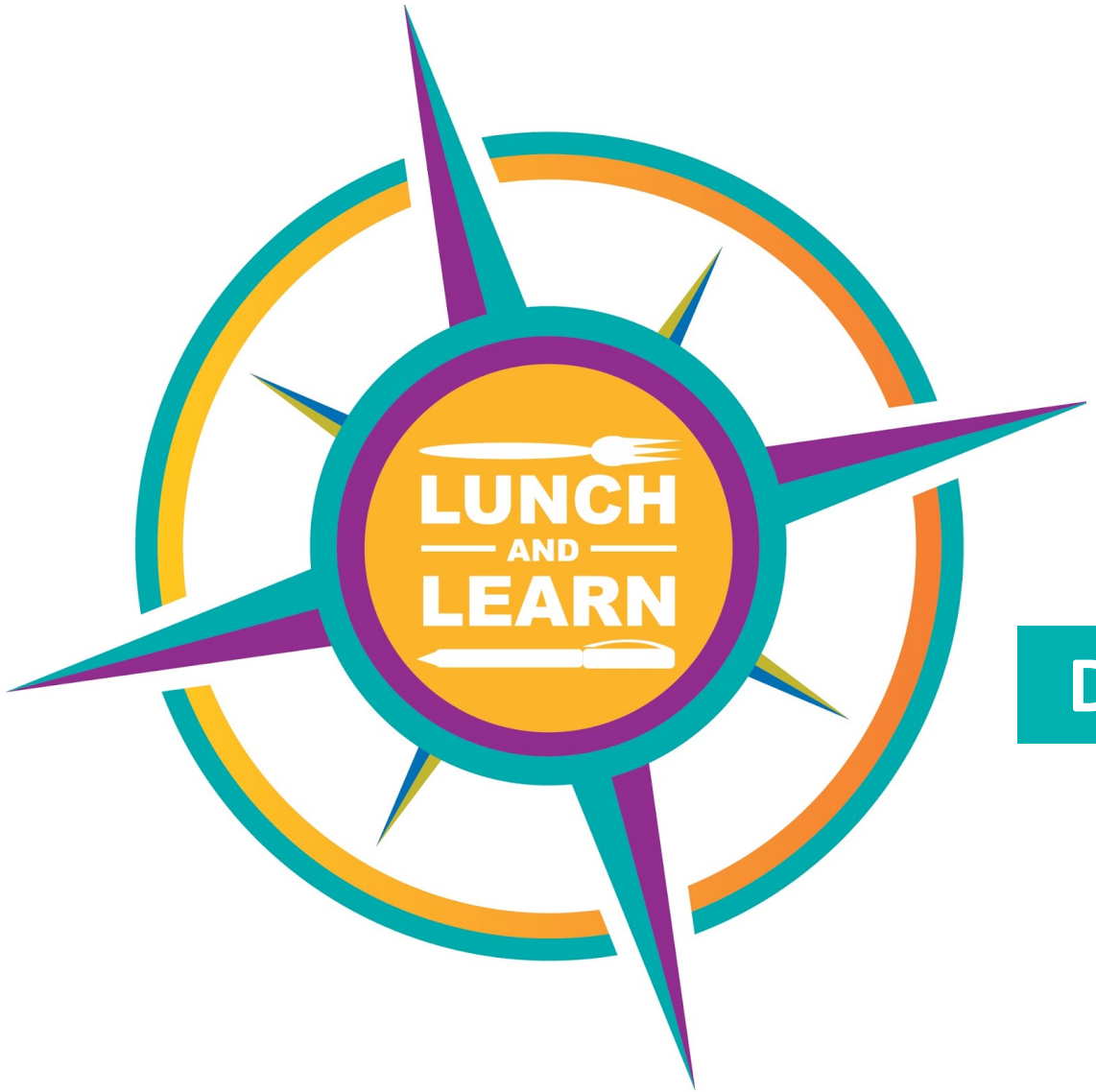

NAVIGATE
UNIVERSITY OF MICHIGAN

Demystifying Data Use Agreements

Welcome and Introduction

Today's Guest Speaker

Patrick Woods

Managing Project Representative – Private Team

Office of Research and Sponsored Projects (ORSP)

Information to know: Agenda

- Can you share the data?
- Did the data come from human subjects?
- Are there regulations controlling the sharing of the data?
- Do you have the appropriate agreement?
- What terms are required?

