Patient Data Use Agreement
(DRAFT model document for Review & Discussion purposes)

PREAMBLE:

This document is a proposed model patient data use agreement. It is intended to establish a relationship between an individual and a data management service entity for the purposes of managing the individual's complete, longitudinal health data on the individual's behalf. It provides complete control over the aggregated copy of the patient's data to the patient, including the destruction of the data should the patient wish to do so. This document does not authorize a data management service entity to function as a healthcare provider unless the data management service is already functioning in such capacity. The patient's aggregated copy of health data does not supplant existing provider-maintained records that law and regulation require healthcare providers to maintain, nor does it have any impact on provider responsibility to report public health data or perform any other functions related to medical records as may be required by federal, state, and local law.

I. Introduction

This **Patient Data Use Agreement** (PDUA or Agreement), by and between ________-_________________ (Patient) and _______________________ (Patient Data Manager, or PDM), authorizes PDM, on Patient's behalf, to request, acquire, receive, aggregate, maintain, curate, secure, share, and delete, with Patient's permission as granted pursuant to this Agreement, Patient's complete, longitudinal digital health record (or any portions of the health record designated by the Patient).

II. Background and Authority

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, provides individuals with a right of access to inspect and obtain a copy of protected health information from their medical records maintained by their healthcare providers [see 45 CFR 164.524(a)(1)]. Under this right of access, pursuant to 45 CFR 164.524(c)(3)(iii), individuals can request, in a signed writing identifying where and to whom, that their personal health information be provided to third parties on the patients' behalf.[1] Using this right of access, an individual can

[1] The HHS Office of Civil Rights provides further interpretive guidance regarding the use of the right of access to transmit PHI to third parties designated by the individual, including the use of an example of transferring PHI to an individual's mobile app on a smartphone, (FAQ #2036, https://www.hhs.gov/hipaa/for-professionals/faq/2036/can-an-individual-through-the-hipaa-right/index.html), and provides further guidance that such requests may be provided on a standing basis to avoid having to repeat requests for access each time PHI is updated (FAQ #2070, https://www.hhs.gov/hipaa/for-professionals/faq/2070/may-a-covered-entity-accept-standing-requests/index.html).

use a third-party patient data manager to aggregate a complete, longitudinal record and maintain it in a way to provide secure access to accurate, reliable personal health data.

Patient wishes to collect personal health data from a variety of providers and sources, including non-clinical sources and patient-generated sources; store that data in one complete, longitudinal record; and exert control over the sharing of and access to such health information.

PDM has the capacity to aggregate, maintain, and secure personal health data in a way that enables it to be: regularly updated; protected; compartmentalized; shared in whole or in part with the Patient's authorization; and maintained free of unauthorized changes or interference that could render the data untrustworthy.

Patient seeks to exert the right of access provided to Patient by 45 CFR § 164.524 and related HHS Office of Civil Rights guidance to regularly access personal health information maintained by healthcare providers in designated record sets and to direct providers to transmit Patient's personal health information to PDM on Patient's behalf.

As Patient wishes to have a complete, longitudinal health record under his or her full control and maintained on his or her behalf by PDM, Patient and PDM agree to the following terms:

III. Definitions

Patient: Patient is an individual who seeks to aggregate personal health data from disparate healthcare providers and sources, including data generated by him or herself.

Patient Data Manager (PDM): PDM is a third-party entity with whom Patient enters into this PDUA for the purposes of requesting, acquiring, receiving, aggregating, incorporating, maintaining, curating, and securing Patient's complete, longitudinal digital health record. Examples of entities who could act as PDMs are healthcare providers, health data systems, health insurers, and third-party mobile medical application entities.

Patient Health Record (PHR): PHR is Patient's aggregated, longitudinal health data that PDM maintains on the patient's behalf pursuant to this Agreement. The PHR does not replace healthcare providers' medical records systems, does not relieve any reporting responsibilities healthcare providers have under federal, state, or local law, and does not provide an alternative method for providers' required maintenance of medical records. Should PDM also be Patient's healthcare provider, the PHR shall not be comingled with the provider/PDM's electronic health record system.

Patient Data Receipt (PDR): An electronic computable set of structured data sent or provided to Patient or Patient's designated PDM at the conclusion of each health encounter or episode of care for inclusion in the Patient's PHR.

Protected Health Information (PHI): PHI is defined in this agreement as it is defined by HIPAA [45 CFR 160.103].

Standing Data Release (SDR): A release through which Patient exercises right of access to personal health information maintained at a healthcare provider on an ongoing, automatic basis and requests Patient's PHI be transmitted to Patient's PDM for curation in Patient's PHR.

IV. Standing Data Release

A. Patient shall be responsible for completing and submitting a Standing Data Release (SDR) to each healthcare provider from whom Patient seeks access to personal health information. PDM may facilitate the SDR process, as feasible. [*append sample form*]

B. The SDR complies with the Department of Health and Human Service's Office of Civil Rights' requirements for the release of personal health information from healthcare providers to third parties on the behalf of patients or patient representatives who are requesting access to personal health information. The SDR enables the Patient to authorize continual updates to Patient's PHR and provides instructions to healthcare providers on enabling automatic updates in the form of a Patient Data Receipt in electronic health record systems.

