-identified information to any third party who may re-identify such information in violation of the HIPAA Regulations.

F. UNF and its workforce members may only use or disclose information that is Permitted Fundraising Information to solicit donations or otherwise support fundraising for the benefit of Nebraska Medicine. This is the case even when the same donors may give (or

may have given) to support other UNF fundraising efforts, such as the University of Nebraska generally.

G. If UNF has independent donor information from an Individual (i.e., no PHI disclosed from Nebraska Medicine but a donor record based on the Individual supporting University of Nebraska generally), that information does not become PHI if the Individual is a patient of Nebraska Medicine. However, if that Individual becomes a patient of Nebraska Medicine and his/her PHI is disclosed to UNF from Nebraska Medicine, the information is PHI and is subject to this policy.

H. Donors who have connections to both the University of Nebraska and Nebraska Medicine may be solicited for University of Nebraska and/or Nebraska Medicine purposes. However, PHI (including Permitted Fundraising Information) may not be used to solicit charitable contributions or other donations for University of Nebraska purposes, or for any other purpose that is not on behalf of Nebraska Medicine.

I. Donors' self-disclosure of other interests while being solicited for Nebraska Medicine purposes will be documented on the constituent record by UNF workforce members and will not preclude future fundraising efforts to support University of Nebraska purposes. However, information about an Individual that is PHI because it was disclosed to UNF from Nebraska Medicine does not lose its status as such due to donations to support general University of Nebraska purposes.

J. UNF is permitted to add attendees brought as guests of a patient (whose information was provided to UNF by Nebraska Medicine) to databases that do not hold PHI and engage in general solicitations of those individuals. UNF could also add this information to Databases that do contain PHI (subject to the guidelines in section II.D on mixing PHI and non-PHI) and engage in general solicitations of those individuals. Regardless of where the information about the non-patient is maintained, any solicitations of the patient would need to continue to be only for the benefit of Nebraska Medicine.

K. Prior to using or disclosing PHI for fundraising purposes, UNF's Privacy Officer or designee must:

1. Determine whether the information is Permitted Fundraising Information that meets the requirements of sections I.B.1 and I.B.2 and that the other requirements outlined in those sections are addressed;

2. Determine whether a HIPAA authorization is required for the use or disclosure of the PHI;

3. Verify that a valid authorization has been obtained by Nebraska Medicine, if it is determined that an authorization is needed;

4. Verify that the other requirements described in this policy have been met.

L. When Individuals opt out of receiving future fundraising solicitations:

1. Individuals who have requested to be removed from future Nebraska Medicine and/or UNF fundraising communications will be appropriately coded as having opted out on their Ali CRM constituent record and in the Grateful Patient Database. The following information should be captured by UNF during the opt-out process:

    a. Individual's name and contact information;

    b. Date of request; and

    c. Whether the patient wants to opt-out of all fundraising communications or only specific materials.

2. Any UNF workforce member advised by an Individual of his or her request to opt out (even if that request is made verbally by the Individual through a telephone call to the phone number below) of receiving future fundraising communications must contact UNF at nebraskamedicineoptout@nufoundation.org to document the request.

3. Written materials mailed or emailed to Individuals for the purpose of soliciting a donation must include the following UNF-approved opt-out language:

    If you wish to no longer be contacted by the University of Nebraska Foundation on behalf of Nebraska Medicine, please call 402-502-4095 or email nebraskamedicineoptout@nufoundation.org.

4. Verbal communications (in person or by phone) made by UNF staff must also advise the Individual of the right to opt out of receiving future solicitations using the following UNF-approved opt-out language:

    Thank you for your time today. Please remember that you can elect not to receive any future calls or mailings from us. Just let us know if you prefer that we not contact you regarding any further fundraising efforts.

5. As long as the communication does not contain any solicitations, UNF may use or disclose Permitted Fundraising Information to engage in communications with Individuals on behalf of Nebraska Medicine relating to increasing public awareness and education about clinical care options at Nebraska Medicine, developments in care delivery, descriptions of research breakthroughs at Nebraska Medicine (though not to recruit Individuals to participate in research), promoting health, alternative treatments and related activities that do not constitute Marketing. Notwithstanding the foregoing, if there is a question as to whether a communication would be considered to include a

"solicitation," it will be treated as including a solicitation and must require the opt-out language as described herein. In addition, although the types of communications described in this section may not be subject to these fundraising rules, they may be subject to other requirements under the HIPAA Regulations.

6. If an Individual opts out of receiving future Nebraska Medicine solicitations and UNF has a constituent record for that individual that is not PHI, the individual may still be solicited for University of Nebraska fundraising initiatives that are unrelated to his or her status as a Nebraska Medicine patient. These solicitations will be governed by UNF policies and procedures related to University of Nebraska fundraising.

M. Departments or individual physicians that wish to engage in fundraising activities must contact the Nebraska Medicine Chief Development Officer for assistance in and coordination of such fundraising activities. Such coordination is necessary to ensure that Individuals that have opted out of receiving fundraising communications are not contacted; that the department or individual treating physician does not inadvertently engage in uses or disclosures of information that is more extensive than Permitted Fundraising Information; and to be sure that all privacy and fundraising-related policies are followed when conducting such activities.

N. UNF staff will comply with the **Minimum Necessary for Requests for, or Uses or Disclosures of, PHI Policy** when using and disclosing Permitted Fundraising Information and other PHI.

