Data Access Procedure for Individual Subjects of Data
(Minnesota Statutes, Chapter 13)

INTRODUCTION

The purpose of Minneapolis Public Housing Authority's (MPHA) Data Access Procedure for Individual Subjects of Data is to comply with Minnesota Chapter 13 regarding Government Data. This procedure **applies to individual subjects of data**. This procedure does not create a standard of care or enlarge MPHA's duties under any law, regulation, code or ordinance. If any provision of this procedure conflicts with applicable law, the applicable law will apply.

A.   DEFINITIONS (See Minn. Stat. § 13.02)

1. **Confidential Data on Individuals** is data on Individuals that by law is inaccessible to the public and the subject of the data.

2. **Data** is all data collected, created, received, maintained or disseminated by MPHA regardless of its physical form, storage media or conditions of use.

3. **Data on Individuals** is all data in which an individual is identified as the subject of that Data. Individual data does not include the appearance of the name or other identifying data that is clearly demonstrated to be only incidental to the data and the data is not accessed by the name or other identifying data of any individual.

4. **Data Practices Requests should be sent to:** datapractices@mplspha.org.

5. **Designees** means any person designated by the Responsible Authority to be in charge of individual files or systems of files containing government data and to receive and comply with all requests for government data. The designees include: Elizabeth Grossman, Assistant General Counsel; Kristen Ferriss, Staff Attorney; and Nancy Horan, Paralegal. The address for all designees is Legal Department, MPHA, 1001 Washington Avenue North, Minneapolis, MN 55401.

6. **Individual** means a natural person. In the case of a minor or an incapacitated person as defined in Minn. Stat. § 524.5-102, subd. 6, individual includes a parent or guardian or individual acting as a parent or guardian, unless withholding the data would be in the best interest of the minor.

7. **Not Public Data** is any data classified by statute, federal law, or temporary classification as confidential, private, nonpublic, or protected nonpublic.

8. **Nonpublic Data** is data not on individuals as defined by statute or federal law that is not accessible to the public; and is accessible to the subject of the data.

9. **Person** is an individual, partnership, corporation, association, business trust, or a legal representative of an organization.

10. **Private Data on Individuals** is data defined by law that as not public and is accessible to the individual subject of the data.

11. **Protected Nonpublic Data** is data not on individuals as defined by law that is not public and is not accessible to the subject of the data.

12. **Public Data Not on Individuals** is data not on individuals as defined by law and that is accessible to the public pursuant to Minn. Stat. § 13.03.

13. **Public Data on Individuals** is data accessible to the public pursuant to Minn. Stat. § 13.03.

14. **Responsible Authority** is the individual who is responsible for the collection, use, and dissemination of MPHA data. MPHA's Responsible Authority is MPHA's General Counsel, Lisa R. Griebel, Legal Department, MPHA, 1001 Washington Avenue North, Minneapolis, MN 55401, or lgriebel@mplspha.org. MPHA's General Counsel is also the designated Data Practices Compliance Officer Data to whom persons may direct questions or concerns regarding problems in obtaining access to data or other data practices problems. The General Counsel may designate one or more designees to fulfill MPHA's data practices responsibilities.

15. **Summary Data** means statistical records and reports derived from data on individuals but in which individuals are not identified and from which neither their identities nor any other characteristic that would uniquely identify an individual is ascertainable.

B. Classifications of Data

MPHA data may be public, private or confidential. Public data are available to the public. Private data is not available to the public but is available to the subject. Confidential data is not available to the public or to the subject. MPHA data is presumed to be public unless a law states that the data is not public.

C. Individual Subject's Rights under the Data Practices Act

1. An individual may have access to private data when the individual is the subject of the data that MPHA has collected and maintained.

2. MPHA may collect and keep only the data about an individual subject that is needed to administer and manage programs as permitted by law.

3. An individual subject may look, free of charge, at the public and private data about the individual.

4. An individual subject may receive a copy of the public and private data about the individual. MPHA may charge the cost of retrieval, mailing and making a copy as permitted by law.

