DC | HEALTH

District of Columbia Department of Health **Access Control**		**PROCEDURE 701.000** Implementing Office: Office of the Director/Office of Information Technology Training Required: Yes Originally Issued: DEC 06 2021 Revised/Reviewed:
Approved by: LaQuandra S. Nesbitt MD, MPH; Agency Director	**Review by Legal Counsel:** Phillip L Husband Phillip Husband, Esq.; General Counsel	**Effective Date** DEC 06 2021 **Valid Through Date:** DEC 06 2024

I. Authority	Reorganization Plan No. 4 of 1996; Mayor's Order 1997-42; District of Columbia Office of the Chief Technology Officer Access Control Policy (last revised May 21, 2021)
II. Reason for the Policy	The District of Columbia Department of Health ("DC Health") collects significant amounts of Personally Identifiable Information (PII). DC Health has both a legal and ethical responsibility to secure such data to the greatest extent possible. A protocol is necessary to ensure that access to PII is limited to those whose job duties require it. Furthermore, protocols are necessary to ensure that those with appropriate access to PII are trained to avoid improper disclosure (both deliberate and accidental disclosure).
III. Applicability	This policy applies to all DC Health full-time and part-time employees, contract employees, interns, employees of other DC government agencies detailed to DC Health, and summer youth employees. These individuals are referred to collectively herein as "employees" or "DC Health employees."
IV. Policy Statement	Access control is jointly governed across units within DC Health. Each administration is responsible for deciding which employees have access to databases and file repositories that contain PII. The Deputy Director for Operations (DDO) of each administration is the accountable manager for authorizing access to databases and/or file repositories that contain PII. The DDO is encouraged to communicate regularly with employees maintaining daily stewardship over PII to ensure that authorization aligns with program requirements. The Senior Deputy Director will perform

this function if the administration does not have a DDO. The DC Health Office of Information Technology (DC Health IT) is the only office with the authority to grant access to databases and file repositories that contain PII, and may only do so with authorization from the applicable DDO. The Chief Information Technology Officer (CITO) is the accountable manager over DC Health IT.

DC Health employee access to a database or file repository that contains PII must be traceable back to an authenticated dc.gov email address unique to that employee. All databases containing PII must be configured to require multi-factor authentication (MFA) when the user logs in.

All file repositories will be organized such that PII is localized to designated trees within that repository. Such trees must be clearly labelled as containing PII. No employee may store a file containing PII outside of a designated tree. This includes a prohibition on storing PII on a desktop or laptop hard drive.

A new server may only begin operating once it has undergone a security review and approval from DC Health IT. DC Health IT is the only office with the authority to create a database or designated tree where PII may be stored.

DC Health IT has sole authority to grant an employee authorization to read, edit, write, and/or delete, files in a designated tree. DC Health IT may only grant such authorization in response to a request by the administration's DDO. Permissions within a file repository shall be limited to what is necessary for an employee to carry out his/her job duties. DC Health IT will ensure that users logging into a server with a PII designated tree must use MFA when doing so.

No employee may extract a file from a designated tree containing PII. Collaborating on work involving files in a designated tree must occur using secure links. Any disclosure of PII using other electronic means, including but not limited to electronic mail or chat forums, is strictly prohibited.

Employees analyzing data in a database that includes PII will de-identify the data in reports intended for transmission within the

	Department, or to external parties. If reporting on a single individual is required, such as during a case study or case investigation, that individual will be referred to using a case number, or other de-identified marker, wherever possible. If the reporting requires identifiable data, such as a case investigation where the individual's address, employer, or other personal details are essential, that report will be stored in a designated tree, and access shared only through secure links. Every DC Health employee is required to enroll in confidentiality training within one year of hire. If the employee's job duties require access to a designated tree in a file repository and/or a database containing PII, he/she will enroll in the next available offering of confidentiality training or complete an e-learning confidentiality training. Such employees must complete confidentiality training annually. If an employee's portfolio of duties changes such that access to a database containing PII and/or a designated tree is no longer essential, that employee's supervisor is responsible for reporting the date of the change in advance to DC Health IT. DC Health IT is, in turn, responsible for terminating access within 24 hours of the change. Per DC Health SOP 520.000 Employee Separations, supervisors are responsible for informing DC Health IT that an employee with access to a database containing PII and/or a designated tree is leaving DC Health service. This notification shall occur in advance of the employee's last day of work. Per that SOP, DC Health IT shall terminate access within 24 hours of a voluntary separation, and immediately for involuntary separations. DC Health IT will ensure that databases containing PII and designated trees are hosted in platforms where active monitoring of usage is enabled. At a minimum, these platforms will be configured to provide administrative reports on login history of all users, and a record of any file extractions. DC Health IT will, to the greatest practical extent, ensure that audit tracking is enabled for all designated trees.

