Vital Records Data Use Agreement

Background and Purpose

The Bureau of Vital Statistics at the Florida Department of Health (DOH) may release vital records data to entities with an approved Vital Records Data Use Agreement (Data Use Agreement) for purposes authorized by section 382.025, Florida Statutes. All persons with data access must sign the Data Use Agreement outlining the terms and conditions for using vital records data. A data use agreement is specific to the individual project and all projects require annual review.

The Bureau of Vital Statistics at the DOH conducts a detailed review of every application for access to vital records data and makes a determination on a case by case basis. Requests for confidential data will be granted only if the project meets the statutory criteria, the criteria above, and the project cannot be reasonably completed with de-identified information.

Approved applicants are held to the highest ethical standards and must agree to the stipulations detailed in the Data Use Agreement.

Return application to:
Bureau of Vital Statistics
Florida Department of Health
Attn: Gary Sammet
1217 N. Pearl Street
Jacksonville, FL 32202

Vital Records Data Use Agreement

Date:

I. Project Director Information

Name of Requestor:

Title:

Requestor's Organization/Agency:

Mailing Address:

Telephone Number:

Fax Number:

E-Mail Address:

Contact Person (if different from Project Director):

Contact Person's Telephone Number:

Contact Person's E-Mail Address:

Does this application update a previous Data Use Agreement? ☐ **Yes** ☐ **No**

If yes, provide Study Number of previous Data Use Agreement:

II. Project Summary

Provide a brief title for your project or study:

Purpose of the Project: (Provide detailed explanation)

Intended Use of the Data: (Provide detailed information)

Please describe your plan for the release of results, including plans for public dissemination, if any:

The publication must cite the DOH as the data source. A disclaimer must also be included that "any published findings and conclusions are those of the authors and do not necessarily represent the official position of the Florida Department of Health."

The Project Director is the Data Custodian for this project; however, there are some circumstances which may allow another person to be the Data Custodian.

[The Data Custodian is responsible for observance of all conditions of use and for establishment and maintenance of physical and electronic security arrangements to prevent unauthorized use. This individual must have the legal authority to keep the information confidential and maintain confidentiality. If the custodian is changed, the organization must promptly notify the DOH Division of Public Health Statistics and Performance Management.

Are you the Data Custodian for this project? ☐ **Yes** ☐ **No**

If no, please indicate the name of the Data Custodian and their relationship to the requestor's organization:

Is the requested data needed for work being performed under contract with the DOH? ☐ **Yes** ☐ **No**

If yes, then please provide the DOH contract manager's name:

III. Data Requested and Specifications

Data Requested

- ☐ Birth
- ☐ Fetal Death
- ☐ Death with cause-of-death
- ☐ Death without cause-of-death
- ☐ Marriage
- ☐ Dissolution of Marriage

Data Specifications

- ☐ Years (Specify)
- ☐ Statewide Data
- ☐ County Only (Specify)

Data Format

- ☐ Photocopies
- ☐ Electronic Transfer (Secure FTP)

IV. Variables and/or Linking (Matching) of Data

List the specific variable names being requested here or in an attachment to the data use agreement :

Will the data requested be linked or matched with any other data sources ? ☐ **Yes** ☐ **No**

If yes, describe in detail any linking of requested vital statistics data with any other data sources. Specify the data sources, the variables which will be used for linking, (SSN, name, etc.), and which variables will be kept in the linked file.

If the applicant will be linking the data, provide a detailed description of the linking methodology to be used. If the requestor will need DOH to match or link records, describe how the data needing to be matched or linked will be provided.

V. Security and Confidentiality

The release of information that may lead to the identification of individuals or be traced back to an individual record is prohibited. However, statistical and research results based on the data provided by the Bureau of Vital Statistics pursuant to this Agreement may be released. Any person(s) who access, disclose or use personally identifiable information in a manner or for a purpose not authorized by this agreement may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

Only the listed Data Custodian or authorized users listed on this agreement may access data. Describe where data will be stored and how data will be accessed by authorized users.

Do you agree to each of the following requirements?

1) The files will be used only to accomplish the research project described in this agreement. ☐ Yes ☐ No
2) These files, or any files extracted or derived from them, will not be released to other organizations or individuals who have not been named in this agreement. ☐ Yes ☐ No
3) No attempt will be made to link information from any other source to records for specific individuals for whom records are included in these files, unless authorized by this agreement. ☐ Yes ☐ No
4) No listing of information from individual records, with or without identifiers, will be published or otherwise released. ☐ Yes ☐ No
5) No statistical tabulations or research results will be released which reveal information about identifiable individuals. ☐ Yes ☐ No
6) Statistical and research results derived from these files may be published. However, no results may be copyrighted by the author without the permission of the Bureau of Vital Statistics. ☐ Yes ☐ No

VI. Data Destruction Schedule

Consistent with Florida law, applicants must make provisions for the destruction of records at the conclusion of their project, or when the data is no longer required. Maintaining the privacy of the individuals whose personal information is included in vital records is required to preserve the integrity of the data sharing process.

