Madison County Health Department
Data Management
Policy & Procedures

PURPOSE:

The Madison County Department of Health (MCDOH) Data Management Policy outlines how data will be obtained, maintained, secured, analyzed, interpreted, disseminated and properly disposed of to ensure it is only used for its intended purposes. This policy articulates the Department's use of data in compliance with state and federal regulations and requirements, County policies (e.g. HIPAA Information Security Policy, Cyber Security Citizens' Notification Policy, Social Media/Social Networking Policy, Use of Computer and Related Equipment, Corporate Compliance) and relevant Department policies.

Data are valuable institutional assets of the MCDOH; however, data policies ensure that these resources are carefully managed and wisely used. The following five areas have been identified, which require data policy statements:

Data Administration: Management responsibility for Department data;
Data Access: Inquiry and download access to Department data;
Data Usage: Appropriate use and release of Department data;
Data Maintenance: Upkeep of Department data; and
Data Security: Appropriate protection of Department data.

Refer to the Glossary of Terms for the comprehensive list of definitions and types of data (Appendix A).

DATE ADOPTED:

October 2019

POLICY: DATA ADMINISTRATION

The purpose of data administration is to ensure that all Department data are managed as institutional assets for fulfilling the Department's mission of assessment, education, and ensuring necessary services. This section outlines roles and responsibilities.

DATA ROLES

Data custodians hold technical accountability for data, including the security, transportation, and storage. These individuals are most often Information Technology (IT) staff and are responsible for the development and maintenance of the database structure.

The ***data owner*** has charge over Department data and is responsible for the operational policies and procedures that govern access, dissemination, usage, collection, maintenance of Department data.

Data stewards carry out the policies and procedures that govern data on a day-to-day basis. Each **data steward** is responsible for the definition and classification of data as well as verifying its authenticity as needed.

A **data steward** may delegate any or all of their data administration duties to ***data entry users***. **Data entry users** interact with data systems on a regular basis, either entering new data or running programmatic reports. Although they do not hold ultimate responsibility, data entry users adhere to rigorous standards of data quality as outlined in this policy.

Documentation of policies and procedures related to Department data will be maintained and made available by **data stewards** on the Employee Intranet [https://www.madisoncounty.ny.gov/2234/Policies-Procedures].

Department policies and procedures will include the following:

- Review of applicable laws and regulations
- Description of applicable data
- Roles and responsibilities of persons with authorized access to the data
- Description on how to obtain authorization for access to the data
- Applicable confidentiality agreements
- Controls for data management, security, and access (physical and electronic)
- Provisions to prevent indirect release of data
- Guidance on appropriate data sharing relevant to their Division or program

The role assignments for each Department dataset are maintained in the Data Systems Inventory [..\..\Data systems inventory\Inventory\MCDOH_data systems inventory_JULY2019.xlsx].

POLICY: DATA ACCESS

Data and ready access to that data in its many forms are vital to the successful operation of the Department. In turn, management, staff, and others with access are obliged to appropriately use and effectively protect Department data.

AUTHORIZATION

Management, staff, trainees, and volunteer need appropriate access to Department data as it pertains to their job duties. The appropriate data steward will review access to Protected Health Information (PHI), confidential, and internal-use data for each case and authorize access to meet Department needs.

Each member of the Department with authorization to access any non-public data must document with a signed statement that they understand and will comply with Department policies and procedures (Appendix D). Authorization to access any non-public data will be terminated when the individual no longer has a need for the data or their affiliation with the Department ends.

POLICY: DATA USAGE

Authorization to access Department data carries with it the responsibility to use the data as intended and not for personal gain or other inappropriate purposes. PHI, internal-use, and confidential data shall only be used in the performance of assigned duties within the Department, unless approved by the data steward. The purpose is to ensure that Department data are used appropriately.

USE OF DATA

Each individual with access to Department data has the responsibility to use those data and any information derived from them appropriately. Individuals will be held responsible for any use made of Department data under their user IDs and passwords [*Use of Computer and Related Equipment,* www.madisoncounty.ny.gov/2028/HR-Policies-Procedures].