O. All questions about this policy should be directed to the Privacy Officer.

WORKFORCE PRIVACY TRAINING

Effective Date: May 14, 2018

I. Policy

A. Purpose

This policy is to provide guidelines for training all members of UNF's workforce on the privacy practices, policies, and procedures used by UNF for complying with the HIPAA Regulations.

B. Policy Implementation

UNF must train all members of its workforce on the policies and procedures regarding PHI, as necessary and appropriate for the members of its workforce to carry out their functions within UNF. "Workforce" includes UNF employees, University of Nebraska staff, volunteers, trainees, and other persons whose conduct, in the performance of work for UNF, is under the direct control of UNF, whether or not they are paid by UNF.

C. Training Requirements

All UNF workforce members must complete the **HIPAA Education Program**. All new workforce members must complete the **HIPAA Education Program** within thirty (30) days of commencing their workforce relationship at UNF or assuming such new roles or responsibilities. Workforce members must complete an initial HIPAA training program prior to receiving credentials that permit access to the Ali CRM Database, and must complete the full **HIPAA Education Program**, and any other required training, prior to receiving credentials that permit access to the Grateful Patient Database. Additional trainings will be provided to workforce members depending on their level of access to PHI/ePHI and their job duties.

UNF will provide training as follows:

1. To each member of the current workforce that has not yet participated in the **HIPAA Education Program**, no later than thirty (30) days after the effective date of this Manual.

2. To each new member of UNF's workforce within thirty (30) days of commencing their workforce relationship at UNF or assuming such new roles or responsibilities; and

3. Following completion of the initial training, to each member of UNF's workforce on an annual basis and as needed to inform workforce about any legal, operational, or environmental changes or updates.

II. Procedure

A. The Privacy Officer will oversee the training of each workforce member on UNF Privacy Policies and Procedures. The Security Officer will oversee the training of each workforce member on UNF Security Policies and Procedures, as set forth in the **Administrative Safeguards for PHI Policies and Procedures**. UNF will be responsible for training all workforce members with access to the Grateful Patient Database.

B. Nebraska Medicine has agreed that it is appropriate to have bifurcated training as follows: All new workforce members must complete the **HIPAA Education Program** within thirty (30) days of commencing their workforce relationship at UNF or assuming such new roles or responsibilities. Workforce members must complete an initial HIPAA training program prior to receiving credentials that permit access to the Ali CRM Database and execute an acknowledgement of completion of the same and that they have read and understood the HIPAA policies and procedures. Workforce members must complete the full **HIPAA Education Program**, and any other required training, prior to receiving credentials that permit access to the Grateful Patient Database.

C. University of Nebraska staff are otherwise subject to all UNF Security and Privacy Policies and Procedures and will be considered part of the UNF workforce for purposes of compliance with the HIPAA Regulations.

D. The Privacy Officer and Security Officer will conduct refresher training sessions annually. Additional trainings will be provided throughout the year with respect to any legal, operational, or environmental changes or updates, as well as for workforce (as necessary) depending on their level of access to PHI and their job duties.

E. The Privacy Officer will ensure that each workforce member with access to PHI receives sufficient training to carry out his or her job duties and responsibilities in compliance with the UNF Privacy Policies and Procedures.

F. The Privacy and Security Officer will document all training provided and monitor attendance and successful completion by UNF workforce. The **HIPAA Overview & Privacy Training Sign In Sheet** (or a substantially similar document) will be tracked and maintained by the Privacy Officer.

BREACH OF UNSECURED PHI

Effective Date: May 14, 2018

I. Policy

A. Purpose

UNF must comply with rules related to privacy incident response and breach notification. UNF will immediately respond to any actual or potential Breach of PHI, including any use or disclosure of PHI not authorized by the **Fundraising Affiliation & Services Agreement** and any successful security incident (collectively referred to as a "Privacy Incident") to ensure confidentiality is maintained and to mitigate any adverse effects resulting from the Privacy Incident.

B. In General

UNF will investigate all Privacy Incidents pursuant to the following procedure:

1. **Notification of Privacy Officer by UNF Staff**

   UNF workforce members will immediately notify the Privacy Officer of any Privacy Incident. The Privacy Officer will ensure that any necessary training occurs so that UNF workforce members understand their obligations to make such reports to the Privacy Officer.

2. **Notification of Nebraska Medicine by UNF Privacy Officer**

   The Privacy Officer will notify Nebraska Medicine of the Privacy Incident within two (2) business days of when UNF first becomes aware of the Privacy Incident. The report will include the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by UNF to have been, accessed, acquired, used or disclosed.

   As soon as possible thereafter, the Privacy Officer will provide Nebraska Medicine with a description of the following (to the extent it is known):

   a. What happened, including the date of the acquisition, access, use or disclosure and the date of its discovery;

   b. The types of Unsecured PHI involved in the acquisition, access, use or disclosure;

   c. Any steps Individuals should take to protect themselves from potential harm from the acquisition, access, use or disclosure; and

d. What UNF is doing to investigate the acquisition, access, use or disclosure to mitigate harm to Individuals, and to protect against any further unpermitted acquisition, access, use or disclosure of Unsecured PHI.

3. **Risk Assessment to Determine Whether the Privacy Incident is a Breach**

Pursuant to the **Fundraising Affiliation & Services Agreement**, UNF will cooperate with Nebraska Medicine's investigation and/or risk assessment with respect to any Privacy Incident that is reported under section I.B.2 (above) and will abide by Nebraska Medicine's decision with respect to whether such Privacy Incident constitutes a Breach of Unsecured PHI. UNF will follow Nebraska Medicine's instructions with respect to any reported Privacy Incident.

