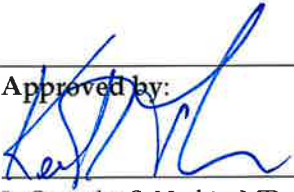
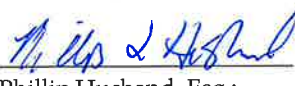


District of Columbia Department of Health <h2 style="text-align: center;">Vital Records Physical Security</h2>		PROCEDURE 1122.000 Implementing Office: Center for Policy Planning and Evaluation/Vital Records Division Training Required: Yes Originally Issued: JUN 15 2022 Revised/Reviewed:
Approved by:  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 District of Columbia Vital Records Division (DCVRD or “the Division”) within the Center for Policy, Planning and Evaluation (CPPE) has jurisdiction over the District of Columbia’s birth, death, fetal death, induced termination of pregnancy and domestic partnership records. Birth, death, domestic partnership and fetal death records may be used to produce certificates for entitled constituents. Counterfeit or fraudulently obtained data or certificates can be used to commit crimes such as identity theft and fraud or targeted for misuse. It is essential that safeguards are in place to mitigate these risks. A policy is required to deter the fraudulent use of vital records; administer and maintain the security of personnel, physical environments, electronic systems, and preservation methods; establish separation of duties between employees working with documents that may be susceptible to fraud or misuse and those who routinely perform audits to identify fraud or misuse within the vital statistics system; provide secure workplace, storage, and technology environments with limited role-based access; and administer and maintain overt, covert, and forensic security measures for certifications, verifications, and automated systems that are part of the vital statistics system.</p>

<p>III. Applicability</p>	<p>This document shall apply to all District of Columbia Department of Health (DC Health) employees, vendor staff, contract employees, interns, employees of other DC government agencies temporarily assigned to DCVRD or whose assignment affords access to information in vital records. These individuals are referred to collectively herein as “employees” or “DCVRD employees.”</p>
<p>IV. Policy Statement</p>	<p>Administration and custodianship of the District of Columbia Vital Statistics system is part of the portfolio of DCVRD. The State Vital Records Registrar (“the Registrar”) is the manager accountable for implementing the safeguards outlined herein.</p> <p>A DCVRD supervisor must be on duty during the Division’s operating hours. The supervisor on duty is responsible for a walkthrough of the unit at the beginning and end of each shift.</p> <p>The walkthrough at the beginning of a shift shall, at a minimum, include an inspection of the vital records area and vault to ensure that they have not been tampered with, and there are no signs of forced entry.</p> <p>The walkthrough at the end of each shift includes, at a minimum, coordinating with all employees on duty to ensure that all security assets, security paper, and documents containing PII are locked and secured.</p> <p>The Registrar shall implement internal controls to manage access to the vital statistics system and serve as custodian of its records. This responsibility includes direction, supervision, and control of the activities of each individual whose duties require access to protected DCVRD datasets.</p> <p>Only employees authorized in advance by the Registrar will have access to secure areas through key fobs or physical keys. Employees with such access are prohibited from loaning keys or fobs to anyone.</p> <p>DC Health reserves the authority to establish satellite locations where a subset of vital records services may be performed according to prescribed guidance from the Registrar. A satellite</p>

location may only open once there is documented compliance with all security requirements articulated herein.

Access to identifiable data or work areas where vital records activities are conducted will be afforded on an as-needed basis. The Registrar must approve access to the vital records work area for employees conducting vital records activities. All other persons entering the vital records work area are considered to be visitors and shall not be privy to vital records information except as authorized by The Vital Records Modernization Amendment Act of 2018, rules issued pursuant to and consistent with the Act, or by an order of the Superior Court of the District of Columbia. In accordance with the law, the Registrar reserves the right to review all work areas and devices to ensure that the Division remains compliant with all security requirements under the applicable statute, regulations, and this SOP.

