**WORKSHEET: DETERMINE IF SECONDARY USE OF DATA IN THE CONTEXT OF AI/ML/BIG DATA TECHNOLOGIES INVOLVES HUMAN SUBJECTS PER HHS DEFINITION**

|  |
| --- |
| **PURPOSE AND APPLICABILITY** |

This worksheet provides assistance for researchers and IRB staff who have already determined that an activity involving secondary use of data in AI, ML or other Big Data technologies meets the definition of research under the HHS and now wish to determine if the activity involves human subjects per the HHS definition.

|  |
| --- |
| **CONTEXT** |

**The HHS regulations at 45 CFR 4.102(e)(1) define a human subject as** “a living individual about whom an investigator (whether professional or student) conducting research: **(i)** obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; **or (ii) obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens.”**

**This worksheet focuses on part ii of the definition.** This part has become challenging to apply because of the impact of AI/ML/Big Data technologies. Examples of these technologies can be found in everyday life now. They include Hey Siri, ChatGPT, Netflix recommendations, PayPal’s fraud detection, facial recognition technologies used by law enforcement. The rapid evolution of these technologies introduces new questions and considerations concerning the privacy and identifiability of data because they can now gather, sort and process information in ways that were not anticipated by human subjects regulations. This worksheet is designed to factor these additional risks into the determination of whether secondary use of data in research with AI, ML or Big Data Technologies includes human subjects.

|  |
| --- |
| **INSTRUCTIONS** |

Assess the research activity against each of the questions in the tables below. **The items should be considered in the order presented** to reach the correct conclusion. **If all boxes are checked as “Met” in response to questions 1, 2, 3 and 4, the research involves human subjects.**

|  |  |
| --- | --- |
| **CHECK ALL BOXES THAT APPLY** | **Met** |
| 1. **Does the project include living individuals?** |  |
| 1. **Is the information about a person?** |  |
| 1. **Will the researcher obtain and use, study, analyze or generate private information?** |  |
| **+ Guidance**   * **Private information**   ***Common Rule definition:*** *information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (e.g., a medical or school record).*  **Consider the questions below when deciding if the information is private.** If there are concerns about the voluntariness and intentionality of disclosure, or differences in privacy expectations, and reliability or lawfulness of the source of information, then there may be a stronger argument for considering the information to be private, particularly if the data could be harmful or damaging to the data subjects.   * + ***What is the likelihood that the data will include information that was disclosed involuntarily or unintentionally?*** Consider the source of the data and keep in mind that as people disseminate personal information in the digital world, they may be unaware of the level to which they have made their data accessible. For example, they may not have been able to disable cookies or set appropriate privacy settings on their social media accounts and inadvertently shared information outside of their intended audience.   + ***Are there significant differences concerning expectations of privacy and control over personal information?***  Big Data technologies allow governments, organizations, and marketers to know, or deduce, an increasing number of data items about aspects more and more information about us. Individuals often agree to terms of use that dictate how their personal information will be used but feel that they have no choice other than to hand it over in order access to the services. Yet, a person’s attitude or disposition towards privacy is contextual and habitual, and influenced by many motivators and deterrents beyond risks and benefits. Many Americans would like to do more to protect their privacy. * ***Could the information be harmful or damaging to the data subjects?***It is especially important to exercise caution when the information is sensitive in nature and could put someone at risk or be damaging to them.This information typically falls into categories of data that are protected by laws and regulations, such as health information protected under [HIPAA](https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html), education records protected under [FERPA,](https://studentprivacy.ed.gov/ferpa) and information covered by state breach notification laws like the one in [WA State](https://apps.leg.wa.gov/rcw/default.aspx?cite=19.255&full=true#:~:text=(2)(a)%20%22Personal,D)%20Full%20date%20of%20birth;). The EU [GDPR](https://gdpr.eu/) calls out special categories of personal data that require a higher degree of protection: * Information about minors. * Information about racial or ethnic origin, religious or philosophical beliefs, or trade union membership. * Information concerning an individual’s health. * Information concerning an individual’s sex life or orientation. * Genetic information. * Biometric data. |  |
| 1. **Will the researcher obtain and use, study, analyze or generate identifiable information?** |  |
| **+ Guidance**   * **Identifiable information.**   ***Common Rule definition:*** *information for which the identity of the subject is or may readily be ascertained by the investigator or associated with the information*  **Identifiability and AI/ML/Big Data technologies.** We live in an era in which AI can use the large volumes of data collected about us to re-identify data subjects in data sets that have been de-identified using techniques such as 1) the removal of attributes, 2) the generalization of attributes, and 3) the obfuscation or transformation of attributes. AI’s enhanced pattern recognition does not require an overlap of data points between databases to re-identify data subjects. Some real-life examples include the [re-identification of NY Taxi trips](https://www.theguardian.com/technology/2014/jun/27/new-york-taxi-details-anonymised-data-researchers-warn), [re-identification of credit card transactions](https://www.science.org/doi/full/10.1126/science.347.6221.468), the [re-identification of browsing data](https://www.theguardian.com/technology/2017/aug/01/data-browsing-habits-brokers), and [re-identification of individuals in government healthcare data](https://www.abc.net.au/news/science/2017-12-18/anonymous-medicare-data-can-identify-patients-researchers-say/9267684). Due to this increased risk of re-identification, the Common Rule definition of identifiable information is not adequate for research using AI/ML/Big Data platforms and when data will be broadly shared.  **Decision-making framework:** The table below lays out additional standards by which to determine when information for this type of research should be considered identifiable. It is intended to be used after the information has been determined NOT identifiable according to the Common Rule definition.   |  |  |  | | --- | --- | --- | |  | **Scenarios** | **Determination** | | **1** | The PI attests that data will not be shared outside of the institution and that data will not be put into any AI/ML/Big Data platform other than an institutional platform within a protected environment. | Information is NOT considered identifiable | | **2** | Data will be shared either with a collaborator, or through a controlled-access repository (e.g. dbGap), but will not be in any AI/ML/Big Data platform other than an institutional platform within a protected environment.   * PI provides certification that risk of re-identification is low. * PI attests that: (i) Data Use Agreements will be in place for data sharing, (ii) data will only be shared through controlled access repositories, and (iii) there will be no attempt to re-identify data subjects. | Information is NOT considered identifiable | | **3** | Data will be shared through open access repositories, or data will be entered into an AI/ML/Big Data technology that is not an institutional platform within a protected environment.   * PI attests that if re-identified, the data are NOT sensitive data (see above list) and do NOT put the data subject at risk. | Information is NOT considered identifiable | | **4** | Data will be shared through open access repositories, or data will be entered into an AI/ML/Big Data technology that is not an institutional platform within a protected environment.  If re-identified, the data ARE sensitive data or could put the data subject at risk. | Information IS considered identifiable for purposes of this determination | |  | Definitions:   * *Protected environment:* A data environment approved by the institution’s ISO with an institutional contract and data sharing controls for use with controlled or confidential institutional data. * *Controlled-access repository*: a data repository that provides access to data only to approved requestors. Access is typically governed by a data use agreement and other licensing requirements. * *Open access repository*: a data repository that is publicly accessible and often doesn't require user registration. * *Risk:* includes the potential for criminal or civil liability, or damage to financial standing, employability, educational advancement, or reputation. | |  * **Data that has high risk of re-identification through use of algorithms.**   + **Whole genome and whole exome data.**   + **Medical imaging data.**   + **Voiceprints, full-face images, and comparable images.**   + **Rare diseases, small datasets, and other distinctive data.** * **How to obtain certification that risk of re-identification is low.** This could be obtained from a company like [ArcherHall](https://archerhall.com/) or using an appropriate tool such as those found on the following websites:   + [NIST Disassociability Tools](https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/focus-areas/de-id/tools)   + [Johns Hopkins De-identification Software](https://guides.library.jhu.edu/protecting_identifiers/software) * **Referrals and Ancillary Reviews.** Use below recommendations for referrals and/or ancillary reviews based on institutional structure and availability of resources as needed. * **Data Protection/Privacy Office/Officer.** Assist in assessment of identifiability. * **Legal Affairs, University Compliance Office.** Review legal aspects, ensuring compliance with laws related to data privacy (GDPR, HIPAA), other relevant items, as applicable. * **Other offices with GDPR experience.** May be able to assist in assessment of identifiability * **Community advisory boards.** Aid in assessment of group harms, even if not considered human subjects research. * **Consultant.** Subject matter experts to assist with IRB office’s assessment. | |