C. Patient understands that healthcare providers cannot transmit PHI to a third party such as PDM without the authorization of Patient or Patient's authorized representative. Patient also understands that once Patient submits the SDR to a healthcare provider, HIPAA provides the healthcare provider up to 30 days to complete the initial request and the right to seek a further 30-day extension.

V. Patient Control

A. Patient shall have complete authority and control over Patient's PHR and all of the data contained within it, regardless of the source of the information. Patient accordingly may direct PDM to share all or part of Patient's PHR with another entity or individual, including but not limited to a healthcare provider or family member.

B. Patient may revoke a third party's previously-granted PHR access. PDM shall immediately implement any such revocation (within one business day). Patient understands that data shared prior to revocation of access often cannot be removed from related records kept by a third party, such as when information from the PHR has been incorporated into a medical record maintained by a healthcare provider who treated Patient.

C. Patient shall have the ability and authority to add notes and comments to the information contained in the PHR. Such annotations shall be clearly distinguished from the original text of any health data provided by healthcare providers to maintain data integrity and provenance.

VI. Sharing of PHR with Designated Parties

A. Patient may authorize PDM to share some or all of Patient's PHR with individuals and entities that Patient identifies. PDM shall not share data without Patient's explicit permission.

B. PDM shall establish a process for Patient to request access for an identified individual or entity and to specify the type of access such individual or entity may have (e.g., full access, access to all except Patient-generated health data, access to medication information only, access to payer data, etc.).

C. PDM cannot guarantee that such designated parties will review the information that Patient chooses to share.

D. Patient may revoke this authorization at any time by notifying the PDM by online form, in writing, by telephone, or via other processes that PDM establishes. PDM shall not limit Patient to one method of notification but shall offer at least three means of revoking authorization. PDM shall implement Patient's revocation immediately and shall indicate in the PHR when the revocation has been so implemented.

E. Emergency Access. Patient may grant permission in advance to the PDM to share Patient's PHR in the case of an emergency during which Patient may not be able to authorize such sharing. Emergency sharing designations and permissions may be established and updated at any time, and may be limited to specific information of particular importance during emergency treatment when Patient is otherwise incapacitated.

VII. Health Data Aggregation and PHR Updates

A. PDM shall aggregate Patient's health data from each of the healthcare providers with whom Patient has executed SDRs into one cohesive, complete, longitudinal compilation of health data. Information can include but is not limited to medical records (including diagnostic imaging files such as X-rays or MRIs, lab results, and genomic sequencing data), billing records, and claims-related information. PDM shall resolve conflicting health data, as feasible *[and pursuant to Patient instruction and/or service tier etc.]*.

B. PDM shall enable the incorporation of Patient-generated health data (PGHD) from fitness trackers, wearables, remote health monitors, and other non-clinically-derived information into Patient's PHR. Such information will be clearly delineated as PGHD.

C. PDM shall enable the incorporation of subjective assessments by the patient of their health outcomes into the PHR (i.e., patient reported outcomes (PROs)). Such information will be clearly delineated as PRO.

D. PDM shall ensure that its system can accept and integrate updates (Patient Data Receipts) from healthcare provider EHRs on an ongoing basis. If SDRs are in place, Patient Data Receipts shall be automatically transmitted from provider EHRs to the PHR at the conclusion of each of Patient's health visits or health encounters.

VIII. Accounting of Disclosures

A. PDM shall maintain a record or log of active SDRs and activity within the Patient's PHR, including updates and disclosures, and shall provide a mechanism by which Patient can ask for additional information about any documented disclosure. Disclosures shall indicate what data was provided, to whom, on what date and time, and the SDR associated with the healthcare provider.

B. PDM shall maintain log entries for a minimum of 7 years from the date of access. Patient retains the right to print or otherwise save the log or information about specific entries at any time.

IX. PHR Security and Restrictions on Use

A. PDM shall not use or further disclose Patient's PHR, either in whole or in part, other than as permitted by this Agreement and as authorized by Patient. [*consider adding here provisions related to law enforcement/access via subpoena and/or court order*]

B. PDM shall use appropriate safeguards to prevent any use or disclosure of Patient's PHR, either in whole or in part, other than as specified in this Agreement and as authorized by Patient. To the extent that PDM receives, maintains, or transmits PHR, PDM shall use appropriate administrative, physical, and technical safeguards that comply with those required by the HIPAA Security Rule and that reasonably and appropriately protect the confidentiality, integrity, and availability of PHR, regardless of whether PDM is a Covered Entity as defined by HIPAA.

C. PDM shall comply with any applicable state and local security and privacy laws to the extent that they are more protective of Patient's privacy than the HIPAA Privacy Rule and the HIPAA Security Rule, regardless of whether PDM is a Covered Entity as defined by HIPAA. If PDM is not a Covered Entity, other federal laws and regulations may apply (e.g., Federal Trade Commission regulations pertaining to health data held by third-party entities not impacted by HIPAA). If PDM offers access to the PHR in a mobile application, Food & Drug Administration rules may also apply. PDM is responsible for ensuring compliance with all applicable law and regulation.

