Firma Clinical Research EU-US Privacy Shield and Swiss-US Privacy Shield Privacy Policy

Privacy Shield Frameworks

H2O Clinical, LLC and its U.S.-based entity Pharma Start, LLC, collectively doing business as **Firma Clinical Research** ("Firma" or "we"), comply with the EU-U.S. Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from European Union member countries ("EU"), European Economic Area ("EEA"), and Switzerland to the United States. Firma Clinical Research has certified that it adheres to the Privacy Shield Principles. If there is any conflict between the policies in this Privacy Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov/.

Definitions

Client" or "Sponsor" means an entity that contracts with Firma Clinical Research to provide contract research organization services for clinical research studies sponsored by such entities and that involve the transfer, processing, or reporting of Personal Information for or on behalf of and under the instructions of such entity.

"Personal Data" or "Personal Information" means *any information relating to an identified or identifiable natural person ('data subject')*" and that is transferred from the EU/EEA or Switzerland. An "identifiable person" is "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity."

"Sensitive Personal Information" means Personal Information that reveals race, ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or that concerns the health or sex life of an individual and for purposes of compliance with the Swiss – U.S. Privacy Shield Framework, includes ideological views or activities, information on social security measures or administrative or criminal proceedings and sanctions, which are treated outside pending proceedings.

"Subcontractor" means any individual, corporation, or other entity under written contract with Firma Clinical Research to assist Firma Clinical Research in fulfilling its responsibilities under its contracts with Sponsors. "Subcontractor" includes home health providers that contract with Firma Clinical Research to provide remote health research study visits.

About Firma Clinical Research

Firma Clinical Research is a contract research organization ("CRO") that performs biostatistics, data management, medical writing, clinical operations, including home health research study visits, and clinical pharmacology in support of specific medical or pharmaceutical research studies ("Clinical Studies"). Firma Clinical Research performs such clinical research support services on behalf of its Clients, who sponsor the Clinical Studies. Firma Clinical Research's contracts with its Clients specify the terms and conditions under which Firma Clinical Research may process and transfer Personal Information, including Sensitive Information, as part of its CRO services ("Clinical Study Contracts"). Firma Clinical Research processes and transfers Personal Information as authorized and permitted by, and to perform its obligations under, the Clinical Study Contracts, or as required by law. To perform its CRO services, Firma Clinical Research receives and processes Personal Information, including Sensitive Information on individuals who are participating as subjects in the Clinical Studies in EU/EEA countries, as well as in Switzerland. Firma Clinical Research may also receive and process anonymized ("key-

coded") data on subjects who participate in Clinical Studies in EU/EEA countries as well as in Switzerland. In addition, Firma Clinical Research obtains Personal Information about home health providers with whom it contracts to credential specific home health providers to provide the remote site visits. The purpose for which Firma Clinical Research collects, processes and transfers Personal Information, including key-coded data and the Personal Information about home health providers, is to support Clinical Studies in which the individual study subjects participate, including to record and summarize the data collected in these Clinical Studies, as directed by the Sponsors.

This Privacy Policy, reflecting Firma Clinical Research's compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework, will summarize Firma Clinical Research's practices with respect to any Personal Information that may be transferred to Firma Clinical Research from the EU/EEA or Switzerland.

- The following is a summary of Firma Clinical Research's management of Personal Information in accordance with the Privacy Shield Privacy Principles. The complete text of these Principles is given in Appendix 1 of this Privacy Policy.

  Notice: Firma Clinical Research obtains Personal Information in its role as a data processor, which is defined as "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller." Any Personal Data that Firma Clinical Research receives from the EU/EEA and Switzerland is data that Firma Clinical Research obtains to provide services to its Clients as the Sponsors of the Clinical Studies. Our Clients are the data controllers, and as such, are responsible for directing us to process Personal Information we obtain on their behalf in accordance with the rights and requirements of the individuals concerned under European data protection law. Firma Clinical Research does not process Personal Information covered by this Privacy Policy for purposes outside the scope of providing services to the Sponsors, or as required by law.

