CRR: Privacy - Patients

Compliance Risk Areas

Compliance Risk Areas	Related Governing Laws, Rules, Regulations, or University Policies
• Privacy/HIPAA	• Health Insurance Portability and Accountability of 1996, 45 C.F.R. 160 and 164 • HITECH • Minnesota Health Records Act • Administrative Policy: Protected Health Information

General compliance question(s)

1. Are there emerging risks in this area? If yes, please explain.
2. Please estimate the number of allegations of misconduct (violation of law, rule, regulation or University policy) that are received annually related to HIPAA, excluding those allegations filed through the UReport system. Of these, how many allegations are substantiated?
3. How is compliance with HIPAA monitored? How frequently does the monitoring occur?
4. What are the typical noncompliance issues found and how are they corrected?
5. How is compliance in this area reported to senior leadership, and how frequently?

Cost of Compliance Questions

1. How many full-time employees (FTEs) are dedicated to compliance-related activities in this area?
2. What are the estimated non-FTE costs, related to compliance area, that are borne by

the compliance unit such as systems and outside consulting services?

3. Please list all training required to maintain University compliance in this subject area. For each training requirement:
    a. Identify the primary source of the requirement as (1) federal or state law, (2) administrative regulations, or (3) University policy. (e.g., Conflict of Interest training is required under federal code of federal regulations for investigators conducting research funded by a Public Health Service agency)
    b. Identify category(ies) of employees (e.g., faculty, P&A, etc.) required to take the training
    c. Estimate the number of employees in each category required to take the training
    d. Identify the frequency (e.g., quarterly, annually) and the length of the training (e.g., 1.5 hours).
4. Estimate the number of employees system-wide who are subject to the compliance requirements in this area. Excluding time required to meet training requirements addressed in Question 3 above, please estimate the time required annually for these employees to comply with other compliance requirements.

Hybrid Entity

1. Describe the process for designating which components of the University of Minnesota are health care components covered under HIPAA.
2. Is the following a complete and accurate list of University of Minnesota health care components under HIPAA? If not, please clarify which areas are not health care components or specify the components that have been omitted.
    a. AHC Administrative Shared Services
    b. AHC Centers
    c. AHC Information Services (AHC-IS)
    d. Athletic Training Twin Cities
    e. Boynton Health Service
    f. College of Pharmacy

g. Community-University Health Care Center
h. Disability Resource Center
i. Internal Audit
j. Julia M. Davis Speech Language Hearing Center
k. Medical School (Twin Cities and Duluth campuses)
l. Minnesota Research Data Center
m. Office of General Counsel (OGC)
n. Office of Institutional Compliance (OIC)
o. Office of Information Technology - Security (OIT-Security)
p. Office of Measurement Services (OMS)
q. School of Dentistry and Dental Clinics
r. School of Nursing
s. UPlan
t. UMD Health Services

3. Do you maintain written or electronic documentation of this designation? Where is the documentation maintained?

Administrative Requirements

1. Attach copies of or provide links to the policies and procedures that the University has implemented to comply with the standards, implementation specifications, or other requirements of § 164.530
    a. How often are these policies and procedures reviewed to ensure they continue to comply with changes in the law?
    b. When and how often are changes made to policies and procedures?
    c. When changes are made to the policies and procedures, are those changes documented?
2. Has the University designated a privacy official who is responsible for the development and implementation of the University's privacy program?
    a. Has this personnel designation been documented?

3. Has the University designated a contact person or office who is responsible for receiving privacy complaints and who is able to provide further information about matters covered by the Notice of Privacy Practices?
    a. Has this personnel designations been documented?
    b. How is this personnel designation made known to the public?
4. Describe the training process for workforce members that carry out functions related to PHI.
    a. How does the University identify these workforce members and ensure their training is completed?
    b. How are new workforce members identified to complete the training and when must they complete the training?
    c. Does the University document that the training has been provided to all applicable workforce members?
5. Describe the safeguards that the University has in place to protect against intentional or unintentional use of or disclosure of PHI.
6. Describe the process for individuals to make complaints concerning the University's policies and procedures.
    a. Has the University received and resolved any complaints?
    b. If so, has documentation been kept for the complaints?
7. Describe the sanction process for workforce members that violate the University's policies and procedures.
    a. Has the University sanctioned any workforce members?
    b. If so, has documentation been kept for the sanctions?
8. Describe the process for the University to mitigate any harmful effect of a use or disclosure of PHI in violation of its policies and procedures.
9. Does the University have a policy or procedure in place to ensure that no intimidating or retaliatory acts are made against any individual for the exercise of any of their rights?
10. Does the University ever require individuals to waive their rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits?

Business Associate Agreements

1. Attach a copy of or provide a link to the standard Business Associate Agreement used for vendors that provide services or perform functions or activities on behalf of the University that relate to PHI.
    a. How does the University ensure that vendors do not violate their obligations under the Business Associate Agreement?