5. **Minors.** In the absence of a law or court order such as a divorce, separation, or custody, or a legally binding instrument that provides to the contrary, a parent of a minor may receive copies of or look at, free of charge, private data when the individual subject of the data is the minor. In writing, a minor may ask the responsible authority to deny a parent access to the minor's private data. The written request must state the reasons for the denial and be signed by the minor. MPHA will make the final decision about the request based upon the best interests of the minor and the criteria in Minnesota Administrative Rule 1205.0500.

   Without a request from a minor, the responsible authority may deny a parent's access to private data on a minor as provided in Minn. Stat. §§ 144.291 to 144.298 or any other applicable law.

6. **Tennessen Warning to an Individual Subject.** MPHA will give a Tennessen warning to an individual subject as required by law, Minn. Stat. § 13.04 subd. 2. If MPHA asks an individual to supply private or confidential data about the individual, MPHA will inform the individual of:

   a. the purpose and intended use of the requested data;

   b. whether the individual may refuse or is legally required to supply the requested data;

   c. any known consequence arising from supplying or refusing to supply the data; and

   d. the identity of other persons or entities authorized by state or federal law to receive the data.

7. **Informed Consent.** MPHA may ask an individual for permission to release private data about the individual to another person or the individual may ask MPHA to release the private data to another person.

8. **Accuracy of Data**. An individual may challenge the accuracy and/or completeness of the public or private data about the individual. To exercise this right, the person in writing shall notify the responsible authority describing the nature of the disagreement.

   The responsible authority shall within 30 days either:

   a.   correct the data found to be inaccurate or incomplete and attempt to notify past recipients of inaccurate or incomplete data, including recipients named by the individual; or

   b.   notify the individual that MPHA believes the data to be correct.

   MPHA shall disclose disputed data only if the person's statement of disagreement is included with the disclosed data. See Minn. Stat. § 13.04 subd. 4.

   An individual who is dissatisfied with MPHA's action may appeal to the Commissioner of the Minnesota Department of Administration, using the contested case procedures under Minnesota Statutes Chapter 14.

   If an individual successfully challenges the data, MPHA will complete, correct, or destroy the data without regard to Minn. Stat. § 138.17.

D. How to Make a Subject Data Request

An individual subject must make a written request to look at or request copies of subject data. The individual must submit the written form to MPHA, by contacting Lisa R. Griebel, General Counsel at the addresses indicated above, or by emailing datapractices@mplspha.org. An individual may use MPHA's Data Request Form. If the Data Request Form is not used, the written request shall include:

1. A statement that the individual subject is making a request, under the Data Practices Act (Minnesota Statutes, Chapter 13) to inspect data in which you are the subject;

2. Whether the request is to inspect the data, have copies of the data, or both;

3. A clear description of the data to be inspected or copied; and

4. Written proof that the individual is the subject or parent of minor who is subject of the data.

E. Identifying Information

1. MPHA may require an adult subject to provide a valid photo identification (ID) such as: a state driver's license; military ID; passport; a state ID, or a tribal ID.

2. MPHA may require a minor subject to provide a valid photo ID, such as: a state driver's license; a military ID; a passport; a tribal ID; or a school ID.

3. MPHA may require a parent to provide a valid photo ID and a certified copy of the minor's birth certificate or other document establishing the parent's relationship to the child. These documents may include: a court order relating to divorce, separation, guardianship, custody, or foster care; a foster care contract; an affidavit of parentage; delegation of powers of a parent under Minn. Stat. §§ 524.5-211; or power of attorney.

4. MPHA may require individuals who do not exercise their data practices rights in person to provide a notarized or certified copy of the required documents or a copy of the required document and a verifying affidavit.

F. MPHA's Response to a Written Data Request

1. MPHA will respond to a request in an appropriate and prompt manner, but no more than within 10 business days of receiving a written request for data from an individual data subject, MPHA will inform the requestor in writing:

    a.   that the request or questions are not requests for data;

    b.   that MPHA needs additional information to clarify the request;

    c.   that MPHA does not have the data;

    d.   whether the data is public, private or confidential;

    e.   of the legal citation for denying access to the data;

    f.   whether the individual is the subject of the data; or

    g.   if the individual is the subject of the data, that MPHA will arrange a date, time and place for a free inspection of the data during business

hours; or will arrange to provide a copy of the data to the requestor at the requestor's expense, including the cost of mailing.