  In its role as a CRO service provider to Sponsors, Firma Clinical Research may be assigned the responsibility to collect Personal Information directly from study subjects, study investigators, home health providers or other sources in the EU or Switzerland or Firma Clinical Research may receive such Personal Information directly from the Sponsor, which is the entity that possesses the legal authority necessary for the conduct of the Clinical Studies. Providing the study subjects with Notice as required under the Privacy Shield Principles is under the Sponsors' control. Sponsors provide such Notice through the Clinical Study informed consent process, which describes the purposes for which the Personal Data are collected and used and the third parties to which the Personal Data is disclosed. Firma Clinical Research provides Notice as required under the Privacy Shield Principles to the home health providers at the time it collects their Personal Information and by posting this Privacy Policy on its publicly website available at http://www.firmaclinicalresearch.com/.

  If in the future Firma Clinical Research acts as a data controller for EU/EEA/Swiss data, it will comply with the Privacy Shield privacy principles for Notice and will amend the policy accordingly.

  - **Choice:** The Clinical Study Sponsors, as the data controllers, direct Firma Clinical Research in providing study subjects with their right to choice. The Sponsors are responsible and will direct Firma Clinical Research to provide study subjects the choice whether their Personal Information is to be disclosed to a third party and the choice whether their Personal Information is to be used for a purpose other than the

purpose for which it was originally collected or subsequently authorized by the individual. Similarly, for Sensitive Personal Information, the Sponsors are responsible for and will direct Firma Clinical Research to give individuals the opportunity to affirmatively or explicitly choose to allow the disclosure of their Sensitive Personal Information for a purpose other than the purpose for which it was originally collected or to be disclosed to a third party. Firma Clinical Research provides the home health providers with their right to choice and will provide them with the choice to whether their Personal Information is to be disclosed to a third party and the choice to whether their Personal Information is to be used for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual, and for Sensitive Information will obtain their explicit consent for such use or disclosure. Requests to opt out of such uses or disclosures may be sent to the Chief Privacy Officer at privacy@firmaclinical.com, or at the following address:

Firma Clinical Research, LLC
Attn: Chief Privacy Officer
224 Schilling Circle, Suite 1888
Hunt Valley, MD 21031

If in the future Firma Clinical Research acts as a data controller for EU/EEA/Swiss data, it will comply with the Privacy Shield privacy principles for Choice and will amend the policy accordingly.

- **Accountability for Onward Transfer:** Firma Clinical Research does not disclose Personal Data to third parties except in accordance with the Privacy Shield Principles, including as required by law. Firma Clinical Research may transfer Personal Information to the Sponsors and to the Principal Investigator pursuant to the Clinical Study Contracts and in accordance with the Privacy Shield privacy principles. Firma Clinical Research may transfer Personal Information to its Subcontractors as necessary to perform its CRO services for Sponsors and only as authorized by its Clinical Study Contracts with Sponsors. When Personal Information will be disclosed to a Subcontractor to perform task(s) on behalf of and under Firma Clinical Research's instructions, Firma Clinical Research will transfer the information only if Firma Clinical Research enters a written agreement with the Subcontractor requiring that Subcontractor to provide at least the same level of privacy protection to the Personal Information as is required by the relevant Privacy Shield Principles. If Firma Clinical Research learns that a Subcontractor is using or disclosing Personal Data in a manner contrary to this Privacy Policy and the Privacy Shield Principles, Firma Clinical Research will take reasonable steps to prevent or stop such processing. If Firma Clinical Research discloses Personal Information to its Subcontractors, then Firma Clinical Research will potentially be liable for the acts or omissions of such Subcontractors' if they process the Personal Information in violation of the Privacy Shield Principles.

- **Data Security:** Firma Clinical Research has implemented physical, electronic, and administrative measures, including procedural and managerial security measures to protect Personal Information from loss, misuse and unauthorized access, disclosure alteration and destructions. Employees who may access such Personal Information receive training on this Privacy Shield policy and are held responsible for compliance to it, with disciplinary action for non-compliance.