Upon Nebraska Medicine's request, the Privacy Officer will conduct a documented risk assessment of the violation to determine if the Privacy Incident meets the regulatory definition of "Breach" or if it can be demonstrated that there is a low probability that the PHI has been compromised based on an analysis of certain factors, as set forth under the HIPAA Regulations at 45 C.F.R. § 164.402. The Privacy Officer will conduct this risk assessment in accordance with the following procedure:

a. **Exceptions**

The Privacy Officer will determine and document if the violation meets any of the regulatory exceptions to the definition of Breach at 45 C.F.R. § 164.402(1)(i)-(iii). These exceptions include:

i. An unintentional acquisition, access, or use of PHI by a UNF workforce member or person acting under the authority of UNF, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure.

ii. Any inadvertent disclosure by a person who is authorized to access PHI at UNF to another person authorized to access PHI at UNF, and the information received as a result of such disclosure is not further used or disclosed.

iii. A disclosure of PHI where UNF has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

b. **Risk Assessment Factors**

Except as provided directly above, any unauthorized use or disclosure of PHI in violation of the Privacy Rule is presumed to be a Breach. However, the Privacy Officer will upon request from Nebraska Medicine conduct a documented risk

assessment of the violation to determine if the regulatory definition of "Breach" has been triggered by the Privacy Incident or if it can be demonstrated that there is a low probability that the PHI has been compromised based on an analysis of at least the four factors set forth below. However, additional factors may need to be considered to appropriately assess the risk that the PHI has been compromised, given the circumstances of the impermissible use or disclosure, and as determined to be appropriate by the Privacy Officer.

i. The nature and extent of the PHI involved including the types of identifiers and the likelihood of re-identification. Examples of particularly sensitive data would include an individual's social security number, credit card number, or health history.

ii. The unauthorized person who used the PHI or to whom the disclosure was made. For example, a recipient who is obligated to abide by HIPAA (e.g., one of UNF's subcontractor business associates) generally poses a lower risk of compromising the PHI than someone who has no independent obligations to comply with HIPAA.

iii. Whether the PHI was actually acquired or viewed. For example, PHI is not actually acquired or viewed when a laptop containing PHI is stolen or lost and a forensic study of the laptop shows that the PHI was never accessed. PHI would be actually acquired or viewed if UNF mails a letter that contains PHI to the wrong person and the person opens the letter.

iv. The extent to which the risk to the PHI has been mitigated. For example, there may be a lower risk of compromise if UNF receives satisfactory assurances from the recipient that there was no further use or disclosure of the PHI and that the PHI has been destroyed.

UNF's analysis should include each of the factors discussed above and such other factors as the Privacy Officer determines to be necessary. UNF will then evaluate the overall probability that the PHI has been compromised by considering all factors in combination.

c. **Burden of Proof**

In the event of a use or disclosure of PHI in violation of the Privacy Rule, UNF has the burden of demonstrating that the use or disclosure does not constitute a Breach.

4. **Mitigation and Notification**

If the Privacy Incident is determined to be a Breach arising out of the acts or omissions of UNF or its agents/subcontractors, UNF has agreed (pursuant to the **Fundraising**

Affiliation & Services Agreement) to perform (or pay the cost of Nebraska Medicine's performance of), reasonable mitigation or remediation services. This includes, at a minimum, the following:

a. Providing notice to Individuals affected by the Breach as Nebraska Medicine reasonably determines to be required;

b. Providing any required notice of the Breach to government agencies, the media, and/or other entities as Nebraska Medicine reasonably determines to be required;

c. Providing individuals affected by the Breach with credit protection services designed to prevent fraud associated with identity theft crimes for a specific period of time (which will not exceed twelve (12) months), except to the extent applicable law specifies a longer period of time;

d. Providing reasonable contact support in the form of a toll-free number for affected individuals for a specific period of time not less than ninety (90) calendar days, except to the extent applicable law specifies a longer period of time;

e. Paying reasonable fees associated with computer forensics work required for investigation activities related or relevant to the Breach;

f. Paying nonappealable fines or penalties assessed by governments or regulators;

g. Paying reasonable costs or fees associated with any obligations imposed by applicable law, including the HIPAA Regulations; and

h. Undertaking any other action both UNF and Nebraska Medicine agree to be appropriate.

5. **Notification to Individuals**

The Privacy Officer will provide required notification to Individuals without unreasonable delay, but in any event within sixty (60) calendar days after the date the Breach was discovered. The Privacy Officer will give notice in the manner described in 45 C.F.R. § 164.404(d) and will reasonably cooperate with Nebraska Medicine regarding the content and timing of the notice. The notification will contain the following information:

a. A brief description of what happened, including the date of the Breach and date of discovery of the Breach, if known;

b. A description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, or other types of information were involved);

c. Any steps the Individual(s) should take to protect themselves from potential harm resulting from the Breach;

d. A brief description of what UNF is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any further Breaches; and

e. Contact procedures for Individuals to ask questions or learn additional information, which will include a toll-free telephone number, an e-mail address, website, or postal address.

6. **Notification to the Secretary of Department of Health & Human Services**

Following the discovery of a Breach of Unsecured PHI, UNF has agreed (pursuant to the **Fundraising Affiliation & Services Agreement)** to notify the Secretary of the United States Department of Health and Human Services in accordance with 45 C.F.R. § 164.408. For Breaches of Unsecured PHI involving 500 or more Individuals, UNF will provide notice to the Secretary contemporaneously with the notice to Individuals discussed above and in the manner specified on the HHS website. For Breaches of Unsecured PHI involving fewer than 500 Individuals, UNF will maintain a log or other documentation of such Breaches and, not later than sixty (60) days after the end of each calendar year, provide notice to the Secretary of Breaches discovered during the preceding calendar year, in the manner specified on the HHS website. UNF can make this notification on the HHS Website.