2. MPHA is not required to provide verbal information over the phone.

3. MPHA will receive and process requests during normal business hours.

4. An individual who may by law receive a copy of the data of which the individual is a subject, may pick up a copy or at its discretion and depending upon the format of the data, MPHA may provide a copy by mail, email or fax.

5. After MPHA has provided access to the requested data, MPHA does not have to show the data, except for newly created data or with regards to a pending data practices dispute or legal action, to the person for six months from the date that the data was copied or reviewed.

6. MPHA will not create or collect new data in response to a data request or provide data in a specific form or arrangement if the data is not stored in that form. For instance, if the data is only on paper MPHA is not required to create an electronic form.

G. Copy Costs

You may inspect public data about you free of charge or get copies for a fee. State law allows MPHA to charge the actual costs of making and certifying the copies. See Minn. Stat. § 13.04, subd. 3. In determining the actual cost of making copies, MPHA factors in employee time, the cost of materials onto which we are copying the data (paper, flash drive, CD, DVD, etc.), and mailing costs (if any). You must pay for costs associated with your request before the data will be released to you. Payment can be made by check, cash or money order. Checks should be addressed to the "Minneapolis Public Housing Authority."

If MPHA cannot timely respond or reproduce the data ourselves, such as photographs, the person requesting copies shall pay the actual cost of the outside vendor for the copies. MPHA will comply with Minn. Stat. §13.03 regarding other costs.

H. Data Protection

MPHA has safeguards to ensure that not public data is accessible to persons whose work assignment reasonably requires access to the data. See Minn. Stat. § 13.05 subd. 5.

Where appropriate, MPHA will use the following safeguards to protect not public data, including:

1. Where available, require use of strong passwords to access data;

2. Where available, require periodic updating of passwords to access data;

3. Instruct users to develop strong passwords and to not share passwords and to periodically change passwords;

4. For some applications, require a separate password unique to each person;

5. Obtain a subject's authorization that permits MPHA to disclose the data;

6. Instruct users to not transmit data to unauthorized recipients;

7. Where practical, use a Drop Box and a protected file in the drop box to transmit protected data;

8. Instruct users to not send protected data to private email accounts and to use webmail to access protected data;

9. Where available, limit access to data by software module;

10. Limit access to those persons whose work assignment reasonable requires access to the data by instruction, module or other available means;

11. Conduct an annual audit of access levels of users to update and limit access to persons whose work assignment reasonable requires the access to the data;

12. Disable terminated employees accounts;

13. Control access to certain offices to protect access to data;

14. Secure data in a locked office or file cabinet;

15. Maintain confidential destruction of data;

16. Use of a system of security cameras that may detect data security breaches;

17. Securely recycle outdated hard drives, computers and mobile devices with a certified vendor;

18. Conduct a periodic data security assessment;

19. Use a CheckPoint firewall to protect the domain of servers, applications and network so that hackers do not penetrate the domain;

20. Automatic update the CheckPoint firewall with new technology;

21. Automatic update of security, operating system and browser software to protect against virus attacks and other vulnerabilities;

22. Use systems with automatic updates that scan for viruses, Trojans, and malwares;

23. Use spam filtering to help recognize spam and phishing attacks scams;

24. Instruct users to avoid phishing attacks and scams intended to access computers by passwords, email addresses and other means;

25. Require vendors who have access to MPHA's information technology to sign an Information and Workplace Technology Certification to comply with MPHA's IT and Data Practices Procedures;

26. Require vendors who may have access to data, for work assignments, to sign a Data Privacy Statement; and

27. Train new employees and periodically train users on this procedure.

I. Breach of Security Minn. Stat. § 13.055

1. **Additional Definitions** applicable to this section.

    a. **Breach of Security** means the unauthorized acquisition of data maintained by MPHA that the compromises the security and classification of the data.