D. Patient shall not share personal login and authentication information for PHR access with anyone. Patient may designate Patient Representative(s) who may access Patient's PHR in Patient's stead, but Patient Representative(s) shall maintain his or her own login and authentication information.

X. Mobile Access to PHR

A. The PHR is an aggregation of Patient's digital health data from various sources, both clinical and non-clinical. PDM may provide various means of PHR access to the Patient, including through mobile applications accessible on a smartphone, smart speaker, or other such electronic device. In such an instance, PDM shall determine whether any such applications meet the Food & Drug Administration's (FDA) definition of a mobile medical application and shall adhere to any additional requirements and guidelines set out by the FDA.

XI. Independence From Provider Medical Records

A. Patient's PHR maintained by PDM is separate and independent from medical records that healthcare providers are required by law to maintain for each patient. Healthcare providers may incorporate information from the PHR into their medical records if the Patient grants them access to the PHR, but the existence of the PHR does not supplant their medical records systems, any reporting responsibilities healthcare providers have under federal, state, or local law, or provide an alternative method for their required maintenance of medical records.

XII. Termination

A. This Agreement shall begin on the Effective Date set forth above and shall continue indefinitely until terminated by either party.

B. Breach of any of the terms of this Agreement may result in immediate termination of the Agreement in some circumstances (e.g., malicious actions, such as attempts to breach security measures, actions that cause substantial harm due to negligence or malfeasance). If the breach results from a mistake or negligence that can be easily remedied without substantial harm to the non-breaching party, the breaching party shall notify the non-breaching party within three (3) business days and take corrective action within a reasonable timeframe as agreed upon by the parties to address the breach. If action is not taken to remedy the breach in a reasonable timeframe, the Agreement shall be terminated. The non-breaching party retains all rights to pursue claims for breach of contract pursuant to the laws of the state of *[Massachusetts]* and any and all other remedies provided pursuant to federal, state, and local law, including HIPAA and Federal Trade Commission regulations.

C. Upon termination by either party, revocations of active SDRs shall be generated by the PDM and submitted to all entities providing data to the PHR on an automatic basis. PDM shall disable the ability of Patient's PHR to receive updates no later than five (5) business days of submitting revocation notices.

  a. Patient understands that SDRs are not transferable to other PDMs and that new forms will need to be completed and submitted to healthcare providers pursuant to the new PDM's policies to authorize automatic updates to the PHR maintained by a new PDM.

D. Patient may terminate this Agreement at any time with written notice to PDM. Upon notice of Patient's desire to terminate the Agreement, PDM shall provide Patient the ability to transfer Patient's PHR and related access logs to another patient data manager of Patient's choosing, to be provided a copy of the PHR for Patient's personal storage, and/or to destroy the PHR data and related access logs. PDM shall provide Patient thirty (30) days to make a decision about disposition of the PHR. Should Patient opt to transfer PHR to another patient data manager, PDM shall assist Patient with the form(s) and process needed to authorize the transfer. PDM shall ensure that the transfer may be effected electronically if Patient so elects and shall be performed expediently and no later than 30 days after Patient notifies PDM of its disposition decision, without undue burden or unreasonable cost.

  a. PDM shall, to the best of its ability, confirm successful transfer of Patient's PHR to a new patient data manager, or the date, time, and method of destruction of Patient's PHR data and access logs, as applicable.

E. PDM may terminate this Agreement with 60 days' notice to Patient and shall require acknowledgement from Patient within five (5) days of such notice to ensure Patient is aware of the impending termination. PDM shall provide Patient with the option to transfer PHR to another patient data manager, to be provided a copy of the PHR for Patient's personal storage, or to destroy the PHR data.

  a. PDM shall, to the best of its ability, confirm successful transfer of Patient's PHR to a new patient data manager, or the date, time, and method of destruction of Patient's PHR data and access logs, as applicable.

F. In the event of Patient's death, PDM shall follow the specific instructions Patient provided at initiation of the PHR. Data will be destroyed or donated to a data repository named by Patient. Patient may request a copy be provided to Patient's named beneficiary prior to disposition.

G. Patient understands and acknowledges that PDM shall not keep a copy of Patient's PHR once an agreement has been terminated, the patient has selected the method of disposition or transfer of the PHR, and the PDM has successfully disposed of or transferred the data. In the event that PDM is the terminating party, Patient shall have one year from the date of termination to determine the method of disposition or transfer. If disposition or transfer does not occur within that year, PDM shall then destroy the data.

XIII. Modifications to Terms of Agreement

A. This Agreement may be updated or amended due to changes in law, regulations, policies, or for other reasons. Parties to this Agreement will be alerted to any such updates or amendments a minimum of 30 days prior to implementation.

B. Neither party shall assign this Agreement without the written consent of the other.

____ ______________________
Patient Date

____ ______________________
XXXX, on behalf of PDM Date