STATE OF IOWA
Department of Public Health

Security Rules for Public Health Data

Purpose

The purpose of this document is to outline the transmission, storage, duplication, and destruction practices for external use of IDPH data. These rules must be followed when using Iowa Department of Public Health data for statistical, verification, research, or other purposes.

Definitions

Confidential Public Health Information, Record, or Data: A record, certificate, report, data, dataset, or information which is confidential under federal or state law. As a general rule, public health records which contain personally identifiable information of a health-related nature are confidential under Iowa Law. More information about confidential public health records can be found in **IDPH Policy #ES 06-13-002, Disclosure of Confidential Public Health Records** located on the Iowa Public Health Data website.

Data Sharing Agreement (DSA): A legal contract between IDPH and any entity (including other departments within state government and Regent's institutions), or between two internal IDPH programs in which parties agree to exchange specified variables within a dataset, or in some cases paper files, at identified intervals of time, and use of the data does not meet the definition of research constituting a need for a Research Agreement.

Implied Confidential Public Health Data: Data which can be used to indirectly establish the identity of a person named in a confidential public health record by the linking of the released information or data with external information which allows for the identification of such person. More information about implied confidential public health data can be found in **IDPH Policy #ES 06-13-002, Disclosure of Confidential Public Health Records** located on the Iowa Public Health Data website.

Research Agreement: A contract between IDPH and any external entity (including other departments within state government and Regent's institutions) in which IDPH agrees to release specific variables within a dataset that includes parameters of time and geography as requested in a research application. A Research Agreement is required when the receiving entity intends to use the requested dataset for the purpose of research and is bound by the confidentiality requirements in the Research Agreement.

Policy

All persons external to the Department with access to IDPH data must abide by the rules for transmission, storage, duplication and destruction outlined in this document. Rules vary for confidential data, implied confidential data, and aggregate data. Data use practices must be appropriate for the level of confidentiality of the data.

Best practices for data security change over time as technology evolves and threats emerge. This policy will be reviewed and updated a minimum of every three years. Data users will be notified of policy changes.

This policy does not apply to data users internal to IDPH. Please refer to the procedures outlined in IDPH Policy# IM 06-07-023, Information Security for rules regarding internal use of confidential, implied confidential and aggregate data.

Policy/Procedure Violations

For all persons and entities participating in a Data Sharing Agreement or Research Agreement, or other agreement which facilitates external access to IDPH data – IDPH has the authority to employ penalties for misuse of data. Penalties for violations of the data agreement may include, but are not limited to:

- Revocation of the DSA or RA and notice to the immediate supervisor of the violating party.
- Notice of revocation of the DSA or RA to the entity's director.
- Immediate destruction of data confirmed by independent third party, and may need to be verified by IDPH.
- Future requests by the violating requestor and other implicated parties may be denied.
- Other sanctions as authorized by federal or state law.

Procedures

	Confidential data	**Implied Confidential Data**	**Aggregate data only** (no confidential or personally identifiable information in file)
Transmission of data (This includes structured and unstructured data. Includes the initial transmission of raw data to the entity from data source or IDPH as well as subsequent transmission or sharing of tables, reports, etc. containing IDPH data)	• Data may be uploaded to and downloaded from a secure folder on a SFTP server setup by either party. • If SFTP is used for transfer, the data file must be encrypted and password protected. Data encryption will be performed by the data owner and password will be transmitted separately by email or phone. • Secure client software *(e.g., FileZilla or WinSCP)* must be used when sending/retrieving data from the SFTP server. • Other secure methods of sharing may be utilized with approval. This includes Direct Secure Messaging or the state Google Drive. • Reports, tables, etc. containing IDPH data should never be shared on or through any social media site, including through the private messaging services of any social media site.	• Data may be uploaded to and downloaded from a secure folder on a SFTP server setup by either party. • If SFTP is used for transfer, the data file must be encrypted and password protected. Data encryption will be performed by the data owner and password will be transmitted separately by email or phone. • Secure client software *(e.g., FileZilla or WinSCP)* must be used when sending/retrieving data from the SFTP server. • Other secure methods of sharing may be utilized with approval. This includes Direct Secure Messaging or the state Google Drive. • Reports, tables, etc. containing IDPH data should never be shared on or through any social media site, including through the private messaging services of any social media site.	• Neither encryption nor password protection is necessary. • Data may be electronically exchanged via email or other forms of transmission.

