Nebraska Medicine **POLICIES AND PROCEDURES MANUAL** ☒ System ☐ Department **Supersedes: BMC-HIM 02.014**	Section: INFORMATION MANAGEMENT (IM) Subject: Privacy, Confidentiality & Security of Patient and Proprietary Information Number: IM06 Attachments: Date Effective: 09/01/00 Date Reviewed: 09/02/03, 10/12/04, 07/31/08, 8/4/10, 07/12/12, 5/19/14, 11/6/14, 6/6/2016

PRIVACY, CONFIDENTIALITY, & SECURITY OF PATIENT & PROPRIETARY INFORMATION

PURPOSE:
To maintain the privacy, confidentiality and security of patient and proprietary information and comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Nebraska Medicine, which includes The Nebraska Medical Center, Bellevue Medical Center, and UNMC Physicians (Organization) workforce and business associates have access to individually identifiable health information (protected health information) and proprietary information. For purposes of this policy, confidential information means protected health information and proprietary information.

POLICY:
It is the policy of Nebraska Medicine to maintain strict confidentiality and security of protected health information and proprietary information.

DEFINITIONS: (as defined by HIPAA 45 CFR 164.501)

1. Business Associate means a third party who performs services on behalf of Nebraska Medicine and has access to protected health information (PHI) when performing services; or provides one of the following services for Nebraska Medicine involving access to PHI: claims processing, data analysis, data processing, practice management, utilization review, quality assurance, billing, benefit management, and repricing.
2. Designated record set is the medical record and billing record.
3. Individual means the person who is the subject of the protected health information (including Nebraska Medicine employees who are patients).
4. Information Security is the ability to control access and protect information from unauthorized alteration, destruction, loss or accidental or intentional disclosure to unauthorized persons.
5. Protected health information (PHI) is individually identifiable health information. Health information means any information, whether oral or recorded in any medium that:
   a. is created or received by Nebraska Medicine; and
   b. relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.
6. Proprietary Information is information relating to business practices, including but not limited to financial statements, contracts, and business plans; employee records; and meeting minutes.
7. Workforce means employees, the medical staff, volunteers, trainees, and other persons whose conduct, in the performance of work for Nebraska Medicine is under the direct control of Nebraska Medicine, whether or not they are paid by Nebraska Medicine.

PROCEDURES:

1. Records containing confidential information, in any form, are the property of Nebraska Medicine. The original medical record in any form shall not be released except in response to a valid search warrant, subpoena, or court order requiring the release of the original record. A copy of the medical record should be offered first in such circumstances. If the original medical record must be released, a copy should be made prior to release if possible.

2. Individuals have the following rights with respect to their PHI:
   a. Right to request access and obtain copies of their designated record set within a reasonable amount of time

and to request amendment (see Access and Amendment policy):
b. Right to request restrictions of how their PHI is used and disclosed (see Use & Disclosure of PHI policy);
c. Right to request an accounting of disclosures (see Accounting of Disclosures policy);
d. Right to receive a Notice of Privacy Practices (see Notice of Privacy Practices policy);
e. Right to file a complaint internally with the Patient Relations Department or with the U.S. Department of Health and Human Services Office for Civil Rights (see Notice of Privacy Practices policy and Patient/Consumer Complaints policy).

Individuals shall not be asked to waive these rights as a condition of receiving treatment.

3. Nebraska Medicine is responsible for safeguarding and protecting confidential information against loss, tampering, and disclosure to unauthorized individuals. The safeguarding of confidential information in any form includes when the information is stored and/or being transferred outside the facility (see Transporting Protected Health Information policy).

4. Nebraska Medicine workforce has a duty to protect confidential information. Breach of this duty includes the following:
   a. Accessing confidential information, in any form, without a "need to know" to perform assigned duties. Workforce members with medical information system access may view their own individual medical records. Workforce members may not print copies of their own records nor access records of family members (including children), relatives, friends and others, unless access is necessary to perform assigned duties. Workforce members may obtain a copy of their medical records from the Health Information Management Department.
   b. Discussing or disclosing patient care events to individuals who do not have a “need to know” to perform assigned duties, even if the patient’s name is not mentioned. The facts surrounding patient care are confidential and can lead to the identity of the patient.
   c. Disclosing confidential information without proper authorization (see Use & Disclosure of Protected Health Information policy);
   d. Accessing patient information via Health Information Exchange in a manner or for a purpose not permitted (see Use & Disclosure of Protected Health Information policy);
   e. Discussing confidential information in the presence of individuals who do not have the "need to know" to perform assigned duties;
   f. Disclosing that a patient is receiving care (except for authorized directory purposes);
   g. Leaving confidential information unattended in a non-secure area;
   h. Improper disposal of confidential information;
   i. Using another person's user ID, password, or other security codes;
   i. Assisting an unauthorized user to gain access to a secured information system;
   k. Transferring confidential information in any form without both parties having a need to know.

5. Nebraska Medicine shall reasonably mitigate or reduce any harmful effects that may result from privacy breaches.

6. All employees, the medical staff, allied health practitioners and members of the workforce with access to confidential information shall sign Nebraska Medicine Information Privacy, Confidentiality and Security Agreement upon initial employment/work/appointment / credentialing (see attachment at the end of the policy).