Data Types and Agreements

- Types of Data to consider:
  - General results data (laser tests, chemicals, animals)
  - Derived from Human Subjects
  - Derived from records related to people (i.e., banking records, housing records, census data, medical records)
  - Raw data vs. coded or identifiable data

Ownership, Regulations and Considerations

- Data cannot be owned directly
  - You can’t own and restrict the use of the # 5
  - Copyright controls the organization of the data itself
- Data derived from human subjects
  - Identifiable data
    - HIPAA, FERPA, Common Rule
    - Banking laws
    - Privacy laws
  - No identifiers (anonymized, de-identified, raw results)
    - Copyright, contractual requirements
      - Do you wish to restrict or limit use, further transfer/disclosure
      - If de-identified data of UM Patients, UM policy requires DUA to transfer
      - If de-identified from non-UM patients or common rule subjects, DUA not required by regulation
        - May be required by agreement providing data to UM

How to Transfer – Considerations

- Is the data identifiable in any format to an individual
  - Aggregated vs. Aggregated:
    - Is this data aggregated at the individual level of several data sets combined OR
    - Is this data aggregated in summary form (i.e., 35% of all respondents were found to have X result)
- Non-human data/basic results
  - Do you wish to add any restrictions on the use of the data? Add these by contract.
    - Cannot disclose to third parties
    - Cannot publish
    - Must acknowledge or provide co-authorship as appropriate
    - Security requirements
  - Basic results data of lasers, chemicals, animals, etc., can be covered in regular NDA

Do Regulations Apply?

- Common Rule – covers research of all human subjects and identifiable information alone or may be supplemental when other regulations apply (HIPAA, FERPA, etc.)
- Regulations generally cover identifiable data
  - Once data is properly de-identified under a given regulation, that regulation no longer governs the data
    - Example – Data is extracted from medical records (governed by HIPAA)
      - The data is not recorded with any identifiers, direct or indirect under HIPAA = the data is likely not governed by HIPAA and authorization is not required
      - Remaining consideration – a general concept of HIPAA is the likelihood that the data can be identifiable to an individual (i.e., rare diseases may be identifiable without the identifiers under HIPAA as the population is so small that it's easy to re-identify someone)
        - This is the same basis for why age becomes an identifier over 89 under HIPAA
  - Is the law/regulation applicable to the entity with the data?
    - HIPAA data given to a non-covered entity only remains governed by HIPAA through contractual obligations
    - Per 45 CFR 160.103 – HIPAA covered entities (Healthcare providers, health plans, and health clearinghouses) are required to comply with the Privacy Rule of HIPAA.
      - This can include Self-insured companies providing health coverage, company health plans, etc.
      - UM is a hybrid entity (We have a covered entity component and a non-covered entity component)

Do Regulations Apply? *(continued)*

- FERPA – Applicable to educational records which are those of an educational agency/institution or party acting on its behalf AND "directly related" to a student (34 C.F.R. 99.3)
  - Also covers medical records of students instead of HIPAA (has its own HIPAA within FERPA for student health center records, etc.)
  - Is the data de-identified?
    - Dept of Ed. guidance refers to anonymization, blurring and de-identification techniques
    - De-identification – minimizing risk of unintended disclosure of the identity of individuals
      - Do new categories need to be created to cover unique cases (blurring)?
      - Considerations:
        - There is not a set list of indirect identifiers like in HIPAA. This requires encompassing all of the elements together
        - Example – demographics, grade level, school – these may all be de-identified by themselves but if you disclose all and there is only one Asian-American female in 10th grade at that school, it becomes identifiable FERPA data
- You can still disclose identifiable FERPA data without consent under several exceptions (34 C.F.R. 99.31(a)).
  - Most common – Directory Information (publicly available); Studies exception; Audit or Evaluation

“Human Subjects” in “Research”

- Each regulation defines what is “identifiable” to a human subject or is “de-identified/anonymized”
  - Properly de-identified/anonymized data renders it research NOT on Human Subjects (caveat for the actual interaction to collect the data directly and whether it is recorded in an identifiable/coded manner).
    - Examples – HIPAA v. Common Rule
      - Limited Data Set is Human Subjects while De-identified is not (Code number is allowed in De-identified data under HIPAA per 45 C.F.R. 164.514)
      - Coded Data under the Common Rule IS identifiable and IS human subjects unless the key is destroyed (this is anonymized in Common Rule as it does not recognize De-identified as a data type)
      - FERPA – “de-identification is considered successful when there is no reasonable basis to believe that the remaining information in the records can be used to identify an individual” (PTAC Guidance from Dept of Education).