- Data stewards are responsible for overseeing the scope and limitations of data collection activities.
- Data stewards will specify minimum data elements and information needed to conduct their specified public health activities.
- Data stewards will collect identifiable data only when necessary and use de-identifiable data whenever possible.
- Data stewards will ensure that data collected for public health research are done in compliance with Federal and State requirements, which includes obtaining institutional review board (IRB) approval when appropriate.

Willful misuse of Department data, violation of state ethics laws and rules with regard to Department data, or other breaches of this policy, can result in termination of access privileges and/or Department disciplinary action, which may include termination of employment, and/or additional penalties.

RELEASE OF DATA

A data steward approves the release of any non-public data under their jurisdiction if the release is in conformance with state and federal regulations. Data custodians can provide a statement of data security risk to the data steward and those considering the release. Such a release is documented by a written agreement between the Department and the third party (Appendix C).

- Data stewards and custodians will ensure that any non-public data is released only for purposes related to public health, except when required by law.
- Release of any non-public data requires compliance with the Federal, State, and MCDOH program-specific requirements.
- Data that include identifiable information may be released under the following circumstances:
  - With written consent of the person (or his/her legal designee) who is the subject of the record being requested.
  - To qualified personnel for public health activities mandated by statute or regulation.
  - To qualified personnel for the purpose of conducting management audits, financial audits, or program evaluation.
  - To qualified personnel for the purposes of health insurance billing and collections.
  - To qualified personnel for the purpose of conducting scientific research after the research protocol has been approved by the appropriate Institutional Review Boards (IRBs), in accordance with MCDOH policies and protocols.
  - By court order pursuant to showing good cause.

A data steward is also responsible for the timely release of public-use data to stakeholders and the community (e.g. Community Health Assessment results). Prior to the release of public-use data, data stewards will ensure that:

- All Department data maintain high quality standards such as appropriate data cleaning (Appendix B).
- All Department data undergo appropriate de-identification procedures (Appendix B).
- All Department data have been analyzed accurately to the best of their knowledge.

DATA SHARING

Data sharing is the act of granting certain individuals or organizations access to data for the purpose of advancing knowledge and eliminating duplication. Data stewards are responsible for ensuring that sharing of any non-public data may only be done with a justifiable public health need.

- Data stewards will assess the risks and benefits of sharing non-public data for other than their originally stated purposes.
- Data stewards will establish procedures for determining whether to grant requests for aggregate data not covered by existing data release policies.

MCDOH will enter in data sharing agreements to ensure that the data are used as intended with specified constraints and provisions to prevent access of the non-public data to the community (Appendix C).

Policy: Data Security

Department data shall be safeguarded to ensure its confidentiality, integrity, reliability and availability. Department data must be effectively protected from unauthorized acquisition or disclosure as well as accidental or intentional modification, destruction, or loss. This must also be done to prevent unnecessary litigation or penalty against the Department and its employees.

The security protocol outlined below pertains to all data that has not been made publically available, including PHI, confidential, and internal-use data (Appendix A).

PHYSICAL DATA SECURITY

- All Department staff are responsible for ensuring the physical security (e.g. double-locked file cabinet) of hard copies with any non-public data.
- All Department staff will dispose of hard copy documents with non-public data in the confidential shredding bin.
- MCDOH will limit access to secure areas that contain any non-public data to authorized persons.
- Data stewards and custodians will ensure that employees working with any non-public data follow security procedures for handling such documents.
- All Department staff will physically secure printed material with non-public data when not in use.
- Data stewards and custodians will ensure that documents with line lists or supporting notes contain the minimum amount of potentially identifiable information necessary.

ELECTRONIC DATA SECURITY

- At the request of MCDOH data stewards, data custodians will ensure that electronic confidential data are securely stored in P:\Drive files with limited permissions for authorized personnel only.
- Data stewards will request support from data custodians to ensure that the release or sharing of non-public data to external entities is done so through a secure transport mechanism or data encryption [see *Use of Computer and Related Equipment, Use of Portable Data Storage Devices;* www.madisoncounty.ny.gov/2028/HR-Policies-Procedures].
- No Department staff will store non-public data on desktop computer (i.e. computer hard drive) or personal cloud-based systems; such data will be stored only on the secure P:\Drive and H:\Drive.
- No Department staff will share their authorization passwords under any circumstances and will put computers in sleep mode or close applications with non-public data when not in use [*Use of Computer and Related Equipment;* www.madisoncounty.ny.gov/2028/HR-Policies-Procedures].