[**[top]**](#Top)

|  |
| --- |
| **REFERENCES** |

1. Secretary’s Advisory Committee on Human Research Protections, [IRB Considerations on the Use of Artificial Intelligence in Human Subjects Research](https://www.hhs.gov/ohrp/sachrp-committee/recommendations/irb-considerations-use-artificial-intelligence-human-subjects-research/index.html), October 19, 2022.
2. Hutson, M., [The Future of Computing](https://www.sciencenews.org/century/computer-ai-algorithm-moore-law-ethics). Science News*,*201(4), 16-22, 2022.
3. Rainie, L., [Americans’ complicated feelings about social media in an era of privacy concerns](https://www.pewresearch.org/short-reads/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/#:~:text=People%E2%80%99s%20issues%20with%20the%20social%20media%20experience%20go%20beyond%20privacy.). Pew Research Center, March 27, 2018.
4. Schairer CE, Cheung C, Kseniya Rubanovich C, Cho M, Cranor LF, Bloss CS., [Disposition toward privacy and information disclosure in the context of emerging health technologies](https://pubmed.ncbi.nlm.nih.gov/30938756/#:~:text=Results:%20Three%20key%20findings%20from%20the%20qualitative%20data%20suggest%20a). J Am Med Inform Assoc. 2019 Jul 1;26(7):610-619. doi: 10.1093/jamia/ocz010. PMID: 30938756; PMCID: PMC6562158.
5. Vamosi, S., Platzer, M. and Reutterer, T., 2022. [AI-based re-identification of behavioral clickstream data](https://arxiv.org/abs/2201.10351). arXiv preprint arXiv:*2201.10351*.
6. Rocher, L., Hendrickx, J.M. & de Montjoye, YA. [Estimating the success of re-identifications in incomplete datasets using generative models](https://doi.org/10.1038/s41467-019-10933-3). Nat Commun **10**, 3069, 2019.
7. Shahid A, Bazargani MH, Banahan P, Mac Namee B, Kechadi T, Treacy C, Regan G, MacMahon P[. A Two-Stage De-Identification Process for Privacy-Preserving Medical Image Analysis](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9141493/). Healthcare (Basel). 2022 Apr 19;10(5):755. doi: 10.3390/healthcare10050755. PMID: 35627892; PMCID: PMC9141493.
8. DuBois, James M., [At the Dawn of Qualitative Data Sharing: Questions IRBs May Want to Ask During Protocol Review](https://blog.primr.org/at-the-dawn-of-qualitative-data-sharing-questions-irbs-may-want-to-ask-during-protocol-review/). January 18, 2024.