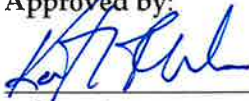



District of Columbia Department of Health <h2 style="color: #0056b3;">Vital Records Confidentiality</h2>		PROCEDURE 1129.000 Implementing Office: Center for Policy Planning and Evaluation/Vital Records Division Training Required: Yes Originally Issued: JUN 15 2022 Revised/Reviewed:
Approved by:  LaQuandra S. Nesbitt MD, MPH; Agency Director	Review by Legal Counsel:  Phillip Husband, Esq.; General Counsel	Effective Date: JUN 15 2022 Valid Through Date: JUN 15 2025

I. Authority	Reorganization Plan No. 4 of 1996; Mayor’s Order 1997-42; The Vital Records Modernization Act of 2018, D.C. Law 22-189, D.C. Official Code §7-231.
II. Reason for the Policy	<p>The DC Health Vital Records Division (DCVRD or “the Division”) within the Center for Policy Planning and Evaluation (CPPE) has jurisdiction over District of Columbia birth, death, fetal death, induced termination of pregnancy and domestic partnership records. District laws and regulations establish authority for the Registrar to certify vital records and issue certificates.</p> <p>DCVRD manages large complex datasets containing Personally Identifiable Information (PII) including demographic and medical information. It is imperative that these data be protected from accidental or malicious disclosure. Protocols are necessary to ensure that PII is fully secure.</p>
III. Applicability	This document shall apply to all DC Health employees, vendor staff, contract employees, interns, employees of other DC government agencies temporarily assigned to DC Health who are assigned to DCVRD or whose assignment affords access to information in vital documents. These individuals are referred to collectively herein as “employees” or “DCVRD employees.”

IV. Policy Statement

The State Vital Records Registrar (“the Registrar”) is the Program Manager over DCVRD. They are the accountable manager for safeguarding the security and confidentiality of vital records data.

All datasets in the DCVRD portfolio are considered PII, and are subject to the safeguards laid out in SOP 701.000 Access Control. VRD datasets may only be considered not PII if they are fully deidentified and/or aggregated such that no specific data may be attributable to a specific person. This includes applying all data suppression thresholds to which the data is legally or ethically subject.

At the time of hire, all DCVRD employees must complete confidentiality training, as well as complete and sign a DCVRD Confidentiality Agreement as a condition of receiving access to DCVRD databases and applications containing PII. The confidentiality training will include, at a minimum, the following content:

1. All protocols regarding entitlement and identity verification to mitigate the risk of unlawful or otherwise inappropriate issuance of a vital record (see SOP 1127.000 Vital Records Entitlement and Identity Verification);
2. Protocols for serving customers who request information including, but not limited to, requests by phone or email, to mitigate the risk of unlawful or otherwise inappropriate disclosure of PII;
3. Practical steps to mitigate the risk of accidental disclosure of PII such as adjusting the angle of monitors in customer service areas, and the responsible use of mobile devices such that a customer or a screen containing PII is not unintentionally photographed (see SOP 240.500 Customer Service);
4. A summary of active data sharing agreements such that the employee is versed on the information that can be disclosed to a specific authorized third party, and the limits of disclosure under the applicable agreement.

The Registrar has the discretion to update the DCVRD Confidentiality Agreement for any reason including, but not limited to a change in any governing statute, regulation, or internal policies and procedures that necessitate a revision. Upon issuance

	<p>of a revised DCVRD Confidentiality Agreement, the Registrar has the authority to require all DCVRD employees to submit an updated attestation reflecting the new provisions.</p> <p>All DCVRD employees will renew confidentiality training annually.</p> <p>The Registrar has the authority to require any DCVRD employee to re-take confidentiality training and sign a new DCVRD Confidentiality Agreement in response to a specific incident or concern. The Registrar also has the authority to require a unit within DCVRD, or all DCVRD employees, to re-take confidentiality training and sign a new DCVRD Confidentiality Agreement as a general precaution to mitigate the risk of an unlawful, or otherwise inappropriate disclosure of PII.</p> <p>In the event of an unlawful, or otherwise inappropriate disclosure of PII, any employee with knowledge of the disclosure shall report all relevant information to the Registrar immediately. The Registrar will, in turn, report the disclosure to the Senior Deputy Director of CPPE, complete an Unusual Incident Report, and submit that report to the DC Health Risk Manager. If the disclosure was electronic, i.e. data was disclosed using any DC Health-managed application, including email, the Registrar will also notify the DC Health Chief Information Technology Officer.</p> <p>DCVRD employees may not access records that they are not working with pursuant to an assigned task. Examples of conduct violating this provision are accessing the record of a public figure, or a person they know personally, when not required to do so for a legitimate business purpose. Violating this provision will be treated as an inappropriate disclosure of PII.</p> <p>The Registrar has the authority to suspend access to DCVRD databases and applications containing PII in response to an actual or suspected unlawful or otherwise inappropriate disclosure of PII.</p> <p>Any employee in violation of any part of this SOP may be subject to commensurate disciplinary action.</p>
<p>IV. Definitions & Acronyms</p>	<p>CPPE- Center for Policy Planning and Evaluation</p>

	<p>DCVRD- District of Columbia Vital Records Division</p> <p>PII- Personally Identifiable Information. Information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available - in any medium and from any source - that, when combined with other available information, could be used to identify an individual.</p>
<p>VI. Procedures</p>	<p>None</p>
<p>VII. Contacts</p>	<p>State Vital Records Registrar</p> <p>Customer Service and Certification Operations Supervisor</p>
<p>VIII. Related Documents, Forms and Tools</p>	<p>SOP 701.000 Access Control</p> <p>SOP 1127.000 Vital Records Entitlement and Identity Verification</p> <p>SOP 240.500 Customer Service</p> <p>DCVRD Confidentiality Agreement</p>