All security incidents or suspected incidents that result in unauthorized disclosure of non-public data require immediate notification of the Public Health Director. Refer to the *HIPAA Information Security* and *Cyber Security Citizens' Notification* policies (www.madisoncounty.ny.gov/2028/HR-Policies-Procedures).

DATA RETENTION & DISPOSITION

A current copy of Department data must be preserved to ensure the restorability of data lost to disaster or destruction. Procedures to recover lost data must be in place. However, other than the official source copy and appropriate backup copies of Department data, data shall be held in other locations only as necessary and only for as long as necessary to conduct the business of the Department as required by policy and/or law.

All non-public Department data recorded in any media must be disposed of in a manner that will render the data unrecoverable. Care must be taken to ensure that information is not recoverable using readily available forensic tools when a computer and/or its storage media are scheduled for surplus sales or other re-use either within or outside of the Department. Data residing on a computer or storage media should be removed before passing the device or media on to another employee unless that individual is assuming the role/duties and has the same data access privileges as the previous user.

ANNUAL REVIEW

Given the speed of new technology, this policy will be reviewed on an annual basis. If the document undergoes significant changes, then the policy will be distributed Department-wide along with a new Statement of Acknowledge (Appendix D). These documents will be collected and maintained electronically by the Director of Public Health's Confidential Secretary.

APPENDIX A: GLOSSARY OF TERMS & TYPES OF DATA

DEFINTIONS

Confidential Record: Any information that could identify an individual, including paper or electronic records. This may include names, addresses or small geographic areas; social security numbers; certain dates; facility names and codes; rare conditions; rare causes of death; individual level data with or without identifiers; aggregate data with small cell sizes if the data could permit the deduction of the identity.

Data: Scientific records which are as accurate and complete as possible.

Data Custodian: An individual responsible for the technical environment and security of data systems.

Data Entry User: An individual acting as a caretaker of a data system on behalf of its owner by entering new data, making appropriate updates, or pulling programmatic reports.

Data Owner: An individual who holds ultimate responsibility for Department data and oversees the carry out of policies and procedures by data stewards.

Data Release: Dissemination of data either for public use or through an ad hoc request. This does not include the release of data under Freedom of Information Act (FOIA).

Data Sharing: Granting certain individuals or organizations access to data for the purpose of advancing knowledge and eliminating duplication.

Data Steward: An individual responsible for the collection, maintenance, release, and utilization of data daily, while adhering to appropriate policies.

De-Identified Data: This type of data has removed or concealed all personally identifiable information from individual records.

Department Data: Items of information, which are collected, maintained, and used for the continued operations of Department, including administrative data and other data maintained and safeguarded for Department operational

purposes, client records, including medical information, and community health information, research data and statistics.
Disclosure Control: Procedures used to limit the risk that information about an individual will be disclosed. These procedures may be administrative, physical, electronic, or statistical. Usually statistical procedures are followed when preparing a public-use data set or a data set that is linkable to another released data set.
Identifiable Data: Data which can be used to establish individual identity, either “directly,” using items such as name, address, or unique identifying number, or “indirectly” by linking data about a case-individual with other information that uniquely identifies them.
Security: Any mechanisms (administrative, technical, or physical) by which privacy and confidentiality policies are set up in computer or telecommunications systems.

TYPES OF DATA
Protected Health Information: Identifiable data containing demographics, medical histories, test and laboratory results, mental health conditions, insurance information, and other data that a healthcare professional collects to identify an individual and determine appropriate care. This type of data is protected under HIPAA law and should be kept strictly confidential.
Confidential: Data containing personal or institutional information that may adversely affect individuals if accessed or modified by unauthorized persons. Access to these data should be restricted to those who have a legitimate purpose.
Internal Use: Information that is less sensitive, but if exposed to unauthorized parties may have an indirect or possible negative effect. This type of data should not be disclosed to unauthorized personnel without appropriate agreements.
Public-Use: Data available to anyone and/or ready for publication; they do not contain sensitive information or have been aggregated and identifiers removed.

