

Guidance: Use of Protected Health Information in Publications

Use of Protected Health Information (PHI) in Publications

Publishing clinical results, departmental activities, and the University of Chicago Medicine (UCM) advancements in educational/medical literature, newsletters, and other types of publications is fundamental to the UCM mission. However, it is important that we use and disclose protected health information (PHI) for these purposes in compliance with the HIPAA regulation. This guidance applies to publications that are distributed both inside and outside UCM.

The HIPAA Privacy Rule allows physicians and staff to use and disclose PHI without a patient's written authorization only for purposes related to treatment, payment, and health care operations. The use of PHI in publications (e.g. medical articles, annual reports, newsletters, quality posters, and written case studies, etc.) does not fall under the purposes of treatment, payment or health care operations, therefore a patient written authorization is required.

UCM physicians and staff who want to include PHI in publications may do so, but must obtain patient written authorization. Only the PHI that the patient agrees may be used and that is reflected on the authorization form can be used and disclosed. Students who want to use patient PHI in the coursework will also need patient written authorization.

UCM physicians and staff should not search UCM databases or applications (e.g. Epic) to search or "data mine" for interesting patient cases to use in publications.

Patient PHI is health information relates to the past, present, or future physical or mental health or condition of an individual and can be used to identify the individual. In general PHI includes the following and must be protected under HIPAA:

1. Names;
2. All geographical subdivisions smaller than a State:
4. Phone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social Security numbers;
8. Medical record numbers;

Guidance: Use of Protected Health Information in Publications

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; and
18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)

Patient information that has been completely de-identified according to Policy [A05-22 Use and Disclosure of Limited Data Set and De-identified Health Information](#) by ensuring all 18 PHI identifiers listed above are removed is no longer subject to the HIPAA regulation and can be used in publications.

Any questions/comments/concerns please feel free to reach out to the Privacy Program at:

773-834-9716 or hpo@bsd.uchicago.edu