Yale University and Yale New Haven Health System
Joint Health Data Governance Council
Guidance on Requests to Share Health Data with External Entities

Background

Yale University and Yale New Haven Health System jointly create and maintain health information for the purpose of providing clinical care to our patients and conducting research. Patients and research participants entrust their health information to us with the expectation that the information will be used to provide care and associated activities including billing and healthcare operations. As an academic medical center, University and Health System staff may wish to combine information relating to multiple patients into health data sets and allow use of these data sets to advance medical care and innovation through collaborations with research institutions and other parties. Sharing health data requires determining the appropriate balance of patient privacy and public good anticipated from the secondary use of health data and must meet our compliance obligations as well as institutional mission. This guidance describes the University and Health System's requirements for approving disclosure of health information to external entities.

Requests Subject to Council Review

The Joint Health Data Governance Council is charged with review of non-standard requests to share health data. Health data includes traditional medical records including information in the electronic health record and extended patient data such as diagnostic imaging and details of genomic sequencing, as well as billing and clinical research records, irrespective of whether the data is individually identifiable. Non-standard requests for sharing of health data may include, but is not limited to:

- Disclosure to commercial entities that are not our business associates for purposes outside the context of Institutional Review Board approved research
- Disclosure to entities that will not agree to contractual controls prohibiting further use or disclosure of the data outside the research project.
- Disclosures involving remuneration, financial or otherwise, in exchange for de-identified data.
- Disclosures for research under a waiver of authorization where the University or Health System are not considered to be engaged in the research.
- Disclosures not otherwise identified as a standard data use request below.

Review is not required for standard data requests including:

- Uses and disclosures pursuant to patient authorization
- Uses and disclosures for treatment and payment purposes
- Uses and disclosures required for legitimate healthcare operations purposes such as state or federally mandated reporting, to authorized business associates performing services on behalf of the University or Health System, licensing or credentialing activities, etc.

- Research projects conducted by or in collaboration with University or Health System staff which have been approved by the relevant Institutional Review Board and where the data either is to be maintained on University or Health System networks and systems or where release of the data is subject to contractual controls prohibiting further use or disclosure of the data outside the research project.

Review Considerations

Regulatory Compliance: The proposed sharing of health data must comply with all applicable regulatory requirements including, but not limited to, requirements for IRB approval, conflict of interest review, informed consent and authorization required under state, federal or international law or as waived under HIPAA.

Proposed Data Use: Health data may only be shared where doing so is consistent with the academic and health care missions of the University and Health System. Proposals to share health data for projects that do not involve University/Health System employees must articulate how the disclosure will improve patient care or advance biomedical knowledge and respect patient expectations of data privacy.

Sharing health data in exchange for financial or other renumeration is prohibited under HIPAA and precludes provision of identified health data in exchange for payment or reduced fee services. Additionally, sale of data, whether or not identified, is not permitted when it will violate University or Health System status as a non-profit. Proposed uses involving commercial entities will be scrutinized to confirm that the proposed use qualifies as research rather than commercialization.

Research is defined under the Common Rule and HIPAA as "A systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge." Under this definition, projects involving commercial partners are considered allowable research rather than commercialization when:

- University or Health System investigators are involved in study design and conduct
- the project intends to disseminate the results through peer reviewed publication and any agreement does not limit our ability to publish study results
- Intellectual property developed in the project is shared equitably with the University/Health System

For information on distinguishing between quality improvement projects and research see Yale HRPP Reference Guide at https://your.yale.edu/sites/default/files/files/ResearchSupport/HRPP/ReferenceGuide-QualityImprovement-ClinicalSetting_WithoutSurvey_2023-01-30.pdf

Nature of the Data: Requests should conform to minimum necessary principles. Additional scrutiny will be afforded to data sets that are identifiable, contain sensitive data, notably data subject to additional restrictions under state or federal law (42 CFR Part 2, HIV, mental health) , are derived from sources where the data subject would expect strict privacy or include a large

number of data subjects (>500 individual data subjects). In addition, it is preferable that the data be provided through provisioning access to a data pool controlled by the University and/or Health System rather than providing a copy of the data to the recipient.

Recipient Organization: Consideration will be given to mission of the recipient organization as well as the privacy posture of the recipient's location. Recipients subject to strict local privacy statutes afford additional comfort that the data will be maintained appropriately. Entities that may commercialize the de-identified data are subject to a higher threshold of analysis to ensure institutional and/or Yale patient benefit from the disclosure. Data sent to or accessed by the recipient organization must be properly encrypted and securely transferred or accessed.

Contractual controls: Data may only be shared under a fully executed data sharing agreement. The agreement should preclude 1) further dissemination of the data; 2) use outside the proposed project; and 3) re-identification or contact of data subjects. The agreement should require, along with standard contractual terms, the recipient to return or destroy the data following completion of the project, require that appropriate data security controls be implement for the transmission and storage of the data, mandate timely reporting of potential breach events and ensure continued access to the data by the University and Health System.

Data subjects' expectations: Data that was collected with the data subjects full awareness that the data may be shared will be considered more favorably than cases where the data subject was unaware that sharing was possible. As such, data related to minors or cognitively impaired individuals would be held to additional scrutiny.

Financial or non-financial remuneration: Compensation for costs associated with preparing, maintaining, or analytic services of the data set may be required, however, remuneration must be in accordance with any regulatory constraints including the prohibition on sale of PHI under HIPAA.

Submissions

Requests may be submitted to either the University Privacy Office or the Health System Office of Privacy and Corporate Compliance. Requests may be submitted by University staff involved in the data request or may be escalated by offices such as Sponsored Projects, Procurement, Human Research Protection Program, Corporate Compliance, etc.

Requests must include the following information:

1. Name and contact information of the University or Health System contact;
2. Name and contact information of proposed data recipient;
3. Description of the purpose of the data request including any associated grant proposal or IRB protocol and a description of University or Health System involvement in the proposed data use;
4. Description of the data to be released including the data fields to be included, any identifiers associated with the data or verification of de-identification of the data, description of the context in which the data was collected (eg with or without patient

consent, internationally or in states with enhanced privacy statutes, etc). Note that 3rd party verification of data de-identification may be required and/or subject to audit as appropriate to the nature of the data;
5. A copy of the proposed data sharing agreement, if available;
6. Description of how the data will be accessed or, if the data is to be transferred, how the data will be secured in transmission and while stored by recipient;
7. Description of how the costs associated with creating and maintaining the data set will be covered;
8. Approvals associated with any relevant compliance reviews (HRPP, Conflicts of Interest) and in the case of data collected in research, approval of the study PI of the initial project where the data was collected.

Council Review

The Joint Health Data Governance Council will review and may require changes to data sharing proposals in order to gain Council approval. The Council will only approve where consensus for approval can be reached by both the University and Health System. In cases where consensus cannot be reached, the case may be escalated to the relevant senior leadership of the University and Health System for consideration.