Please detail the manner and timeline for destruction. If you are following a data destruction policy set by your organization or agency, please attach that policy to your application.

VII. Data Use by Others

Will any sub-contractors affiliated with this project use the data during the course of the project?
☐ Yes ☐ No

If yes, each sub-contractor or other individual will need to complete a separate Data Use Agreement. Please identify the individuals of the sub-contractor who will have access or be using the data and describe the work they will perform.

VIII. Fees

Prior to generating the data, the DOH will provide an estimate of the costs incurred in its preparation. Once the request is approved and payment received, the data will be provided. A waiver or reduction of the fees authorized by section 382.0255(1), Florida Statutes, will be considered only if the intended use of the data will have a direct health-related benefit to Florida citizens. If a waiver or reduction of the fees is requested, describe how use of the data is a direct benefit to Florida citizens.

IX. Contact with Human Subjects

No contacts of any kind can be made with any person named on a certificate or data file or related persons without the written permission of the Bureau of Vital Statistics and review by the DOH Institutional Review Board (IRB). If the project requires DOH IRB review, applicants must first submit a signed and notarized Data Use Agreement along with the protocol for review to the Bureau of Vital Statistics. A Data Use Agreement may be rejected if the research protocol involves intrusive follow-back of research subjects.

Will the project involve direct contact with individuals or establishments mentioned on the record?
☐ **Yes** ☐ **No**

If so, describe the need for such activity and the types of individuals or establishments who will be contacted.

X. All Staff Accessing the Information

List name, title, affiliation and role in this project for each authorized user:

XI. Use and Consent of the Data

Vital records data may only be used for the specific purpose(s) described in this agreement. All persons with data access must maintain the confidentiality of the data and prevent release to unauthorized parties. All publications, tabular presentations, maps or depictions of cartographic information must aggregate results to protect the identity

of individuals and comply with applicable state and federal laws. The Division of Public Health Statistics and Performance Management, Bureau of Community Health Assessment, Section of Public Health Reporting shall be notified immediately by phone (850-245-4037) after discovery of any use or disclosure of the data not provided for by this agreement.

As the signatory for this agreement as the Data Custodian, the Data Custodian bears full responsibility for adhering to all data confidentiality, security policies, and the terms of this agreement. The Data Custodian serves as the point of contact for receiving, maintaining, protecting, and ultimately destroying the data provided by DOH. Data may be used by the custodian only for the purpose stated in this agreement and may not be used for any other purpose. No entity with data access may link vital records data with any other source of information without the written authorization of the Bureau of Vital Statistics. Additionally, proper physical, computer and system security safeguards will be maintained by the signatory's requestor's organization/agency pursuant of the agreement.

Physical Security

The requestor's organization shall ensure that DOH data are used and stored in an area that is physically safe from access by unauthorized persons during working hours and non-working hours. The requestor's organization agrees to safeguard DOH data from loss, theft, or inadvertent disclosure and, therefore, agrees to:

1. Secure all areas of the organization's facilities where employees assist in the administration of the program's use or disclose DOH data. Ensure that authorized individuals only access these secure areas with properly coded key cards, authorized door keys or access authorization; and access to premises is by official identification.

2. Issue identification badges to workers who assist in the administration of the organization's programs and require the organization's workers to wear these badges at organization's facilities where DOH data are stored and used.

3. Store paper records with DOH data in locked spaces, such as locked file cabinets, locked file rooms, locked desks, or locked offices in facilities which are multi-use, meaning that where the requestor's organization and non-requestor's organization functions in one building in work areas that are not securely segregated from each other.

4. Use all reasonable measures to prevent non-authorized personnel and visitors from having access to, control of, or viewing DOH data.

Computer Security Safeguards

The requestor's organization agrees to comply with the general computer security safeguards, system security controls, and audit controls in this section.

General Computer Security Safeguards:

1. Encrypt portable computer devices, such as but not limited to, laptops and notebook computers, that process and/or store DOH data with an encryption solution that is full-disk utilizing a minimum algorithm of 256 bit AES or 3DES (Triple DES) if AES is unavailable.

2. Encrypt workstations where DOH data are stored using an encryption product that utilizes a minimum algorithm of 256 bit AES, or 3DES (Triple DES) if AES is unavailable, and is recognized as an industry leader in meeting the needs for the intended solution.