7. **Notification to the Media**

For any Breach involving more than 500 Individuals, UNF has agreed (pursuant to the **Fundraising Affiliation & Services Agreement)** to notify the media in accordance with 45 C.F.R. § 164.406. UNF will provide such notice without unreasonable delay and in no case later than sixty (60) calendar days after discovery of a Breach. UNF will reasonably cooperate with Nebraska Medicine regarding the content and timing of the notice.

C. **Retention**

The Privacy Officer will maintain a log of all Privacy Incidents, risk assessments and Breach notifications made by the UNF pursuant to this policy. The log should maintain documentation that all required notifications were made, or alternatively, of the risk assessment analysis that an impermissible use or disclosure did not constitute a Breach in cases where it was determined that a Breach did not occur. All phases of the process must be documented in detail on a case-specific basis, in a manner sufficient to demonstrate all

appropriate steps were completed. All supporting documentation associated with the Privacy Incident will be maintained for a minimum of six (6) years.

II. Procedure

The Privacy Officer and UNF workforce members will comply with the procedures set forth in this policy when responding to any Privacy Incident.

SANCTIONING WORKFORCE MEMBERS WHO VIOLATE UNF POLICIES

Effective Date: May 14, 2018

I. Policy

A. Purpose

This policy outlines a process for imposing sanctions in the event that UNF's policies and procedures for the privacy and security of PHI or ePHI are violated.

B. General Rule

UNF shall apply appropriate sanctions against members of its workforce and business associates who fail to comply with UNF's policies and procedures for the protection of PHI/ePHI and/or the HIPAA Regulations, including, but not limited to, violations of requirements applicable to workforce under the **IT Security Practices and Procedures Manual**.

Workforce members should be aware that UNF's system has the ability to identify when, and by whom, ePHI/PHI has been accessed. Workforce members have been entrusted with accessing such information on a need-to-know basis; if an audit and review of access by a workforce member determines that such access could not be justified on a need-to-know basis, the sanction procedure will be utilized.

In addition to these policies and procedures, UNF's **Employee Handbook** provides for disciplinary action against employees who violate UNF policies.

Workforce are thus expected to take an active role in protecting individual privacy rights. If there is reasonable doubt on the part of workforce members as to their right to access PHI/ePHI about an individual they should consult with their supervisor and act accordingly.

C. Exceptions

UNF will not impose sanctions against members of its workforce or business associates for:

1. Engaging in whistleblower activities;

2. Disclosure by workforce members who are victims of a crime;

3. Submitting a complaint to the Secretary of the Department of Health and Human Services;

4. Participating in an investigation of UNF's compliance with the HIPAA Regulations; or

5. Registering opposition to a violation of these policies and procedures or the HIPAA Regulations.

D. Sanctions

1. *Members of UNF's workforce* who violate UNF's policies and procedures for the protection of PHI/ePHI will be subject to sanctions, which may include, but are not limited to, suspension or termination of employment. The type of sanction imposed will depend on the severity of the violation. For additional detail about the sanctions that may be applied, please refer to the **Employee Handbook** on page 5 under "Disciplinary Action."

2. *Volunteers* who materially violate UNF's policies and procedures for the protection of PHI/ePHI shall not be permitted to provide further assistance to UNF as a volunteer.

3. *Business Associates***.** If UNF knows of a pattern of activity or practice of a business associate that constitutes a material breach or violation of the business associate's obligations under his/her/its contract with UNF, UNF will provide written notice of such breach and provide an opportunity for the business associate to cure the breach or end the violation, as applicable. If such steps are unsuccessful, UNF will terminate the contract or other arrangement with the business associate.

II. Procedure:

A. As part of the training requirements, UNF shall inform members of its workforce of this sanction policy. UNF shall also instruct members of its workforce to bring potential violations of these policies and procedures to the attention of the Privacy and/or Security Officers, as appropriate.

B. When the Privacy and/or Security Officers becomes aware of a potential violation of these policies and procedures, such Officer shall:

1. Investigate and document the potential violation;

2. Notify other appropriate persons in authority, including but not limited to the Human Resources Manager and workforce member's supervisor;

3. If a violation is found to have occurred:

   a. Determine the cause of the inappropriate use and/or disclosure and take corrective actions to prevent such uses and/or disclosures from re-occurring;

b. Take all practicable steps to mitigate the harmful effects of a confirmed inappropriate use or disclosure;

c. Formulate a corrective action plan to address the violation;

d. Impose sanctions as appropriate, giving consideration to whether the use or disclosure was made as a result of: (i) carelessness or negligence; (ii) curiosity; (iii) concern for individual welfare; or (iv) the desire for personal gain or malice; and

4. If sanctions are applied, document the sanctions imposed for the violation and retain the documentation in written or electronic form for at least six (6) years.

MINIMUM NECESSARY FOR REQUESTS FOR, OR USES OR DISCLOSURES OF, PHI

Effective Date: May 14, 2018

I. Policy

A. Purpose

The purpose of this policy is to limit the use and disclosure of PHI to only that which is needed for the purpose of the use or disclosure, in situations where the minimum necessary principle applies.

