## Negotiation Guidance for Data Agreements

### PURPOSE

This Job Aid provides guidance on Data Agreements, in two broad categories of Data Use Agreements ("DUA") and Business Associate Agreements ("BAA").

### A. DEFINITIONS:

1. **Data Use Agreement ("DUA"):** is a contractual document used for the transfer of data that has been developed by an entity (non-profit, governmental or private industry), where the data is non-public or is otherwise subject to some restrictions on its use or access.
    - May or may not involve Protected Health Information (PHI).
    - May also be known as Data License Agreement, Data Sharing Agreement, Data Transfer Agreement, Data Access Agreement, Data Exchange Agreement, End User License Agreements (EULA) or contained within an Agreement or under the generic label of Memorandum of Agreement (MOA) or Understanding (MOU).
    - If having general discussions about unprotected data, use Non-Disclosure Agreement ("**NDA**").
    - If transferring/receiving material with unprotected data, use Material Transfer Agreement ("**MTA**").
    - Data from internet sources may be subject to Cyber Security regulations, or other restrictive terms, and the agreement may require review by the Office of General Counsel (OGC) and the Office of Research Integrity and Assurance (ORIA).

2. **Business Associate Agreement ("BAA"):** is a business relationship between a Provider who may be deemed a "Covered" Entity for sending data and a "Business Associate" for receiving data as defined by HIPAA (Health Insurance Portability and Accountability Act of 1996. ASU can be either type of entity, and as a hybrid, certain departments within ASU may be "Covered Entities" (Speech & Hearing, for example). More information about these ASU departments can be found in the ORIA website. https://researchintegrity.asu.edu/

   **Covered Entities** - under the HIPAA Privacy Regulations include the following entities: 1) health plans; 2) healthcare clearinghouses; and 3) healthcare providers who conduct certain electronic transactions, including billing and claims. Therefore, "covered entities" will include hospitals, skilled nursing facilities, pharmacies, most physician practices and most other healthcare providers. Entities such as ASU may also be covered entities, even if the entity's primary purpose is not the provision of healthcare services, if the entity has a unit that is a health plan, healthcare clearinghouse or healthcare provider. Such

entities are referred to as "hybrid entities" under the regulation. More information about ASU's hybrid entities can be found at: https://getprotected.asu.edu/training/asu-and-hipaa

- The agreement intends to protect the privacy of data and provide for the security of the data as required by HIPAA for data being accessed that is Protected Health Information ("PHI") or Limited Data Set with de-identified information which is ASU's preference.
- These requirements apply:
  - Standards for Security and Privacy of Individually Identifiable Information (the "Security and Privacy Regulations"), as applicable, covered under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")
  - Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), Subtitle D-Privacy (§§13400-13424), as part of the American Recovery and Reinvestment Act of 2009, and as amended.
  - The Security Rule requires Covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting electronic-PHI (e-PHI).

## B. PROCESS TO DETERMINE WHICH TYPE OF AGREEMENT TO USE:

**1.** Proposal and Negotiations Team (PNT) receives a Data Transfer-Use Request Form for creation of a Data Agreement or another entities' Data Agreement for review and assigns it to a Contracts Grant and Contract Officer (GCO).

The PNT GCO reviews the characteristics of data described by the requestor. If related to personally identifiable information, confirm with ORIA if there is an IRB protocol required.

- If data is De-identified, use the template from the FDP DTUA for De-identified Information.
- If data is for a Limited Data Set, use the template from the FDP DTUA for Limited Data Set.
- If data is for Student Records, use the DUA template which includes FERPA.
- For all other data types (restricted data, criminal records, mental health psychotherapy notes, GDPR, treatment records), check with ORIA for IRB or IACUC coverage.

If Data is from or to a Covered Entity use the Business Associate Agreement template.

NOTE: Restricted Data includes: Export-controlled, Publication restrictions, Sensitive but Unclassified and the EU GDPR. The access to, control of, and protection of this type of data will be governed by other laws and regulations (e.g. ITAR, EAR, NISPOM, etc.). Contact ORIA for any agreements regarding this type of data. (If accessing Classified data- this

must have a DD254 from the Sponsor. Contact Research.Integrity@asu.edu when this is marked.)

**2. Which One? Data Use Agreement (DUA) or Business Associate Agreement (BAA)**

- Determined by the usage of the information
    - If information is Protected Health Information (PHI), and/or for or related to providing services to a patient, a Business Associate Agreement ("**BAA**") is required to share this information. The Covered Entity is responsible for controlling the BAAs which are issued.

      Example: ASU's Department of Speech and Hearing is a Covered Entity because they have patients receiving hearing aids. They disseminate information about the patients and hearing aids to manufacturers and health entities under outgoing BAAs.

    - If the information is de-identified, or non-PHI, a Data Use Agreement ("**DUA**") is appropriate.

    - If having general discussions about unprotected data, use Non-Disclosure Agreement ("**NDA**").

    - If transferring/receiving material with unprotected data, use Material Transfer Agreement ("**MTA**").

**3. Signature Authority:** The assigned PNT GCO determines who should sign the Data Agreement: ORIA Director, the PI's department, or PNT Director (either Assistant or Associate Director).

a. When might the ORIA Director sign? If the data involves:
    - Compliance Review
    - Other Data types: Export Control, Restricted Data, GDPR, Treatment Records, Mental Health Records, Criminal Records
    - IRB approval is required

b. When might the PI's department sign?