3. Ensure that only the minimum necessary amount of DOH data is downloaded to a laptop or hard drive when absolutely necessary for current business purposes.

4. Encrypt all electronic files that contain DOH data when the file is stored on any removable media type device (i.e., USB thumb drives, floppies, CD/DVD, portable hard drives, etc.) using an encryption product that utilizes a minimum algorithm of 256 bit AES, or 3DES (Triple DES) if AES is unavailable, and is recognized as an industry leader in meeting the needs for the intended solution.

5. Ensure that all emails sent outside the requestor's organization's e-mail environment that include DOH data are sent via an encrypted method using an encryption product that is recognized as an industry leader in meeting the needs of the intended solution.

6. Ensure that all workstations, laptops and other systems that process and/or store DOH data have a commercial third-party anti-virus software solution and are automatically updated when a new anti-virus definition/software release is available.

7. Ensure that all workstations, laptops and other systems that process and/or store DOH data have current security patches applied and are up-to-date.

8. Ensure that all DOH data are wiped from all systems and backups when the data is no longer legally required. The requestor's organization shall ensure in writing that the wipe method conforms to the US Department of Defense standards for data destruction.

9. Ensure that any remote access to DOH data are established over an encrypted session protocol using an encryption product that is recognized as an industry leader in meeting the needs of the intended solution. The requestor's organization shall ensure all remote access is limited to the minimum necessary and maintains the principles of least privilege.

System Security Controls

In order to comply with the following system security controls, requestor's organization agrees to:

1. Ensure that all systems containing DOH data provide an automatic timeout after no more than 15 minutes of inactivity.

2. Ensure that all systems containing DOH data display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only. Users shall be directed to log off the system if they do not agree with these requirements.

3. Ensure that all systems containing DOH data log successes and failures of user authentication and authorizations granted. The system shall log all data changes and system accesses conducted by all users (including all levels of users, system administrators, developers, and auditors). The system shall have the capability to record data access for specified users when requested by authorized management personnel. A log of all system changes shall be maintained and be available for review by authorized management personnel.

4. Ensure that all systems containing DOH data uses role-based access controls for all user authentications, enforcing the principle of least privileges.

5. Ensure that all data transmissions over networks outside of the requestor's organization's control are encrypted end-to-end using an encryption product that is recognized as an industry leader in meeting the needs for the intended solution when transmitting DOH data. Encrypt DOH data at the minimum of 256 bit AES or 3DES (Triple DES) if AES is unavailable.

6. Ensure that all systems that are accessible via the Internet or store DOH data interactively use a comprehensive third-party real-time host-based intrusion detection and prevention program or are protected at the perimeter by a network based IDS/IPS solution.

Any failure of persons listed in this agreement to abide by the terms of this agreement constitutes a breach and may result in legal action and/or the demand for immediate return of all data obtained hereunder and the destruction under the supervision of the DOH of all copies of the data in the requestor's, the organization's, employees, agents, assigns, or subcontractor's possession. All actions brought under this agreement will be in the State of Florida. In any action brought by the DOH under this agreement in which the DOH prevails, the DOH shall be entitled to its attorney's fees and court costs.

***** All persons who come in direct contact with vital statistics data are required to sign this agreement. If additional signatures are required, please provide them on the last page of this agreement.**

Project Director's Name (Please Print):

Project Director's Signature (Notarization Required):

_____

Attest (If applicant is a corporation): _____
(As Corporate Secretary)

Subscribed and sworn before me _____this_____day of _____, 20_____.

Notary Public, State of _____
Notary Public Signature (Affix Notary Stamp)

FOR OFFICE USE ONLY

Fees Waived: Yes ☐ No ☐ Fees Reduced: Yes ☐ No ☐

DOH IRB Recommendation: Yes ☐ No ☐

Florida Department of Health Reviewers:

_____ **(Reviewer 1)**

_____ **(Reviewer 2)**

Florida Department of Health Authorization:

_____ _____
Ken Jones **Date**
State Registrar/Bureau Chief
Bureau of Vital Statistics

This agreement shall expire one year from the date above. If the agreement is not renewed, all vital records data must be handled in accordance with the Data Destruction Plan .

Vital Records Data Use Agreement

Signatures below, by individuals who will access vital records data as authorized users, acknowledging agreement to the terms of this Data Use Agreement.

Name
(Please Print)

Signature:_____

Name:
(Please Print)

Signature:_____

Name:
(Please Print)

Signature:_____

Name:
(Please Print)

Signature:_____

Name:
(Please Print)

Signature:_____