B. Rule

When using or disclosing PHI, or when requesting PHI from Nebraska Medicine, UNF will make reasonable efforts to limit use and disclosure of PHI to the minimum necessary to carry out the purpose of the use, disclosure, or request.

This "minimum necessary standard" does not apply to the following categories of uses and disclosures of PHI:

1. Disclosures to the Individual who is the subject of the information;
2. Uses and disclosures made in accordance with an Authorization;
3. Uses and disclosures Required by Law;
4. Disclosures made to the Secretary of the Department of Health and Human Services as part of an investigation of UNF's compliance with HIPAA; and
5. Disclosures to a health care provider for treatment.

II. Procedure

A. UNF and its workforce members will apply the minimum necessary rules outlined in this policy to uses, disclosures, and requests for PHI.

B. The Privacy Officer is responsible for making determinations regarding the appropriate level of access to PHI by UNF workforce, in accordance with the Privacy and Security Policies and Procedures. The Security Officer will oversee implementation of access on a technical level, in accordance with the Security Policies and Procedures.

C. The Privacy Officer has identified workforce members that need access to Permitted Fundraising Information to carry out their job duties and, for each person, has identified the category(ies) of Permitted Fundraising Information to which access is needed and any conditions that are appropriate to such access. The Privacy Officer has made efforts to

limit the access of UNF workforce in accordance with the HIPAA Regulations. As set forth in the **Protected Health Information—Defined Policy**, Permitted Fundraising Information includes the following categories of PHI:

1. Demographic information, including name, address, other contact information, age, gender, and date of birth;

2. Dates of health care provided to an Individual;

3. Clinical department where services were provided (i.e., at Oncology Center, Department of Pediatrics, Center for Social Work, etc.);

4. Treating physician;

5. Outcome information (e.g., information about the death of a patient or other result of treatment); and

6. Health insurance status.

D. The Privacy Officer has determined that the UNF workforce members listed on **Schedule A** need access to the Grateful Patient Database, which contains Permitted Fundraising Information, to perform their job duties.

E. The Privacy Officer has determined that the UNF workforce members listed on **Schedule B** need access to ePHI in the Foundation Advancement CRM (referred to herein as the "Ali CRM Database"), to perform their job duties. The specific members are identifiable by running a search following the search instructions on **Schedule B**.

F. Prior to having access to the Databases, UNF will ensure that the workforce member has completed a background check consistent with the requirements outlined in the Business Associate Agreement set forth in the **Fundraising Affiliation & Services Agreement** effective November 1, 2017.

G. UNF will adhere to the guidelines in the **Administrative Safeguards for PHI Policies and Procedures** pertaining to training and education for the Grateful Patient Database and the Ali CRM Database in making access to either Database available to workforce. UNF will terminate access if such workforce member fails to follow UNF's **Privacy and Security Policies and Procedures**, no longer needs access to perform their job duties, or if they are no longer employed by (or otherwise providing services to) UNF. The Privacy Officer will also review access levels to make any necessary modifications on an annual basis.

H. The Privacy Officer has determined that UNF will make certain requests for, and uses and disclosures of, PHI consisting only of Permitted Fundraising Information for fundraising purposes on a routine and reoccurring basis. The Privacy Officer, with the assistance of the Security Officer, will implement and comply with UNF's **Privacy and Security Policies and Procedures** to limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

I. UNF workforce members will notify the Privacy Officer of all other requests for disclosures (i.e., non-routine and non-recurring disclosures) of PHI. The Privacy Officer will review the request on an individual basis and will determine how best to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought. Examples of disclosures that must be referred to and reviewed by the Privacy Officer include:

1. Requests for disclosure of PHI made by third-parties with which UNF does not have a subcontractor business associate agreement;

2. Requests for disclosures of PHI that are for "Marketing" as defined in 45 C.F.R. § 164.501;

3. Subpoenas and/or court orders; and

4. Investigations by law enforcement.

No workforce members will request, use or disclose PHI in excess of the minimum necessary PHI as determined by the Privacy Officer.

J. The Privacy Officer is responsible for monitoring the individuals listed in sections II.D and II.E to confirm that access to the Grateful Patient Database and Ali CRM Database continues to be warranted

Schedule A

Roster of Workforce Members with Access to Grateful Patient Database

I. Nebraska Medicine Development Staff

a. Amy Volk, Chief Development Officer, Nebraska Medicine
b. Lisa Anibal, Director, Philanthropic Programs, Nebraska Medicine
c. Edwin Lyons, Director of Development, Nebraska Medicine
d. Matt Pohren, Director of Development, Nebraska Medicine
e. Meghan Perrin, Director of Development, Nebraska Medicine
f. Tom Thompson, Senior Director of Development, UNMC
g. Ashley Christiansen, Director of Development, UNMC
h. Cindy Meschede, Administrative Assistant, Nebraska Medicine

II. Research, Reporting and Analytics

a. Lane White, Director II, Prospect Information Management
b. Jessie Rader, Director II, Advancement Records and Research
c. Stephanie Krebs, Director of Data Acquisition & Integrity

III. Information Technology Department

a. Ben Storck, Assistant Vice President, Advancement and Security Officer
b. Cameron Oelke, Senior Software Developer
c. Alan Hald, Software Support Specialist
d. Barb Scholz, Software Developer II
e. Roxanne Paulsen, Software Developer
f. Terry Benes, Sr. Director Network Technology
g. Kaj Stauffer, Director Infrastructure Architecture and Security

IV. Privacy Officer

a. Keith Miles

Schedule B

Roster of Workforce Members with Access to ePHI in the Ali CRM Database

The list of Ali CRM users is built as a smart query. Instructions are below.