“Human Subjects” in “Research” *(continued)*

- Is the project ”Research”?
- No Human Subjects or not Research may mean no informed consent is required
  - This does not necessarily negate the need for an agreement to transfer the data.
  - IRB review may still be required
  - Consent may be required but may not be reviewed and regulated by your IRB

Data Transfer/Use without Consent

- Most data regulations provide exceptions allowing transfer and use of data derived from Human Subjects without their consent:
  - HIPAA – Transfer of a Limited Data Set allowed without consent upon IRB approval and an agreement between the entities with certain terms required
    - One required term is to use no more than the minimum amount required for the purpose of the project
    - De-identified data not regulated under HIPAA and no agreement or consent required
    - QA/QI allows for transfer without consent pursuant to proper agreement in place to control use of the Data (not Research)
  - FERPA – Several exceptions (Directory Information, Studies Exceptions, Audit and Evaluation, School Official, De-identified)
    - Requires agreements in most cases
  - GDPR Implications going forward

Agreement Types and Information

- Data Use Agreement
  - Agreement to control terms and restrictions on data in general (used for HIPAA, Common Rule, FERPA, etc.)
  - Includes standard terms of:
    - Transfer grants no rights except those of this Agreement
    - Use appropriate safeguards
    - Do not transfer to other parties without consent of provider and an equally restrictive agreement
    - Report unauthorized use or disclosure
    - Do not attempt to identify or contact individuals
    - Return or destroy

Agreement Types and Information *(continued)*

- Data Transfer Agreement
  - Used for transfer of identifiable data for research purposes such as HIPAA transfer of Protected Health Information (PHI).
  - Terms to add
    - Same as Data Use Agreement
    - Additional terms to include:
      - Request and use the minimum amount of data necessary for the purpose
      - Follow HITECH, NIST destruction requirements, etc.
      - Use/contact of individuals limited to authorization
      - Notify HHS of breach/unauthorized use and disclosure
      - IRB determination prior to use

Agreement Types and Information *(continued)*

- Business Associate Agreement
  - DHHS Guidance – "If a covered entity engages a **business associate** to help it carry out its health care activities and functions, the covered entity must have a written business associate contract or other arrangement with the business associate that establishes specifically what the business associate has been engaged to do and requires the business associate to comply with the Rules' requirements to protect the privacy and security of protected health information"
  - Used when receiving/transferring identifiable (full PHI) data under HIPAA for a <u>service</u>
    - Covered entity transfers to billing agency names and addresses to bill and collect for treatment
    - Billing agency becomes Business Associate
      - Steps into the place of the Covered Entity and acts as the Covered Entity
      - Agreement limited to the specific service being provided
    - **<u>NOT</u>** for research projects involving full PHI (see Data Transfer Agreement).

Agreement Types and Information *(continued)*

- FERPA Additions
  - Must be time limited under the exceptions (can be extended)
  - Must destroy information when no longer needed
  - Must provide who is authorized to receive it and to whom it can be shared
  - Must state the purpose (this allows the study or audit/evaluation exceptions to be covered as those are limited to the very purpose included only)
  - Often includes a requirement for a deliverable of a report
    - You cannot easily claim you were auditing a program or improving instruction if you do not provide a report back to the school/district
    - May include language about keeping a log of all copies of the data shared
      - These are required to be provided by the district to the students and parents in some situations annually.