APPENDIX B: DATA QUALITY & DE-IDENTIFICATION

Prior to data sharing, MCDOH will be responsible for evaluating the quality and readiness of data.

Data Cleaning Checklist
High-quality data encompasses the following principles: validity, accuracy, completeness, consistency, and uniformity. Data cleaning is the process of ensuring that your data meet those standards by identifying any errors or corruptions in the data, correcting or deleting them, or manually processing them as needed to prevent the error in the future. The checklist below should be used to evaluate the data quality:

- Identify and correct inaccurate records for data set
- Identify and correct incomplete records for data set (method: Pivot Tables, Stratified Frequency Tables)
- Remove duplicate records (complete duplicate or duplicate ID)
- Spell out data variable names
- Confirm data match the variable type
- Confirm data match appropriate rules for the field (method: 1-way frequency table)
- Compute summary statistics for numerical data to evaluate quality and logical errors (e.g. pregnant male)

- Consolidate data sets if applicable

Following the data cleaning process, document all changes made to the dataset to describe frequency of error and maintain the ability to reverse any changes.

Disclosure Control

The majority of data sharing activity will require de-identification beforehand. De-identification refers to the process of concealing or removing all personally identifiable information from individual records. The ultimate goal is to minimize the risk of unintended disclosure of the identity of individuals and information about them.

Expert Determination

A third-party individual with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(1) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(2) Documents the methods and results of the analysis that justify such determination

Safe Harbor Method

The removal of all 18 identifiers of the individual or of relatives, employers, or household members of the individual as outlined by HIPAA Privacy Rule [https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html].

Appendix C: Data Use Agreement Template

This Data Use Agreement is made and entered into on {Date} by and between the County of Madison, hereafter “Holder” and the {Institution}, hereafter “Recipient.”

1. Background
2. Purpose

   This agreement sets forth the terms and conditions pursuant to which Holder will disclose certain health and environmental information in the form of de-identified data sets (Data Sets) to the Recipient; what the Recipient will analyze, and how the analyses and results will be reported to the Holder. Both Parties are committed to complying with the Standards for Privacy of Individually Identifiable Health Information (the “Privacy Regulation”) under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).
3. Scope of Collaboration
4. Permitted Uses and Disclosures
5. Recipient Responsibilities

   a. Recipient will not use or disclose the Data Set for any purpose other than permitted by this Agreement pertaining to the {Specified Project} or as required by law;

   b. Recipient will use appropriate administrative, physical and technical safeguards to prevent use or disclosure of the Data Set other than as provided for by this Agreement;

   c. Recipient will report to the Holder any use or disclosure of the Data Set not provided for by this Agreement of which the Recipient becomes aware within 15 days of becoming aware of such use or disclosure;

d. Recipient will ensure that any agent, including a subcontractor, to whom it provides the Data Set, agrees to the same restrictions and conditions that apply through this Agreement to the Recipient with respect to the Data Set;

e. In no event will the Recipient, its agents or assigns, try to identify the information contained in the Data Set; and

f. In no event will the Recipient, its agents or assigns, contact the individuals who are the subject of the protected health information contained in the Data Set.

6. Holder Responsibilities

a. Initial data collection, verification, and documentation will be conducted by the Holder. All paper documents will be filed under the client's de identification number and double locked in Holder's office. Electronic, aggregated tabular data will be logged and stored in password-protected Microsoft Access database files. The Holder will determine access to electronic data files.

b. The Holder will be responsible for obtaining the data from the field staff and laboratories, data integrity and security, quality checks and review, data storage, analysis and production of reports. The Holder will work closely with the Recipient to ensure data related protocols and policies are adhered to and in the analysis and reporting of the data results.

c. All participant information will be de-identified by the Holder pursuant to the requirements of 45 C.F.R. § 164.514(b).

d. The Holder will send the de-identified Data Sets to the Recipient via an encrypted secure email.

e. The Holder will conduct monthly data verification and protocol checks in accordance with the Data and Safety Monitoring Plan (DSMP) developed by the Holder.

f. The Holder will conduct annual reports detailing the assessment progress, and subject status and participation, as well as any unanticipated events or deviations from the original assessment protocols.

g. Statistical review of the study will be a collaborative effort. The Holder will complete pre-study population analysis, baseline and post-phase reporting, as well as annual reports detailing the overall progress of the study, using descriptive statistical analyses techniques in Microsoft Excel. High level, inferential statistical analyses will be conducted primarily by the Recipient, using aggregated tabular datasets in .xlsx and .accdb formats, with input from the Holder.