1. Go to the Analysis functional area, under Information library select Add a smart query instance.
2. In the Name field of the Smart Query Search form type active application users and select the smart query from the results.
3. Type in the date added on or after or leave it blank to see all application users.
4. Click on the Results tab to see the results.
5. Click Export to Excel or CSV with the buttons on the bottom to download the results.
6. No need to set save options and click the Cancel button after the results are downloaded.

DISCLOSING INFORMATION TO SUBCONTRACTOR BUSINESS ASSOCIATES

Effective Date: May 14, 2018

I. Policy

A. Purpose

This policy establishes guidelines for the disclosure of PHI to, and use by, UNF's business associates.

B. Policy Implementation

1. General Rule

A "business associate" is a person or entity that performs certain functions, activities, or services for or on behalf of a Covered Entity that involves the use or disclosure of PHI. UNF provides fundraising services to Nebraska Medicine that involves the use and disclosure of PHI and, therefore, UNF is functioning in the capacity of a business associate to Nebraska Medicine. However, a subcontractor that creates, receives, maintains, or transmits PHI on behalf of a business associate (such as UNF) is also a business associate under the HIPAA Regulations.

If UNF engages a vendor or other subcontractor, and such subcontractor creates, receives, maintains, or transmits PHI (including any Permitted Fundraising Information) on behalf of UNF, the subcontractor is a business associate (referred to as a "Subcontractor BA" in this policy). UNF must enter into a Subcontractor Business Associate Agreement and obtain satisfactory assurance that the Subcontractor BA will appropriately safeguard PHI and ePHI.

Examples of UNF's Subcontractor BAs include:

- Outside vendors that prepare fundraising mailings that include PHI (including Permitted Fundraising Information);
- Outside vendors that prepare personalized event or recognition materials that include PHI (including Permitted Fundraising Information);
- Wealth screening companies that evaluate PHI (such as Permitted Fundraising Information) created, received or maintained by UNF for purposes of designing fundraising solicitations, events or programs;
- Software or technology vendors that maintain ePHI (including electronic Permitted Fundraising Information) for UNF; and
- Outside vendors (i.e., not workforce members) that perform services to UNF and have access to ePHI in the Ali CRM or Grateful Patient Databases.

2. **Determining Who is a Business Associate**

   UNF will determine whether or not an entity/vendor is a Subcontractor BA through the following two primary questions:

   a. Is there a contractual or other business or services relationship (written or verbal) in place under which the entity/vendor performs services or activities on behalf of UNF (e.g., legal, actuarial, accounting, management, financial, administrative, or other business services)?

   b. Does UNF need to supply the entity/vendor with PHI/ePHI or access to (or otherwise facilitate access to) PHI/ePHI in order for the entity/vendor to perform its service or activity on behalf of UNF?

   If the answer to both questions is "Yes", the entity/vendor is a Subcontractor BA of UNF. There are some exceptions to this general rule. For example, members of UNF's workforce are not Subcontractor BAs. The UNF Privacy Officer is responsible for making all determinations as to subcontractor business associate status in accordance with the HIPAA Regulations.

3. **Business Associate Agreement with Nebraska Medicine**

   UNF has entered into a Business Associate Agreement with Nebraska Medicine that complies with the HIPAA Regulations. This business associate agreement is set forth as part of the **Fundraising Affiliation & Services Agreement** (and is hereinafter referred to as the "**UNF/Nebraska Medicine BAA**").

4. **Subcontractor Business Associate Agreements**

   UNF will enter into written agreements with its Subcontractor BAs to ensure and document that the Subcontractor BA will appropriately safeguard PHI/ePHI received from (or created on behalf of) UNF. UNF will use the **Template Subcontractor Business Associate Agreement** when possible and will use the **Business Associate Agreement Checklist** when reviewing other template agreements.

   If UNF becomes aware of a pattern of activity or practice of the Subcontractor BA that constitutes a material breach or violation of the Subcontractor BA's obligation under the contract or other arrangement, UNF will take reasonable steps to provide an opportunity for the Subcontractor BA to cure the breach or end the violation, as applicable. If the steps taken to cure the breach or end the violation are unsuccessful, UNF will terminate the contract, if feasible.

5. **Requirements for Subcontractor Business Associate Agreements**

A Subcontractor Business Associate Agreement between UNF and its Subcontractor BAs *must comply with the* **UNF/Nebraska Medicine BAA**. Generally, the Subcontractor Business Associate Agreement between UNF and a Subcontractor BA must:

a. Comply with the **UNF/Nebraska Medicine BAA**. UNF must ensure that its Subcontractor business associate agreements do not give the Subcontractor BA the ability to use or disclose PHI that is more extensive than what Nebraska Medicine has given to UNF in the **UNF/Nebraska Medicine BAA**. Note, however, that UNF can give the Subcontractor BA rights to use/disclose PHI that are not as extensive as UNF has under the **UNF/Nebraska Medicine BAA** or make the Subcontractor BA subject to restrictions that are more stringent than those which apply to UNF.

b. Establish the permitted and required uses and disclosures of PHI by the Subcontractor BA. The agreement may not authorize the Subcontractor BA to use or further disclose the PHI in a manner that would violate the HIPAA Regulations or these policies if the use or disclosure was done by UNF. However, the agreement may permit the Subcontractor BA to use and disclose PHI for the proper management and administration of the Subcontractor BA.

