Guidance on Patient Privacy and the Publication or Dissemination of Case Reports

Q. What constitutes a case report?

A. A case report is an unsystematic clinical observation that states the outcome or response of a single patient to a diagnostic strategy or treatment. Case reports serve to document and share novel cases amongst the medical community for educational purposes.

Q. Is IRB approval required to prepare a clinical case study?

A. Generally, case studies are not reviewed by the IRB. Case studies do not meet the Common Rule definition of research because it is not a systematic investigation designed to develop or contribute to generalizable knowledge[1]. As case reports, by definition, have a very limited sample size, they are not designed to be predictive of similar circumstances and hence do not meet the generalizable requirement of this definition and therefore are not subject to IRB review.

Q. Are there other approval requirements needed for case studies?

B. Even though case reports generally are not regulated as research, patient data is protected under HIPAA and users must comply with the HIPAA Privacy Rule when using or disclosing protected health information (PHI)[2] as part of a case report. HIPAA compliant use or disclosure of a case report for purposes other than treatment, payment, or healthcare operations[3] requires either: (1) obtaining written authorization of the patient[4] or the patient's legal representative; or (2) de-identifying the PHI. Note that a waiver of authorization, issued by either an IRB or a Privacy Board, is not a mechanism that can be used for case reports, as HIPAA limits waivers to uses and disclosures that meet the definition of research; as described above, case reports do not meet the definition of "research."

Q. When is patient authorization required?

A. When case reports describe or discuss unique or rare circumstances, as they often do, it may be difficult or impossible to de-identify those cases such that there is no reasonable expectation that the individuals included can be identified, so patient authorization generally would be required.

---

[1] Research is defined at 45 CFR 164.501 as "a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge."

[2] Individually identifiable information held or transmitted by a covered entity or its business associate, in any form or medium, which relates to: (1) the individual's past, present, or future physical or mental health or condition, (2) the provision of health care to the individual, or (3) the past, present, or future payment for the provision of health care to the individual. See 45 CFR 164.501

[3] This guidance is not intended to discuss case reports or presentations for healthcare operations purposes such as education of the covered entity's own workforce or quality improvement purposes. Workforce members presenting individual patient cases for health care operations purposes should be mindful to use or share only the minimum necessary PHI for the purpose.

[4] For purposes of this Guidance, references to "patient" also include "research participant," as applicable.

Q. What is the process when patient authorization cannot be obtained?

A. The following questions may be helpful for determining whether it is appropriate to proceed with a case report when written authorization has not been or cannot practically be obtained, such as when the patient is deceased, and patient's representative is not known, and de-identification is not possible.

- How many other cases with the same or highly similar circumstances have there been at Yale in the last year?
- In your professional judgment, do you believe the case report can be written in such a way that the combination of the remaining details likely could not be used to uniquely identify the patient by itself or in combination with other information known to a reader? You may wish to consider whether information such as age, gender, diagnosis, or other details, and the fact that the patient likely received care from the author or at a location where the author worked, can lead to identifying the subject.
- If the patient's family member or friend happened to read the anticipated content of the case report, do you believe they would likely identify the patient? Note – the ability for a patient to self-identify is not a concern, but you may wish to consider whether a close family member or friend's ability to identify the subject could lead to them learning information not already known to them.
- If the patient is reportedly lost to follow up, have all reasonable efforts to obtain patient authorization been exhausted? Unsuccessful attempts to get authorization or similar activities such as attempts to locate and contact the patient should be well documented, and all reasonable efforts to obtain patient authorization should be exhausted.
- If the patient is deceased -- Do you know if the patient has a personal representative or other individual with legal authority to act on his behalf whom you could ask to sign an authorization?
- If the patient is deceased -- If this patient were still alive, would you feel comfortable asking for his authorization for the case report? If no, why not?
- If the patient is deceased - Did this patient express any sensitivities or preferences on confidentiality or using his case for educational or research purposes that you are aware of?

Q. What are the options for de-identifying a patient?

A. It is important to understand that determining whether data are de-identified under HIPAA is a more restrictive determination than determining whether private information is individually identifiable under the Common Rule. The HIPAA rule considers PHI as any information that may identify an individual; was created or received by a member of a HIPAA covered entity; and relates to the individual's past, present, or future physical/mental health or condition, health care, or payment for health care. HIPAA recognizes two methods for de-identification of data.

Option 1: Safe Harbor De-identification[5]

PHI includes any of the following 18 identifiers of the patient or of his/her relatives, employers, or household members, all of which must be removed to de-identify the data. This is known as safe harbor de-identification.

1. Name
2. Address (all geographic subdivisions smaller than a state, including street address, city, county and zip code)

[5] 45 CFR 164.514(b)(2)(i)

3. All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, 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. Email 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
16. Biometric identifiers, including fingerprints and voiceprints
17. Photographic images – including full facial photographs and other comparable images
18. Any other unique identifying number, characteristic, or code that could identify an individual.

The Office for Civil Rights published guidance on de-identification[6] and provides details regarding a "safe harbor" approach to de-identification. The safe harbor approach of removing all of the 18 identifiers above from a data set to render it de-identified is only adequate if there is no reasonable basis to believe that an unauthorized person could use the remaining information alone or in combination with other information to identify the patient.

The OCR provides specific guidance regarding de-identification of dates, age, and zip code as follows[7]:

Dates:

- Elements of dates that are *not permitted* for disclosure include the day, month, and any other information that is more specific than the year of an event. For instance, the date "January 1, 2009," could not be reported at this level of detail. However, it could be reported in a de-identified data set as "2009."

Age:

- Many records contain dates of service or other events that imply age. Ages that are explicitly stated or implied as over 89 years old must be recoded as 90 or above. For example, if the patient's year of birth is 1910 and the year of healthcare service is reported as 2010, then in the de-identified data set the year of birth should be reported as "on or before 1920." Otherwise, a recipient of the data set would learn that the age of the patient is approximately 100.

Zip Code:

- The first three digits of the ZIP code may be included if, according to the current publicly available data from the Bureau of the Census:

[6] See https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification
[7] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification

(1) The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; or

(2) The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000. This means that the initial three digits of ZIP codes may be included in de-identified information *except* when the ZIP codes contain the initial three digits listed in the Table below. In those cases, the first three digits must be listed as 000.

- 036
- 059
- 063
- 102
- 203
- 556
- 692
- 790
- 821
- 823
- 830
- 831
- 878
- 879
- 884
- 890
- 893

Option 2: Expert Determination[8]

When safe harbor de-identification is not possible or the opportunity to identify the patient exists, even after de-identification, the expert determination method for de-identification can be considered. For purposes of de-identification, an expert is defined as:

A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

1. Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
2. Documents the methods and results of the analysis that justify such determination

For additional information on de-identification under the HIPAA Privacy Rule, see HHS guidance at https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification.

[8] 45 CFR 164.514(b)(1)