Agreement Types and Information *(continued)*

- GDPR Issues
  - Applicable to data collected or processed in the EU (and other EU Economic Area) or data accessed from the EU
  - Controller-Processor Agreements
  - Controller-Controller Agreement
  - Processor-Sub-processor Agreement
  - Controller – has control of the type of data being collected (drafted protocol) and how it is used (coordinating center)
  - Processor– is collecting, manipulating and providing data on behalf of the controller
  - U.S. Universities (if not receiving data – you may not be subject to GDPR)
    - Are you collecting data in the EU?
    - Are you accessing the data from the EU?
    - If collecting data from EU residents while in US, are you following up with them when they return to the EU?
  - Is there such a thing as ”anonymized” data under GDPR?
    - Standard of de-identification is not the same as HIPAA and is not de-identified (”anonymized”)
    - Regulation states it must be impossible to re-identify
    - No definition or cases yet on what is “impossible” and how to know if you’ve met that standard

Options to change nature of data

- It is possible to be more inclusive in consents.
  - Notify the subjects de-identified versions of the data will be used in the future with both for-profit and non-profit entities. Describe whether identifiers would be potentially shared, destroyed at some point, etc.
- Be more restrictive on what/how data is shared.
  - Do dates need to be provided (Limited Data Set) or can the duration between admission/discharge, recurring events, etc. be shared by calculation instead
    - EX: Date of admission and Date of 2nd admission (LDS and more likelihood of re-identification) vs. 145 days between admission (De-identified and harder to re-identify)
    - Only use LDS indirect identifiers when absolutely needed rather than convenience, because of computer system requirements that could be modified, etc.
- Evaluate with heads of institutions what is most important and driving consideration (i.e., concern explaining to medical patients about use of their data and losing patients vs. if sharing with non-profits you have fewer concerns than with a for-profit?)

Summary

How did you get the data?

- From UM Patient Records?
- From a project in which you collected it directly?
- From another entity?
  - Under an agreement or without an agreement?
- Does the agreement (funding agreement for UM Project or agreement transferring data to UM) allow for data to be transferred?

Do you have data covered under regulation?

- Is it regular results not derived from human subjects?
- Is it aggregated into summary results or is it individual level of human subjects?
- If not – do you want an agreement for adding restrictions or is one required by UM policy

Is the data identifiable in any form?

- If not, see #1
- If so, was it collected with consent/authorization?
  - Does that allow further transfer?
- Can you transfer without consent

Have you received IRB review?

- May be required. If you're not sure, ask IRB as they can determine whether you need their review.

Use the correct agreement.

- DUA, DTA, BAA, NDA, Other

Include any required terms by regulations or agreements that provided the data to UM.

- Your funding agreement or subcontract to a subcontractor may allow transfer but does it include required terms or is an amendment/additional agreement required?

Additional Resources

- FDP has template agreements and FAQs and Guidance on Human Subjects identification (Tool for Classifying Human Subject Data)
  - http://thefdp.org/default/committees/research-compliance/data-stewardship/
- Government Guidance Sites (HHS, Dept of Ed, etc.)
- Citations:
  - FERPA – 20 U.S.C. 1232g and 34 C.F.R. Part 99 (especially 99.31)
  - HIPAA – Pub.L. 104-191 and 45 C.F.R. Parts 160 and 164, Subparts A and C
  - Common Rule (codified separately by 15 Federal Departments and Agencies

Additional Resources *(continued)*

- Common Rule Citations:
  1. Department of Agriculture: 7 CFR Part 1c
  2. Department of Energy: 10 CFR Part 745
  3. National Aeronautics and Space Administration: 14 CFR Part 1230
  4. Department of Commerce - National Institute of Standards and Technology: 15 CFR Part 27
  5. Consumer Product Safety Commission: 16 CFR Part 1028
  6. Agency for International Development (USAID): 22 CFR Part 225
  7. Department of Housing and Urban Development: 24 CFR Part 60
  8. Department of Defense: 32 CFR Part 219
  9. Department of Education: 34 CFR Part 97
  10. Department of Veterans Affairs - Office of Research Oversight - Office of Research and Development: 38 CFR Part 16
  11. Environmental Protection Agency - Research and Development: 40 CFR Part 26
  12. Department of Health and Human Services: 45 CFR Part 46
  13. National Science Foundation: 45 CFR Part 690
  14. Department of Transportation: 49 CFR Part 11
- GDPR – EU 2016/679 (27 April 2016)

Questions?

Patrick J. Woods

Managing Project Representative

ORSP – University of Michigan

pajwoods@umich.edu

734-764-8566