c. Provide that the Subcontractor BA will not use or further disclose the PHI other than as permitted or required by the contract or as required by law;

d. Provide that the Subcontractor BA will use appropriate safeguards and comply, where applicable, with the HIPAA Regulations provisions pertaining to ePHI, to prevent use or disclosure of ePHI other than as provided for by its contract;

e. Provide that the Subcontractor BA will report to UNF any use or disclosure of the PHI not provided for by its contract, whenever it becomes aware of such unauthorized use or disclosure, including breaches of unsecured PHI;

f. Provide that the Subcontractor BA will ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Subcontractor BA will agree to the same restrictions and conditions that apply to the Subcontractor BA with respect to the PHI;

g. Provide individuals access to PHI in accordance with these policies and the HIPAA Regulations;

h. Provide individuals the right to amend PHI in accordance with these policies and the HIPAA Regulations;

i. Provide individuals the right to an accounting of disclosures of PHI in accordance with these policies and the HIPAA Regulations;

j. Provide that to the extent the Subcontractor BA is to carry out UNF's and/or Nebraska Medicine's obligations under the HIPAA Regulations, the Subcontractor BA will comply with the requirements that apply to UNF and/or Nebraska Medicine;

k. Require the Subcontractor BA to make its internal practices, books, and records relating to the use and disclosure of PHI received from UNF (or created or received by the Subcontractor BA on behalf of UNF) available to the Secretary of Health and Human Services for purposes of determining UNF's compliance with the HIPAA Regulations;

l. Requires the Subcontractor BA to report to UNF any security incident of which it becomes aware, including breaches of unsecured PHI;

m. At termination of the agreement, if feasible, return or destroy all PHI received from UNF (or created or received by the Subcontractor BA on behalf of UNF) that the Subcontractor BA maintains in any form (including copies of such information). If the return or destruction of the PHI is not feasible, the Subcontractor BA must extend the protections of the contract to the information and limit further uses and disclosures of the PHI to those purposes that make the return or destruction of the information infeasible; and

n. Authorize termination of the contract by UNF, if UNF determines that the Subcontractor BA has violated a material term of the contract.

When entering into arrangements with business associates, UNF will use the **Template Subcontractor Business Associate Agreement** to the extent possible.

6. **Documentation Regarding a Business Associate Agreement**

UNF will document and retain its subcontractor business associate agreements in written or electronic form for at least six (6) years from the date when the business associate agreement was last in effect.

II. Procedure

A. UNF workforce members must contact the Privacy Officer a minimum of two (2) weeks prior to engaging an outside entity/vendor to ensure UNF has adequate time to determine whether such entity/vendor is a Subcontractor BA and, if so, execute a written agreement in accordance with this policy.

B. The Privacy Officer is responsible for making determinations regarding subcontractor business associate status and for entering into written agreements that comply with the HIPAA Regulations and this policy.

C. If an entity/vendor is a subcontractor business associate of UNF, the Privacy Officer will ensure that the parties enter into a subcontractor business associate agreement that complies with the HIPAA Regulations and the **UNF/Nebraska Medicine BAA**. The Privacy Officer will use the **Template Subcontractor Business Associate Agreement** to the extent possible.

D. If the entity/vendor insists on using a different subcontractor business associate agreement, the Privacy Officer will use the **Business Associate Agreement Checklist** and the **UNF/Nebraska Medicine BAA** to ensure that the form complies with the HIPAA Regulations.

E. UNF will only disclose PHI to a Subcontractor BA in accordance with this policy and the written agreements.

RESPONDING TO INDIVIDUALS' REQUESTS FOR ACCESS TO THEIR DATA

Effective Date: May 14, 2018

I. Policy

A. Purpose

This policy establishes guidelines to be followed by UNF's workforce members when an Individual has requested access to their PHI.

B. General Rule

Subject to limited exceptions, HIPAA requires that Individuals be provided the right to access PHI maintained about the Individual in a "Designated Record Set". This right enables the Individual to inspect and obtain a copy of this information. UNF, as Nebraska Medicine's Business Associate, will support Nebraska Medicine in responding to these requests. The UNF Privacy Officer is the responsible party for receiving and processing requests for an Individual to access his/her own PHI at UNF.

C. Nebraska Medicine Requests for Access

Individuals may submit requests for access directly to Nebraska Medicine. Pursuant to the **Fundraising Affiliation & Services Agreement**, UNF will follow Nebraska Medicine's direction with regards to an Individual's request for access. If Nebraska Medicine concludes that an Individual is entitled to access PHI that is held by UNF, Nebraska Medicine will communicate the decision to UNF and UNF will provide access in the same manner as would be required of Nebraska Medicine.

D. Individual Requests for Access to PHI

If the request comes directly to UNF from the Individual, UNF's Privacy Officer will provide notice of the request to Nebraska Medicine within five (5) business days, as set forth in the **Fundraising Affiliation & Services Agreement**.

E. Documentation

UNF shall, for a minimum of six (6) years, maintain the following:

1. The PHI that is the subject to access by Individuals;
2. A copy of the access request and any related records; and
3. The titles of the persons or offices responsible for receiving and processing the request for access.

II. Procedure

A. UNF workforce members must notify the Privacy Officer of any requests to access PHI.

B. The Privacy Officer will comply with this policy when responding to such request for access.

ACCOUNTING FOR DISCLOSURES OF PHI—TRACKING DISCLOSURES AND RESPONDING TO REQUESTS BY INDIVIDUALS

Effective Date: May 14, 2018

I. Policy:

F. Purpose

This policy establishes guidelines to be followed by UNF to account for certain disclosures of PHI for which an "accounting of disclosures" is required under HIPAA. UNF workforce members must follow these guidelines when Individuals request an accounting of disclosures of PHI that UNF has made about them.