7. Term and Termination

a. The terms of this Agreement shall be effective as of {Date}, and shall remain in effect, unless otherwise terminated as provided in this section, until either all Data Sets provided to the Recipient are destroyed or returned to the Holder, with sufficient proof provided of either event, or the {specified period of time} expires, whichever is shorter.

b. As provided for under 45 C.F.R. § 164.504(e)(2)(iii), the Holder may immediately terminate this Agreement and any related agreements if the Holder makes the determination that the Recipient has breached a material term of this Agreement. Alternatively, the Holder may choose to: (i) provide the Recipient with thirty (30) days written notice of the existence of an alleged material breach; and (ii) afford the Recipient an opportunity to cure said alleged material breach upon mutually agreeable terms. Nonetheless, in the event that mutually agreeable terms cannot be achieved within fifteen (15) days. Failure to cure in the manner set forth in this paragraph is grounds for the immediate termination of this Agreement.

c. The Holder may terminate this Agreement in the event of a breach by Recipient.

d. Effect of Termination. Upon the event of termination pursuant to this Section 7, Recipient agrees to return or destroy all Protected Health Information pursuant to 45 C.F.R. § 164.504(e)(2)(I), if it is feasible to do so. Prior to doing so, the Recipient further agrees to recover any Protected Health Information in the possession of its subcontractors or agents. If it is not feasible for the Recipient to return or destroy said Protected Health Information, the Recipient will notify the Holder in writing. Said notification shall include: (i) a statement that the Recipient has determined that it is infeasible to return or destroy the Protected Health Information in its possession, and (ii) the specific reasons for such determination. Recipient further agrees to extend any and all protections, limitations and restrictions contained in this Agreement to the Recipient's use and/or disclosure of any Protected Health Information retained after the termination of this Agreement, and to limit any further uses and/or disclosures to the purposes that make the return or destruction of the Protected Health Information infeasible. If it is infeasible for the Recipient to obtain, from a subcontractor or agent, any Protected Health Information in the possession of the subcontractor or agent, the Recipient must provide a written explanation to the Holder and require the subcontractors and agents to agree to extend any and all protections, limitations and restrictions contained in this Agreement to the subcontractors' and/or agents' use and/or disclosure of any Protected Health Information retained after the termination of this Agreement, and to limit any further uses and/or disclosures to the purposes that make the return or destruction of the Protected Health Information infeasible.

e. Change in Law/Regulation. In the event that any new laws, regulations or interpretations of HIPAA are promulgated, the Parties shall use reasonable efforts to promptly amend this Agreement to comply with such change without any financial concession. No new or additional legislative, regulatory or judicial requirement related to Protected Health Information confidentiality shall take effect under this Agreement until an appropriate amendment is signed by the Parties, except by operation of law. If the Parties are unable to reach agreement on the necessary change within ninety (90) days or such other time mutually agreed upon by the Parties (or such lesser period of time as may be required by governing authority), this Agreement shall terminate at the expiration of the ninety (90) day period, or such other period agreed upon by the Parties (or shorter period, if applicable).

f. Injunctive Relief. Notwithstanding any rights or remedies provided for in this Agreement, Holder retains all rights to seek injunctive relief to prevent or stop the unauthorized access to, or use or disclosure of Protected Health Information by Recipient or any agent, subcontractor or third party that received Protected Health Information from Business Associate.