- **Data Integrity and Purpose Limitation:** As a processor on behalf of its Clients, Firma Clinical Research processes Personal Information only in a manner that is consistent with

its obligations to the Sponsors under Clinical Study Contracts. To the extent necessary and appropriate for those purposes, Firma Clinical Research takes reasonable steps to ensure that Personal Information is accurate, complete, current and reliable for its intended use. Firma Clinical Research collects Personal Information covered by this Privacy Policy that is relevant for the purposes of processing and does not process such Personal Information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individuals who are the subjects of the Personal Information. Firma Clinical Research also takes reasonable and appropriate steps to comply with the requirement under the Privacy Shield to retain Personal Information in identifiable form only for as long as it serves a purpose of processing, which includes Firma Clinical Research's obligations under its Clinical Study Contracts and its own business purposes, and Firma Clinical Research adheres to the Privacy Shield Principles for as long as it retains such Personal Information.

- **Access:** Firma Clinical Research acknowledges the individuals' right to access their personal information. For Firma Clinical Research to provide such access to an individual who is a study subject, the relevant data controller (Firma Clinical Research's Client) would need to confirm that the individual is who he/she claims to be. Participants in "blinded" clinical trials do not have to be provided access to the data on their treatment during the trial if this restriction has been explained when the participant entered the trial and the disclosure of such information would jeopardize the integrity of the research effort.
  - Consistent with the fundamental nature of access, Firma Clinical Research will always make a good faith effort to provide access. If individuals communicate their intention to access, correct, or delete their personal data to the data controllers who are our Clients, and our Clients inform Firma Clinical Research of such individuals' requests, then Firma Clinical Research will, as required, provide these individuals with these rights. Firma Clinical Research provides the home health providers with their right to access their Personal Information covered by this Privacy Policy and to correct, amend, or delete such Personal Information if it is inaccurate or has been processed in violation of the Privacy Shield Principles. Requests for such access, correction, amendment, or deletion should be sent to the Chief Privacy Officer at privacy@firmaclinical.com, or at the following address:

    Firma Clinical Research, LLC
    Attn: Chief Privacy Officer
    224 Schilling Circle, Suite 1888
    Hunt Valley, MD 21031

- **Recourse, Enforcement and Liability:** There are three necessary components to compliance with this Privacy Shield privacy principle:
  - **Independent recourse mechanism:** In compliance with the Privacy Shield Principles, Firma Clinical Research commits to resolve complaints about your privacy and our collection or use of your Personal Information. European Union or Swiss individuals with inquiries or complaints regarding this privacy policy should first contact Firma Clinical Research at: privacy@firmaclinical.com, or at the following address:

    Firma Clinical Research, LLC
    Attn: Chief Privacy Officer
    224 Schilling Circle, Suite 1888
    Hunt Valley, MD 21031

Firma Clinical Research has further committed to refer unresolved privacy complaints under the Privacy Shield Principles to BBB EU PRIVACY SHIELD, a non-profit alternative dispute resolution provider located in the United States and operated by the Council of Better Business Bureaus. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit www.bbb.org/EU-privacy-shield/for-eu-consumers/ for more information and to file a complaint.

Finally, as a last resort and under limited circumstances, individuals whose complaints have not been satisfied may seek recourse before the Privacy Shield Panel, a binding arbitration mechanism.

- **Verification**: Firma Clinical Research uses a self-assessment approach. Firma Clinical Research verifies that:
  - Its published Privacy Policy regarding Personal Information received from the EU/EEA and Switzerland is accurate, comprehensive, prominently displayed, completely implemented and accessible.
  - Its Privacy Shield Privacy Policy conforms to the Privacy Shield privacy principles.
  - Through its Privacy Shield Privacy Policy, individuals are informed of any in-house arrangements for handling complaints and of the independent mechanisms through which they may pursue complaints.
  - It has in place procedures for training employees in its implementation, and disciplining them for failure to follow it.
  - It has in place internal procedures for periodically conducting objective reviews of compliance with the above.
  - A statement verifying the self- assessment will be signed by the Firma Clinical Research Chief Privacy Officer, an authorized representative of the organization, at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about non-compliance.
- **Remedy**: Firma Clinical Research's commitment to the independent recourse mechanism of the BBB EU Privacy Shield Program includes its commitment to remedies that arise from dispute resolution carried out by that entity.
  - Firma Clinical Research is potentially liable in cases of onward transfer of Privacy Shield Personal Data to third parties.
  - Firma Clinical Research is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