    - IRB approval is <u>not</u> required; AND
    - the agreement is <u>not</u> related to a sponsored project; AND
    - the agreement only includes terms and conditions that the department has the authority to agree to. For example, this would not include indemnification, insurance, etc.

- Per OGC guidance on signatory authority policy as of 4-28-2014, **certain VPs and Deans** are granted the ability to sign Business Associate Agreements so long as they directly relate to the functions of the department, don't impose any financial obligations on the University, and are on the OGC approved template (as marked in the footnote). If they are using an approved template, they do not need to go through either PNT or Purchasing. However, when someone is proposing any modifications to the template or when they are going to have Purchasing/PNT sign the agreements then they would go through PNT who will review and either modify/approve or escalate to OGC as appropriate.

c. PNT Director (Associate or Assistant) signs in ALL other instances

**Note:** If the ORIA Director or the PI's department is going to sign the agreement, PNT should still review the terms of the agreement and offer to handle the negotiations with the sponsor, or at least redline the agreement and provide a copy to whomever is handling the negotiations.

**4. Notice and Distribution**

Send to the ORSPA PNT physical location mailing address (not PO Box) with courtesy email to ASU.Awards@asu.edu

PNT GCO to forward official Notices to OGC with copy to ORIA, RTSHelp (IT Security Officer) and University HIPAA Privacy Officer, as needed

Distribution Requirements of Data Agreements:

a. **For ALL DUAs:** Distribute to PI, RA and/or Department Business Manager AND:
   - ORIA Research.Integrity@asu.edu

b. **For ALL BAAs:** all parties listed in a. PLUS:
   - University HIPAA Privacy Officer – Dr. Aaron Krasnow aaron.krasnow@asu.edu
   - Clinical Partnership Office – Dr. Alan Rawls alan.rawls@asu.edu

c. If agreement includes IT security questions for data access or Data Security Plan, distribute also to:
   - UTO IT Security Officer – AVP Tina Thorstenson tina.thorstenson@asu.edu
   - OKED IT Support - RTSHelp@asu.edu (Rick Gould)

d. If ASU receives notice of violation action (non-administrative), send to all in a. and b. above PLUS:

- Office of General Counsel – Benjamin Mitsuda bmitsuda@asu.edu HIPAA specialist

e. End User License Agreements: If signed by PNT, distribute to PI and RA only

Can the PI accept web-based agreements to access data when the **End-User License Agreements (EULA)** or other similarly named Agreement may contain indemnity, confidentiality, IT security or other clauses?

- Answer – Perhaps. EULAs are not negotiable. The PI may need his department to assume risk of accepting the agreement, especially if indemnity terms are included. Before the department signs, the PNT reviews terms to identify those that cannot be revised so the department may assess its risk of accepting.

- If IT Security is required on the EULA, PNT coordinates through his PNT Lead or Director before forwarding to RTSHelp@asu.edu for review and determination of departmental IT security robustness. If there is no IT Security support at departmental level, then OKED RTS may facilitate it.

**5. Related Documents**

- **Data Security Plan.** This document should be completed by the PI and PNT will coordinate with RTSHelp@asu.edu as necessary. The final Data Security Plan needs to be included in the IRB submission. A sample plan for REFERENCE ONLY can be found at Sample DUA NCES Data Security Plan SO =Senior Official (ORIA Director); PPO = Principal Project Officer (Principal Investigator); SSO = System Security Officer (Department IT or RTS Lead Administrator)

- **Non-disclosure Agreement or Pledge of Confidentiality**. Data Agreements frequently require the PI, and often their staff with access to the data, to sign a separate Non-disclosure Agreement or Pledge of Confidentiality. Before obtaining signatures, review this document to ensure that the PI/research staff have the authority to agree to all of the terms and conditions. A sample Affidavit can be found at Sample DUA NCES Affidavits of Nondisclosure by Individual.

**6. Flagged Terms and Conditions commonly found in DUAs and BAAs that may need further negotiation or a business decision:**

- **Background Checks and Fingerprinting**: ASU is prohibited from holding personal information from non-ASU personnel (i.e., subcontractors). Especially important to exclude when ASU personnel will not "provide services directly to juveniles or vulnerable adults".

- **Confidentiality.** Data provider considers all data confidential, even unmarked.
- **Access Fees.** Similar to Membership Fees, question is whether department pays or is university-wide access.
- **Governing Law of another State or Country.** (if non-negotiable may need PNT Business Decision)
- **HIPAA protected PHI.** Information that might identify individuals.
- **Intellectual Property**. Generally silent but might be that the data and derivatives is owned by the data source holder. (Notify Skysong Innovations)
- **IT Security.** Data may not be placed in the general ASU network of shared files. Might require a secured office or lab and laptop with encryption. Sometimes access is in person only at the data holder's site. (Notify RTSHelp)
- **Return or Destruction of Data.** Either removing from computers, systems or files and returning to Licensor, or destroying data with evidence of destruction. (Department might need assistance to verify electronic removal from RTSHelp)
- **Notification of Violation**(s) – including by Subcontractors – less than five (5) days of occurrence or "immediately" **watch for Different Reporting Dates for Receiving versus Sending Data ** ASU prefers at least five (5) days to notify or "reasonably promptly". If outside party requires less than five (days) or immediately, PNT will coordinate with the PI, department's IT and RTSHelp@asu.edu to ensure that ASU will be able to comply with the notification requirement.
- **Cyber security** regulations require coordination with UTO, OGC and ORIA review for data being accessed and secure storage (including Sensitive but Unclassified).
- Waiver request due to **Publication Restrictions**