SUBJECT:	Confidentiality of Patient Records (HIPAA)
REVIEWED/REVISED:	9/2015; 2/2022
PURPOSE:	Protect the privacy of protected health information (PHI) in compliance with applicable laws and regulations.
POLICY OWNER:	Vice President of Institutional Effectiveness

POLICY:

Nebraska Methodist College is committed to protecting the privacy of protected health information (PHI) in compliance with all applicable laws and regulations. To achieve this end, the College, an affiliate of Methodist Health System, has adopted policies and procedures to protect the privacy, and provide for the security of PHI. Students who have access to PHI in the course of their programs are required to maintain the confidentiality of any and all PHI they have been appropriately granted authorization to use and view.

Students with access to PHI must respect their patient's rights to privacy and understand and adhere to their clinical site's privacy policies. When using or disclosing PHI, or when requesting PHI from others, students must make reasonable efforts to limit the information to the minimum necessary to accomplish the educational purpose of the use, disclosure, or request. Students must remove any patient identifiers before transporting, disclosing, or transmitting any document or assignment. (See below for steps to remove patient identifiers).

Students who access PHI are responsible for protecting and safeguarding it and to properly dispose (i.e., shred) of any notes, e-mails, thumb drives, CD-ROMs, Care Plans, and any other device or medium that contains PHI. Because of the risk of loss or theft of mobile devices, PHI should never be stored on or transferred to mobile devices unless specific approval is given and the mobile device contains the appropriate safeguards.
Students are also prohibited from disclosing any PHI on social media. Social media include, but are not limited to, collaborative projects (e.g, Wikipedia), blogs and microblogs (e.g., Twitter), content communities (e.g., YouTube), social networking sites (e.g., Facebook).

Failure to abide by the College's HIPAA Privacy Policy, and any other Methodist Health System HIPAA policy, may result in the suspension or dismissal from the College and/or legal action brought against the student.

Removing/De-identifying Protected Health Information (PHI)

Protected Health Information (PHI): Information in any format that identifies the individual, including demographic information collected from an individual that can reasonably be used to identify the individual. Additionally, PHI is information created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual.

De-identified: Information that has certain identifiers (see "identifiers" below) MUST be removed so that it is no longer considered Protected Health Information.

Identifiers: Under the HIPAA Privacy Rule "identifiers" include the following:

1. Names (e.g. patient initials (do not reverse order))
2. Geographic subdivisions smaller than a state (except the first three digits of a zip code if the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000).
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, and date of death and all ages over 89 and all elements of dates (including year) indicative of such age (except that such ages and elements may be aggregated into a single category of age 90 or older)
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code (excluding a random identifier code for the subject that is not related to or derived from any existing identifier).