Storage of data on server (includes the original data file as well as data being manipulated or used in a database)	• Data to be stored on an access-protected server. • Best practices for data storage must be followed. • Principal Investigator/Database Admin/IT Admin must ensure the operating systems remain updated with currently supported versions. • Principal Investigator/Database Admin/IT Admin must ensure security patches are applied in a timely manner • Access to data on the server must be granted within a centrally controlled directory access program (which sets user permissions to each folder based upon network password). • Servers must be located in a dedicated locked room with restricted access.	• Data to be stored on an access-protected server. • Best practices for data storage must be followed. • Principal Investigator/Database Admin/IT Admin must ensure the operating systems remain updated with currently supported versions. • Principal Investigator/Database Admin/IT Admin must ensure security patches are applied in a timely manner. • Access to data on the server must be granted within a centrally controlled directory access program (which sets user permissions to each folder based upon network password). • Servers must be located in a dedicated locked room with restricted access.	
VPN access to a server	• VPN/remote access must be configured using strong cryptographic methods *(e.g., IPsec or SSL v3 and TLS-V1 with strong encryption)*	• VPN/remote access must be configured using strong cryptographic methods *(e.g., IPsec or SSL v3 and TLS-V1 with strong encryption)*	• VPN/remote access must be configured using strong cryptographic methods *(e.g., IPsec or SSL v3 and TLS-V1 with strong encryption)*
Storage of data on mobile storage device	• Data must not be stored on a mobile storage device.	• Data may be stored on a mobile storage device if the device is encrypted and password-protected.	• Data may be stored on a mobile storage device.

Storage of data on Cloud services	• Data may be stored on Department sponsored or approved Cloud services.	• Data may be stored on Department sponsored or approved Cloud services.	• Data may be stored on a cloud service.
Access, Use and Viewing of Data	• If utilizing a laptop computer, either personal or issued, the following security measures must be followed: • Laptop must have Whole Disk Encryption installed *(e.g., PGP, WinMagic or BitLocker).* If this installation is not possible, no data files should be stored on the device. • Anti-virus and anti-malware software must be up- to-date. • Data must not be accessed while laptop is connected to an unsecured public wifi. • Data must not be viewed on a mobile device unless connected through a secure VPN connection.	• If utilizing a laptop computer, either personal or issued, the following security measures must be followed: • Laptop must have Whole Disk Encryption installed *(e.g., PGP, WinMagic or BitLocker).* If this installation is not possible, no data files should be stored on the device. • Anti-virus and anti-malware software must be up- to-date. • Data must not be accessed while laptop is connected to an unsecured public wifi. • Data must not be viewed on a mobile device unless connected through a secure VPN connection.	• Data may be viewed on a mobile device
Storage on personal devices	• Storage on a personal home computer or laptop is **<u>not</u>** allowed. •	• Storage on a personal home computer or laptop is **<u>not</u>** allowed. •	• Data may be stored on a personal device.
Storage of hard copy documents	• Must be maintained in a locked room within locked file cabinets. • Only researchers should have access to paper records on an as-needed basis.	• Must be maintained in a locked room within locked file cabinets. • Only researchers should have access to paper records on an as-needed basis.	• Only researchers should have access to paper records on an as-needed basis.

Making copies of data files	• Researchers within the same organization should share data sets for analysis using a secure shared network drive. • Any copy made must be stored in a secure manner as outlined in this document. • Any copy made must be inventoried to ensure the data is destroyed properly as outlined in the agreement.	• Researchers within the same organization should share data sets for analysis using a secure shared network drive. • Any copy made must be stored in a secure manner as outlined in this document. • Any copy made must be inventoried to ensure the data is destroyed properly as outlined in the agreement.	• Any copies made must be inventoried to ensure the data is destroyed properly if indicated for aggregate data.
Destroying data when agreement has ended. (Unless otherwise stipulated in the Research Agreement or Data Use Agreement)	• When the agreement has expired, all copies of the data set must be destroyed (including backup copies). • Data should be destroyed in a manner it cannot be retrieved (subject to inspection). • A Confirmation of Destruction form must be submitted to the Department when data are destroyed.	• When the agreement has expired, all copies of the data set must be destroyed (including backup copies). • Data should be destroyed in a manner it cannot be retrieved (subject to inspection). • A Confirmation of Destruction form must be submitted to the Department when data are destroyed.	• When the agreement has expired, all copies of the data must be destroyed if indicated for aggregate data.