All visitors, non-employees, vendors, delivery personnel must request access to enter the Vital Records work area at the front desk. All visitors, non-employees, vendors, delivery personnel must be escorted through the vital records work area by a DCVRD employee. DCVRD employees must report to their immediate supervisor any visitors, non-employees, vendors, delivery personnel that is not escorted by a DCVRD employee.

The Registrar must approve employee access to any database containing personally identifiable information (PII). The Registrar will ensure that only employees requiring access to PII to carry out assigned job duties have such access. Access controls shall encompass requirements established by the DC Health Chief Information Technology Officer (CITO). See SOP 701.000 Access Control for additional detail on these requirements.

The Registrar shall establish separation of duties between employees managing tasks that may be susceptible to fraud or misuse, and those who perform audits to identify fraud or misuse within the vital statistics system.

When not in use for authorized vital records activities, DCVRD security assets shall be stored in a secured vault. The vault shall only contain DCVRD security assets. The vault specifications must

be aligned with current National Association for Public Health Statistics and Information Systems (NAPHSIS) Security Committee standards, including climate control, secured physical plant (e.g., secure ceiling), video surveillance, and access control.

Persons who have been authorized to receive access to the DCVRD secure vault, or specifications for security paper or the security printer may not disclose this information without approval from the Registrar.

Original paper vital records and microfilmed vital records images shall be stored in an access-controlled location approved by the Registrar.

Working copies of vital records, or any document containing vital records information, shall only be destroyed by using an approved, high-security cut (P7), security shredder approved by the Registrar. Scanner, computer or multifunction hard drives, microfilm, servers or other machines containing vital records information shall be destroyed using a method approved by the Registrar.

All DCVRD employees and authorized data consumers shall complete annual security training for handling Vital Records and Security within Vital Records spaces, systems and equipment. New employees and authorized data consumers shall complete security training within 60 days of hire/access to data or the next offering.

In the event of a breach or compromise of security protocols of any kind, any employee with relevant knowledge shall that 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 breach or compromise was electronic, e.g. data was disclosed using any DC Health-managed application, including email, the Registrar will also notify the DC Health Chief Information Technology Officer. Examples of compromised security include, but are not limited to:

1. Any unlawful or otherwise inappropriate disclosure of PII;
2. A visitor having access to secure DCVRD areas without preauthorization or escort;

	<p>3. Actual or suspected loss or theft of a security asset; 4. Actual or suspected loss of theft of security paper;</p> <p>Any DCVRD employee in violation of any part of this SOP may be subject to commensurate disciplinary action.</p>
<p>V. Definitions & Acronyms</p>	<p>Authorized Staff- The Registrar, the CSCO Supervisor, and the Compliance Specialist</p> <p>CPPE- Center for Policy, Planning and Evaluation</p> <p>CSCO- Customer Service and Certification Operations Unit</p> <p>DCVRD- District of Columbia Vital Records Division</p> <p>Final delivery- The final stage of the security paper delivery process in which the delivery driver places the full order at the door of the secure vault. The driver is not permitted inside the secure vault.</p> <p>Security Asset – Any tool utilized to issued a certify record that include security paper and manual and electronic embossed seal.</p> <p>Security feature- Any technology designed to prevent tampering or duplication, and/or facilitate reliable authentication that is built into security paper.</p> <p>Security paper- Paper created with technologies designed to prevent tampering or duplication, and/or facilitate reliable authentication.</p> <p>Security printer- A printer authorized by the Registrar that includes security features to safeguard and enhance encryption of security paper.</p> <p>Unsuitable or unusable certificate- A certificate that has been deemed unsuitable or unusable due to a printer malfunction, image quality issue or discovery of potentially erroneous data values.</p>

VI. Procedures	None
VII. Contacts	State Vital Records Registrar
VIII. Related Documents, Forms and Tools	SOP 701.000 Access Control SOP 1121.000 Handling of Security Paper SOP 1129.000 Vital Records Confidentiality NAPHSIS Security Committee Guidelines