US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/07/2025

OPDIV:

NIH

Name:

Framingham Heart Study

PIA Unique Identifier:

P-4907704-268849

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

Does the system include a Website or online application available to and for the use of the general public?

Yes

Identify the operator.

Contractor

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

No

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The Framingham Heart Study (FHS) is a scientific resource for the research community to expand knowledge about the determinants of health and disease in heart, lung, blood, and sleeping disorders. The overall goals of this acquisition are to (1) enhance statistical power to perform analyses of predictors of clinical events; (2) study the progression of risk factors with aging; and (3) identify new risk factors or interactions between risk factors that inform disease patho-physiology and/or disease progression.

Describe the type of information the system will collect, maintain (store), or share.

FHS collects the following information from our participants: Social Security Number (SSN), Name, Mother’s Maiden Name, E—mail Address, Phone Numbers,Medical Notes, Date of Birth, Biometric Identifiers, Mailing Address, Medical Records Number, Device Identifiers, Medical Images and scans, Voice and Audio Recordings, Centers for Medicare & Medicaid Services data, Geocodes, and Genomic information.

FHS users authenticate their access to the system by providing a valid username and password combination.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

FHS is a scientific resource for the research community to expand knowledge about the determinants of health and disease in heart, lung, blood, and sleeping disorders. The overall goals of this acquisition are to (1) enhance statistical power to perform analyses of predictors of clinical events; (2) study the progression of risk factors with aging; and (3) identify new risk factors or interactions between risk factors that inform disease patho-physiology and/or disease progression.

FHS collects the following information from our participants: SSN, Name, Mother's Maiden Name, E—mail Address, Phone Numbers,Medical Notes, Date of Birth, Biometric Identifiers, Mailing Address, Medical Records Number, Device Identifiers, Medical Images and scans, Voice and Audio Recordings, CMS data, Geocodes, and Genomic information.

FHS users authenticate their access to the system by providing a valid username and password combination.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Social Security Number
Date of Birth
Biometric Identifiers
Mother's Maiden Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Device Identifiers
Medical images and scans
Voice and audio recordings
CMS data
Geocodes and genomic data
usernames and passwords

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Public Citizens
Patients

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

Personally Identifiable Information (PII) is primarily collected and regularly updated so that FHS can maintain contact with participants for the duration of their participation in the study.

Describe the secondary uses for which the PII will be used.

PII is also used for the purpose of collecting annual medical history updates from participants and

recruiting them for participation in ongoing and new research activities.

Identify legal authorities governing information use and disclosure specific to the system and program.

42 USC § 285b, 241, 282, and 284

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-25-0200, Clinical, Basic and Population-based Research Studies of the National Institutes of

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Online

Government Sources

Within HHS

Other HHS OpDiv

State/Local/Tribal

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

OMB information collection approval number and expiration date are not applicable. Public Law 114-255, Section 2035, exempts research conducted by NIH from Paperwork Reduction Act (PRA) requirements.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

Prior to sharing any study participant PII, FHS and the recipient organization must enter into a Data and Materials Distribution Agreement (DMDA). The agreement must be signed by a qualified individual at both organizations before any PII can be shared with the recipient. DMDA's have a start and end date, and the scope of data sharing is well defined.

Describe the procedures for accounting for disclosures.

Investigators that would like to conduct research using existing FHS data and/or collect new data from participants are required to submit a detailed research application to FHS, receive approval from all applicable review committees, and establish DMDAs (if PII will be shared), before data will be released.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Every time participants are asked to participate in a study and provide PII to FHS or other researchers, they go through the informed consent process and sign the consent document that is approved by the Institutional Review Board charged with study oversight.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

All research study consent documents clearly state that participants can refuse to share information they do not wish to share. Participants are also informed of their right to withdraw consent for their data to be used or shared, and/or to withdraw from the study completely, at any time, and provided the information on how to do so.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

All conditions for the collection, use, storage and sharing of PII, agreed to by participants, as indicated by signing an FHS informed consent document, will be adhered to until the next time they are invited to continue their participation and sign a new FHS consent document. If major changes are made to how PII are handled, but a participant has not signed a consent document that describes the changes, the changes will not be applied to the individual participant's PII.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

Every study informed consent document provides the name and contact information for individuals/parties that are responsible for study oversight and who can be contacted to report any suspected misconduct. These include the FHS Principal Investigator, the National Heart, Lung, and Blood Institute point of contact for FHS, and the Boston Medical Center and Boston University Medical Campus Institutional Review Board (IRB).

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

Study participants are contacted annually to provide a medical history update, and at that time, they are also asked to provide updated PII/contact information. They are also asked to provide an update any time they are contacted and invited to be in a new study.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Users are granted access to PII based on the roles and responsibilities of their position.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Determinations are made based on role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

Per NIH policy, all staff are required to successfully complete annual security awareness training. Training is completed on the http://irtsectraining.nih.gov site.

All potential users of Patient Tracking System (PTS) (and staff accessing paper medical records that may include PII) are required to complete a 30-minute electronic training called, "Online FHS

Research Records Security Training", that was developed by the manager of the FHS Health Information Management department. Testing must be completed at the end of the training and a score of 85% must be attained before access to PTS is granted. In addition, users must sign the "FHS Electronic and Paper Research Records Protocol and Agreement" after completing the training.

Describe training system users receive (above and beyond general security and privacy awareness training).

In addition to the training described in question 34 above, users must undergo hands-on training of the proper and efficient use of PTS, provided by the FHS Recruitment Team Manager. Following completion of this training, the manager notifies the PTS Administrator that access for the user can be granted.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

03-005, Patient Medical Records. Cut off patient case file annually after 5 years of inactivity. Destroy when case file is no longer needed for scientific reference (Disposition Authority: DAA-0443-2012-0010)

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative Controls: PII is protected by ensuring all necessary approvals and agreements are in place before data is released, requiring personnel to complete training, and releasing only the minimum amount of data necessary for research.

Technical Controls: Determinations are made using role-based access controls and the principle of least privilege, with user rights provisioned based on system controls, allowing access only to the minimum amount of PII necessary for users to perform their job.

Physical Controls: Data is stored on servers in an on-site data center with locked doors, accessible only to two authorized individuals. Visitors are required to sign in when entering the data center.

Identify the publicly-available URL:

https://www.framinghamheartstudy.org/

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

Yes

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

No