G. Tracking Disclosures

UNF will document disclosures of PHI and information related to such disclosures as would be required for Nebraska Medicine to fulfill its obligations under the Privacy Rule. The following chart summarizes the disclosures UNF is required to document and the exceptions to the documentations requirement:

Required to be Tracked and Included in Accounting **Disclosures:**	**EXCEPTIONS:** **NOT required to be Included in Accounting** **Disclosures:**
Required by law (*e.g.*, mandated reporting under state law)	Made based on the Individual's written Authorization
In response to a subpoena or discovery request	As part of a Limited Data Set, or information that has been de-identified
In response to a court order	To the Individual
To the Secretary of the federal Department of Health & Human Services	For treatment
For health oversight activities (*e.g.*, licensure actions)	Incidental to permitted disclosures
For public health activities/reporting	For healthcare operations, which includes fundraising on behalf of Nebraska Medicine that occurs in accordance with this Manual
About victims of abuse, neglect or domestic violence (except reporting under the VA Act)	To persons (e.g., family) involved in the Individual's care
For law enforcement	For national security or intelligence purposes
To a medical examiner or funeral director, or for cadaver organ donations	To Law Enforcement Officials or correctional institutions about an inmate or other individual in legal custody
For Research (under an IRB waiver)	For payment
To avert a serious threat to health or safety	Made more than six (6) years prior to the date of the request

Required to be Tracked and Included in Accounting **Disclosures:**	**EXCEPTIONS:** **NOT required to be Included in Accounting** **Disclosures:**
Certain specialized government functions (e.g., regarding armed forces personnel)	
For workers' compensation	
A disclosure not permitted by law, such as a Breach of Unsecured PHI (as defined in the **UNF Breach Policy**)	
Any other disclosures not on the list of **EXCEPTIONS**	

The accounting must include the following for each disclosure:

1. The name of the entity or person who received PHI and, if known, the address of such entity or person;

2. A brief description of the PHI disclosed;

3. A brief statement of the purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure if any; and

4. The date of the disclosure.

H. **Nebraska Medicine Request for an Accounting of Disclosures of PHI**

Upon request from Nebraska Medicine, the Privacy Officer will make available the information necessary to provide an accounting of disclosures of PHI made by UNF, in accordance with the **Fundraising Affiliation & Services Agreement**.

I. **Individual Requests for an Accounting of Disclosures of PHI**

HIPAA requires that organizations provide Individuals requesting it an accounting of disclosures of his/her PHI. In the event an Individual submits a request for such an accounting directly to UNF, UNF's Privacy Officer will notify Nebraska Medicine within five (5) business days and will follow Nebraska Medicine's direction with respect to such request.

J. **Documentation**

UNF shall, for a minimum of six (6) years, maintain the following:

1. The information required to be included in the accounting;

2. The written accounting that is provided at the direction of Nebraska Medicine, if any; and

3. The titles of the persons or offices responsible for receiving and processing the request for access.

II. Procedure:

UNF will follow this policy as its procedure on accounting of disclosures. All documentation will be kept in the file (of the Individual at issue) for a minimum of six (6) years.

RESPONDING TO INDIVIDUALS' REQUEST TO AMEND PHI OR RECORDS

Effective Date: May 14, 2018

I. Policy

A. Purpose

This policy establishes guidelines to be followed by UNF's workforce members when an Individual has requested to amend their PHI or record.

B. General Rule

HIPAA requires that Individuals be provided the right to request an amendment to PHI or records maintained about the Individual in a "Designated Record Set." A Designated Record Set is a group of records maintained by or for Nebraska Medicine that is:

1. Medical records and billing records about individuals maintained by or for Nebraska; or

2. Records used, in whole or in part, by Nebraska Medicine to make a decision about an individual.

UNF, as Nebraska Medicine's Business Associate, will support Nebraska Medicine in responding to these requests. The UNF Privacy Officer is the responsible party for receiving and processing requests for an Individual to amend his/her own PHI or record at UNF.

C. Nebraska Medicine Requests for Amendments to PHI or Records

Individuals may submit requests for amendments directly to Nebraska Medicine. Pursuant to the **Fundraising Affiliation & Services Agreement**, UNF will follow Nebraska Medicine's direction with regards to an Individual's request for amendment. Nebraska Medicine will determine whether any Individual is entitled to amend his or her PHI or record in accordance with 45 C.F.R. § 164.526. If Nebraska Medicine concludes that an Individual is entitled to amend his or her PHI, and such PHI is both in a Designated Record Set and is under the control of UNF, Nebraska Medicine will communicate the decision to UNF and UNF will provide an opportunity to amend the PHI in the same manner as would be required of Nebraska Medicine under 45 C.F.R. § 164.526.

D. Individual Requests for Amendments to PHI or Records

If the request comes directly to UNF from the Individual, UNF's Privacy Officer will provide notice of the request to Nebraska Medicine within five (5) business days, as set forth in the **Fundraising Affiliation & Services Agreement**.

E. **Documentation**

UNF shall, for a minimum of six (6) years, maintain the titles of the persons or offices responsible for receiving and processing the request for amendments, and all documentation related to investigating and responding to such request.

II. Procedure

A. UNF workforce members must notify the Privacy Officer of any requests to amend PHI.

B. The Privacy Officer will comply with this policy when responding to such requests for amendments.