DC Health IT is responsible for completing an audit of PII access twice per year. This audit includes, at a minimum, ensuring that all users with access to PII are still employed by DC Health, and still require access to a database containing PII and/or a designated tree in a file repository. The CITO will designate an employee within DC Health IT to manage the audit process. To ensure integrity and separation of duties, the DC Health IT auditor may not administer any database containing PII or a designated tree, nor may he/she manage access/termination requests.

The DC Health IT auditor will communicate a list of all users with such permissions to the DDOs of all administrations. Within seven (7) calendar days of receipt, each DDO is required to identify any users whose access should be removed. Reasons for removal include, but are not limited to: having left DC Health service, and having been reassigned to duties that no longer require access.

In addition to the scheduled audits, the CITO has the authority to direct an ad hoc audit in response to any direct evidence, or reasonable suspicion, of an improper disclosure of PII or mismanagement of PII that creates unacceptable risk of disclosure.

Program managers who serve as the primary data stewards over a database and/or file repository are responsible for enforcing access control among employees under their supervision. This includes, at a minimum, ensuring:

1. No file containing PII is stored outside of a designated tree in a file repository;
2. Employees managing PII inside a database are preparing analytics and reporting within the database whenever possible, limiting the need for extracting files;
3. Files containing PII are only created and stored when there is an explicit business purpose for doing so;
4. Files containing PII are retained in a file repository for only as long as necessary to complete the analytics and reporting they support;

Any employee with knowledge, or reasonable suspicion, of an improper disclosure of PII, is required to complete an Unusual Incident Report (UIR)and submit to the DC Health Risk Manager. See SOP 350.100 Incident Reporting and Investigation for more detail.

	DC Health IT will provide all information requested by the DC Health Risk Manager to complete an investigation of a possible improper disclosure of PII. DC Health reserves the right to suspend, or revoke, access to PII for any employee found through an investigation, to have improperly disclosed PII. Any employee in violation of any part of this SOP may be subject to commensurate disciplinary action.
V. Definitions & Acronyms	**Access Control-** A method of maintaining security over Department data using both authorization (a conscious determination that an employee's access to specific data is necessary) and authentication (the use of software tools to ensure that user is who they claim to be). **CITO-** Chief Information Technology Officer **Database-** A structured set of data held in computer storage and typically accessed or manipulated by means of specialized software. **DC Health IT-** Department of Health Office of Information Technology **Designated tree-** A directory of files in a file repository that authorized to contain PII. A designated tree is clearly labelled as containing PII. **DDO-** Deputy Director for Operations **File Repository-** A repository is a central file storage location. It is often stored on a server, which can be accessed by multiple users. Examples of file types that may contain PII within a file repository are spreadsheets, or word-processed documents. **MFA-** Multi-Factor Authentication. MFA is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication

	mechanism: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is). MFA protects user data—which may include personal identification or financial assets—from being accessed by an unauthorized third party that may have been able to discover, for example, a single password. **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. **UIR-** Unusual Incident Report
VI. Procedures	**Procedure A: Providing Access to a Designated Tree or Database Containing PII** 1. The employee will enroll in the next offering of the confidentiality training or complete an e-learning confidentiality training. The employee may skip this step if he/she has completed the training in the past year. 2. The employee's supervisor will relay a request for access to the administration's DDO. The request will include specific requirements for which protected files and/or database the employee requires. 3. The DDO will send a written request for access to DC Health IT. 4. DC Health IT will facilitate access to the requested files/databases.

	Procedure B: Access Control Audit 1. At six-month intervals, the CITO, or designee, will generate a list of all employees with access to any database or file repository containing PII. 2. The designated DC Health IT employee will forward audit findings to every DDO. 3. Each DDO will coordinate with all of the program managers that oversee databases and file repositories in their administration to evaluate the audit findings. 4. Within seven (7) days of receipt of the audit findings, the DDO will respond to DC Health IT with any users who need permissions removed. 5. The designated DC Health IT employee will adjust permissions as stipulated in the DDO responses.
VII. Contacts	Chief Information Technology Officer
VIII. Related Documents, Forms and Tools	None