7. Workforce members who suspect a privacy or information security violation must report it immediately to their respective manager and the Privacy and/or Information Security Office. A full investigation of the suspected violation shall be conducted. Staff who wish to remain anonymous may report the suspected violation to the Compliance Hotline at 800-822-8310. Sanctions shall be imposed for substantiated breaches or failure to report suspected violations. The Medical Staff and allied health practitioners shall report suspected violations to the System Chief Medical Officer.

8. Sanctions for violations of privacy or information security may include revocation of medical staff privileges, allied health credentials, or employee corrective action up to and including termination of employment (see Confidentiality policy and Corrective Action policy). Civil and criminal fines and penalties can also be levied under

HIPAA.

9. Workforce members may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for reporting a suspected privacy or information security violation, or for filing of a complaint within the organization or to the Office for Civil Rights.
10. Access to patient information via Health Information Exchange shall be conducted in accordance with “Uses and Disclosure of Protected Health Information” policy.
11. Paper medical records shall be maintained in the Health Information Management Department.
    a. Records sent to clinic areas shall be returned to the Health Information Management Department within one working day.
    b. Records of discharged patients will remain on the units until Health Information Management picks them up. Medical records of deceased patients scheduled for an autopsy may be sent to the morgue.
    c. Records signed out to the attending physician's office or other authorized areas shall be returned to the Health Information Management Department as soon as possible (preferably by 5:00 pm each working day).
12. Editing, authenticating and correcting the medical record.
    a. Please reference, Contents of the Medical Record policy for editing and authenticating the medical record.
13. Business Associate agreements/addenda shall be established with any individual or corporation who performs a function on behalf of Nebraska Medicine involving the use or disclosure of PHI, other than as a member of the workforce or a healthcare provider providing treatment (see Contract Management policy).
14. Human Subjects Research shall be conducted in accordance with UNMC Human Research Protection Program (HRPP) Policies and Procedures, including HRPP Policy 3.4, “Use of Protected Health Information in Research and Registries” and Use and Disclosure of Protected Health Information policy.
15. Retention of the designated record set and other protected health information shall be in accordance with federal, state, and local laws, and regulatory association guidelines. Documents required to demonstrate HIPAA compliance shall be retained for a period of six years.
16. The Privacy Officer shall be designated in writing and shall be responsible for developing and implementing written policies and procedures necessary to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
17. All members of the workforce shall receive training on privacy and security of confidential information upon hire, and when policies and procedures relevant to their position change.

STAFF ACCOUNTABILITY:
Director, Health Information Management
Privacy Officer

PLEASE SCROLL DOWN TO THE NEXT PAGE TO SEE THE ATTACHMENT.

NEBRASKA MEDICAL CENTER
INFORMATION PRIVACY, CONFIDENTIALITY AND SECURITY AGREEMENT

Patient and proprietary information is confidential. Medical staff, allied health professionals, employees, students, and volunteers of Nebraska Medical Center must maintain the privacy and security of all patient and proprietary information in any form, including written information, electronic information, and verbal communication.

CONFIDENTIALITY AGREEMENT

1. I will comply with Policy, “Privacy, Confidentiality & Security of Patient & Proprietary Information” which I have read and understand.
2. I will comply with Policy, "Computer Use and Electronic Information Security Policy" which I have read and understand.
3. I will access, use and share patient and proprietary information with others on an authorized “need to know” basis only to perform assigned duties.
4. I will not discuss confidential information in the presence of individuals who do not have a “need to know”.
5. I understand that audits of information are conducted to verify information is being accessed by authorized individuals only.
6. I will immediately report suspected privacy and information security violations to my department manager, the Privacy and/or Information Security Office, the Human Resources Department, or the Compliance Hotline.
7. I understand that violation of this confidentiality agreement may result in corrective action up to and including termination of employment, as well as possible fines and/or civil or criminal penalties under state or federal law.

_____	_____	_____
Signature	Department	Date

COMPUTER ACCESS SECURITY AGREEMENT

I may be assigned a computer identification number and instructed to develop personal passwords. To maintain confidentiality of information maintained electronically, I understand that:

1. Authorization from my department manager is required to gain access to specific computer functions necessary to perform my assigned duties.
2. My computer user IDs and passwords will be memorized and not shared with anyone, at any time, for any reason, except in cases necessary to facilitate computer maintenance and repairs.
3. I will not leave a terminal without first closing any computerized application containing confidential information.
4. I will contact my department manager immediately if I discover my user ID has been revealed and I need a new one.
5. I understand that Organization information must be stored only on Organization computer network drives or an encrypted local computer drive.
6. If I use a portable device containing Organization information, the device must be both password protected and encrypted.
7. I understand that improper use of my computer user ID or password may result in corrective action up to and including termination of employment.

_____	_____	_____
Signature	Department	Date

Department Approval		Administrative Approval	
Signed | s |:	Jana Danielson	Signed | s |:	Harris Frankel, MD
Title:	Executive Director	Title:	System Chief Medical Officer
Department:	Revenue Cycle		