8. General Provisions

a. This Agreement shall not be assigned by Recipient without the prior written consent of the Holder, which consent may be given or withdrawn in the Holder's absolute discretion.

b. Hold Harmless: To the fullest extent permitted by law, the Recipient shall defend, indemnify and hold harmless the Holder, its representatives, agents, servants, employees, officers, departments and authorities, from and against all claims, injuries, demands, judgements, settlements, damages, losses, liabilities, costs and expenses of any kind of nature, including but not limited to litigation costs and attorney's fees, whether arising in law or in equity, all without any limitation whatsoever, arising out of or resulting from the Recipient's performance of the work and/or duties and/or the transactions contemplated by this Agreement and which are caused, in whole or in part, by or because of any negligent, culpable and/or wrongful act or omission of the Recipient, directly or indirectly, and/or any person or entity employed by Recipient or for whose conduct or action the Recipient may be found or held liable, directly or indirectly. It is the intention of the parties that the right and entitlement to a defense the right and entitlement to be held harmless; and the right and entitlement to indemnification shall be as broad as permitted under applicable law. Further, the Recipient agrees to indemnify the Holder in like regard in an action upon the contract between the Parties and claims between the Parties, including counsel fees and litigation costs and expenses. The terms of this Agreement shall not be construed to negate, abridge or otherwise reduce any other right or obligation of contribution or indemnity which would otherwise exist as to any party or person subject to this Agreement. This Agreement and paragraph shall be liberally construed so as to afford the Holder the fullest possible protection and indemnity. In the event that Recipient shall fail or refuse to defend, hold harmless and/or indemnify the Holder against any such claim, loss, damage, judgement, settlement or action, Recipient shall be liable to the Holder for all expense, expenditure and cost incurred or to be incurred by the Holder in defending, resolving and/or satisfying any such claim, loss, damage, judgment, settlement or action, together with all cost and expense of the Holder, including all attorney's fees, incurred in the Holder pursuing claim or suit or action against or recovering fees, costs and expense from Recipient.

c. Insurance: Recipient represents that they, through their Director, have Professional Liability insurance coverage, and agree to maintain same at all times during the term of this Agreement, at their sole cost and expense. If possible, the Recipient shall name the Holder as an additional insured under this policy. If Recipient fails to procure insurance as required, recoverable damages shall not be limited to the cost of premiums for such additional insurance, but shall include all sums expended, and damages incurred by Holder, and their respective insurers, which would have other been paid by the Recipient's required insurance.

   If possible, the required insurance policies shall be endorsed to include Madison County, its representatives, agents, servants, employees, officers, departments and authorities as additional insureds, with such policies to provide that the additional insured coverage is primary and non-contributory. Also, to include the provision that the issuing company(s) will notify the Certificate of Insurance Holder, who shall be {name}, Clerk to the Board of Supervisors, located in the County Office Building, Wampsville, NY 13163, by certified mail thirty (30) days prior to any change diminishing coverage, limits, cancellation or non-renewal of the insurance policies. For the duration of this contract, the issuing company(s) shall notify the Certificate of Insurance Holder upon renewal of the policies.

   All insurance required to be carried by Recipient shall be issued by a Company licensed to conduct business in the State of New York rated by A.M. Best with a minimum Class "IX" or higher as to financial rating and "A" (Excellent) as to policyholder rating. The form of such policies and insuring Company must be satisfactory to Holder as determined by the Certificate of Insurance Holder or County Attorney.

   Upon request of the Certificate of Insurance Holder or County Attorney, certified copies of the policies shall be delivered to the County, with evidence satisfactory to the Certificate Holder or County Attorney of the payment of the full premiums on the policies.

IN WITNESS WHEREOF, the parties hereto execute this agreement as follows:

{INSERT NAME OF HOLDER OF DATA}

Date: ____________ By: ____
(Title person with authority to sign agreement for the holder of the data)

{RECIPIENT}
Date:___________ By: ______________________________________
(Title of recipient or person with authority to sign agreement for the recipient)

APPENDIX D: STATEMENT OF ACKNOWLEDGEMENT

Statement of Acknowledgement

This is to acknowledge that I have reviewed a copy of the Data Management Policy for Madison County Department of Health. I understand that the policy provides general guidelines about data administration, access, usage, maintenance, and security.

I understand that it is my responsibility to read, comprehend, and comply with the standards that have been established. I also understand that if I have questions, at any time, regarding data management, I will consult with my immediate supervisor. Failure to adhere to the MCDOH Data Management Policy can result in progressive discipline up to and including termination.

____

Print Name

__________________________ ________

Employee Signature **Date**