- **Limitations:** Adherence by Firma Clinical Research to the Principles (and this Privacy Shield Policy) will be limited as explicitly permitted by the Principles: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; or (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, Firma Clinical Research's non-adherence is limited to the extent necessary to meet the overriding legitimate interests. Where the option is allowable under the Principles and/or U.S. law, Firma Clinical Research will opt for the higher protection where reasonably possible.
- **Amendments**: This Firma Clinical Research, LLC Privacy Shield Privacy Policy may be amended from time to time consistent with the requirements of the Privacy Shield. Firma Clinical Research will post any revised policy on this website.

Appendix 1: Privacy Shield Privacy Principles

1. **NOTICE**
   a. An organization must inform individuals about:
      i. its participation in the Privacy Shield and provide a link to, or the web address for, the Privacy Shield List,
      ii.. the types of personal data collected and, where applicable, the entities or subsidiaries of the organization also adhering to the Principles,
      iii. its commitment to subject to the Principles all personal data received from the EU and Switzerland in reliance on the Privacy Shield,
      iv. the purposes for which it collects and uses personal information about them,
      v. how to contact the organization with any inquiries or complaints, including any relevant establishment in the EU or Switzerland that can respond to such inquiries or complaints,
      vi. the type or identity of third parties to which it discloses personal information, and the purposes for which it does so,
      vii. the right of individuals to access their personal data,
      viii. the choices and means the organization offers individuals for limiting the use and disclosure of their personal data,
      ix. the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, and whether it is: (1) the panel established by DPAs, (2) an alternative dispute resolution provider based in the EU, or (3) an alternative dispute resolution provider based in the United States,
      x. being subject to the investigatory and enforcement powers of the FTC, the Department of Transportation or any other U.S. authorized statutory body,
      xi. the possibility, under certain conditions, for the individual to invoke binding arbitration,
      xii. the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and
      xiii. its liability in cases of onward transfers to third parties.

      This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.
2. **CHOICE**
   a. An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.
   b. By derogation to the previous paragraph, it is not necessary to provide choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. However, an organization shall always enter into a contract with the agent.
   c. For sensitive information (i.e., personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), organizations must obtain affirmative express consent (opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt- in choice. In addition, an organization should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.

3. **ACCOUNTABILITY FOR ONWARD TRANSFER**
   a. To transfer personal information to a third party acting as a data controller, organizations must comply with the Notice and Choice Principles. Organizations must also enter into a contract with the third-party data controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles.
   b. To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized processing; and (v) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.
4. **SECURITY**
   a. Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.
5. **DATA INTEGRITY AND PURPOSE LIMITATION**
   a. Consistent with the Principles, personal information must be limited to the information that is relevant for the purposes of processing. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. An organization must adhere to the Principles for as long as it retains such information.
6. **ACCESS**
   a. Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.
7. **RECOURSE, ENFORCEMENT AND LIABILITY**
   a. Effective privacy protection must include robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include:
      i. readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by reference to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide;
      ii. follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of non-compliance; and
      iii. obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.
   b. Organizations and their selected independent recourse mechanisms will respond promptly to inquiries and requests by the Department for information relating to the Privacy Shield. All organizations must respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State authorities through the Department. Organizations that have

chosen to cooperate with DPAs, including organizations that process human resources data, must respond directly to such authorities with regard to the investigation and resolution of complaints.

c. Organizations are obligated to arbitrate claims and follow the terms as set forth in Annex I, provided that an individual has invoked binding arbitration by delivering notice to the organization at issue and following the procedures and subject to conditions set forth in Annex I.
d. In the context of an onward transfer, a Privacy Shield organization has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. The Privacy Shield organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage.
e. When an organization becomes subject to an FTC or court order based on non-compliance, the organization shall make public any relevant Privacy Shield- related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality requirements. The Department has established a dedicated point of contact for DPAs for any problems of compliance by Privacy Shield organizations. The FTC will give priority consideration to referrals of non-compliance with the Principles from the Department and EU Member State authorities, and will exchange information regarding referrals with the referring state authorities on a timely basis, subject to existing confidentiality restrictions.