Notice of Privacy Practices

1. Attach a copy of or provide a link to the Notice of Privacy Practices.
    a. Does the University elect to limit the uses or disclosures that it is permitted to make under § 164.520?
2. Is there a process in place for revising and distributing the Notice of Privacy Practices?
    a. When did the University last make changes to the Notice of Privacy Practices that required re-distribution of the Notice?
3. Describe the process for distributing the Notice of Privacy Practices provided to all individuals that the University has a direct treatment relationship with.
    a. How does the University verify that all such individuals receive the Notice of Privacy Practices?
    b. Is the Notice of Privacy Practices posted prominently on the University website?
    c. Does the University utilize electronic distribution for individuals?
4. Does the University have a relationship(s) with a separate covered entity, such that a joint Notice of Privacy Practices is used?

Patient Rights

1. Does the University provide individuals the opportunity to restrict the uses or disclosure of PHI to carry out treatment, payment, or health care operations?

a. Describe the process, if applicable, that the University uses to review and grant such requests.

2. Does the University permit individuals to request communications of PHI by alternative means?
    a. Describe the process for reviewing and granting such requests.
3. Does the University permit individuals to request access of their PHI? Are requests required to be in writing?
    a. Describe the process for reviewing and granting such requests.
        i. Are requests acted on no later than 30 days after receipt of request?
            1. If not, are individuals provided with a written statement of the reasons for delay?
        ii. If requests are denied, are denials made in writing, with the basis of the denial, a statement of the individual's right to review, and a description of the University's complaint procedures?
            1. For denied requests that are appealed by the individual, describe the process of designating a licensed health care professional to the review denied requests.
    b. If the University imposes a reasonable, cost-based fee for requests, describe the process for determining the fee. Is the fee less than the maximum charges permitted under Minnesota State Statute 144.292?
4. Does the University permit individuals to request that their PHI be amended?
    a. Describe the process for reviewing and granting such requests.
        i. Are requests acted on no later than 60 days after receipt of request?
            1. If not, are individuals provided with a written statement of the reasons for delay?
        ii. If requests are granted, describe the process for amending the records and informing others.
        iii. If requests are denied, are denials made in writing, with the basis of the denial, a statement of the individual's right to submit a statement disagreeing with the denial, and a description of the University's complaint procedures?

1. For denied requests, are individuals provided the opportunity to submit a statement disagreeing with the denial and the basis of the disagreement?

5. Does the University permit individuals to request accounting of the disclosures of PHI made by the University in the six years prior to the date of the request?
    a. Describe the process for capturing the information requested by the individual.
    b. Are requests acted on no later than 60 days after receipt of request?
        i. If not, are individuals provided with a written statement of the reasons for delay?
6. For questions 1 through 5 above, how many requests have you received in the past 12 months?

Use and Disclosures of PHI

1. Does the University use PHI for marketing, or sell PHI?
    a. If so, describe the process for getting valid authorization from individuals for the use and disclosure of PHI. If the University uses a standard valid authorization form, attach a copy of the form.
    b. How does the University retain documentation of valid authorizations?
    c. Is the individual provided a copy of the authorization form?
2. Does the University provide an opportunity to object to use of PHI for facility directories, disclosure to family members, and emergency situations?
    a. How does the University document that individuals were given the opportunity to object?
    b. How does the University document any objections from individuals?
3. Describe the process for determining that PHI used in research meets one of the conditions of § 164.512(i).
    a. Where applicable, how does the University document the release of PHI?
4. Describe the process for verifying that de-identified PHI meets the requirements of § 164.514.

Minimum Necessary Standard

1. How does the University determine which workforce members need access to PHI to carry out their duties?
    a. Does the University periodically review these workforce members to determine if they still need access to PHI to carry out their duties?
2. For those workforce members who need access to PHI, describe the reasonable efforts made by the University to limit access to PHI.
3. For routine and recurring disclosures of PHI, describe the process for limiting the disclosure to the amount reasonably necessary to achieve the purpose of the disclosure.
4. For disclosures made on an individual process, describe the criteria to limit the disclosure of PHI to the amount reasonably necessary to achieve the purpose of the disclosure.
5. Does the University have a standard Data Use Agreement for use of limited data sets? If so, attach the Agreement.
    a. How does the University ensure that data set recipients do not violate their obligations under the Data Use Agreement?
6. Does the University use or disclose PHI for fundraising communications? If so:
    a. With each fundraising communication, is an individual given a clear and conspicuous opportunity to elect not to receive any further fundraising communications?
    b. Is an individual's treatment ever conditional with respect to individual's decision on receipt of fundraising communications?
    c. How does the University ensure that those individuals who have opted out of fundraising communications no longer receive such communications?
7. For all of the above disclosures of PHI, describe how the University verifies the identity of the person requesting PHI and whether the individual has the authority to access the PHI.

Breaches

1. Describe the process for identifying when a HIPAA breach has occurred.
2. Describe the process for notifying individuals and HHS when a HIPAA breach has occurred.
    a. Are notifications made to individuals within 60 days of all breaches?
    b. Has the University identified any breaches in the past six years?
    c. Has the University had any breaches of more than 500 individuals' PHI in the last six years? If so, was the media notified?
    d. Have any business associates notified the University of breaches within the last six years?
3. Does the University have a HIPAA breach response plan in place for handling HIPAA breaches?

Miscellaneous

1. Describe any other areas or processes that may warrant further assessment and potential adjustment.