    An employee, contractor, or agent of MPHA who in good faith acquires or accesses data for a legitimate MPHA work purpose is not a breach of the security. See Minn. Stat. § 13.05, subd. 5.

    Data under this section includes data maintained by a person under contract with MPHA that provides for the acquisition of or access to the data by an employee, contractor, or agent of MPHA.

    b. **Contact Information** means either name and mailing address or name and e-mail address for each individual who is the subject of data maintained by MPHA.

c. **Unauthorized Acquisition** means a person has obtained, accessed, or viewed data without the informed consent of the subject of the data or statutory authority and with the intent to use the data for nongovernmental purposes.

d. **Unauthorized Person** means a person who accesses data without a work assignment that reasonable requires access, or regardless of work assignment, for a purpose not authorized by Minn. Stat. § 13.05 subd. 5.

2. **Notice to Individuals**

a. When MPHA reasonably believes there has been a breach of security, MPHA shall send a written notice to the subject of the data. The notice shall state how the subject of the data may request a copy of the investigation report by mail or email.

b. MPHA shall send the notice in the most expedient time possible and without reasonable delay, consistent with law enforcement needs and other measures necessary to determine the scope of the breach and to reasonably restore the security of the data.

c. MPHA may delay sending the notice if a law enforcement agency determines that notice will impede an active criminal investigation. MPHA will send the notice after law enforcement determines that the notice will not compromise the investigation.

d. MPHA may provide notice by one of the following methods:

   1) written notice by first class mail to each affected individual;

   2) electronic notice to each affected individual and consistent with electronic records and signatures in U. S. Code title 15, section 7001; or

   3) substitute notice if MPHA shows that written notice would exceed $250,000, the affected class of persons exceeds 500,000, or MPHA does not have sufficient contact information for the affected individuals. Substitute consists of the following:

      a) email notice, if MPHA has an email address;

	b)	conspicuous positing of the notice on MPHA's web site; and
	c)	notice to major media outlets to reach the general public within the City of Minneapolis.

e. If MPHA has to send a notice to more than 1,000 persons, MPHA will notify without delay all consumer reporting agencies as defined in U.S. Code title 15, section 1681a of the time, distribution and content of the notice. See Minn. Stat. § 13.055 subd. 5.

3. **Investigation Report**

Upon the completion of the investigation of a breach of security and the final disposition of any disciplinary action under Minn. Stat. § 13.43, including the rights of appeal under a collective bargaining agreement, MPHA shall prepare a report on the facts and results of the investigation. The report will include:

a. A description of the type of data that was accessed or acquired;

b. The number of individual whose data was improperly accessed or acquired;

c. In cases of a final disposition of disciplinary action under Minn. Stat. § 13.43, the name of the responsible employee; and

d. The final disposition of disciplinary actions taken against the employee.

4. **Security Assessments**

At least annually, MPHA shall conduct a comprehensive security assessment of the personal information maintained by MPHA. Personal information is defined under Minn. Stat. § 325E.61, subd. 1 paragraphs e and f.

Personal information is an individual's first name or first initial and last name in combination with any one or more data element listed below, when the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data is also acquired.

A data element is a:

a.   Social Security number;

b.   Driver's license number or Minnesota identification card number; or

c.   Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

5.   **Penalties**

A person who willfully violates Minn. Stat. § 13.055 or any rules adopted under this section or whose conduct is considered unauthorized acquisition of not public data is guilty of a misdemeanor. In addition to criminal penalties, MPHA shall have just cause to discipline, suspend without pay, or terminate an employee who willfully violates Minn. Stat. § 13.055.

J. Housing Agency Data Minn. Stat. § 13.585

1.   **Identifying Confidential Data**

The following data on individuals maintained by MPHA is considered confidential data:

a.   Correspondence between MPHA and its Legal Department containing data collected as part of an active investigation undertaken for the purpose of commencing or defending potential or active litigation;

b.   Initiation of lease termination or eviction actions;

c.   Admissions denial hearings concerning prospective tenants;

d.   Commencement of actions against independent contractors of MPHA; and

e.   Tenant grievance hearings.

2.   **Law Enforcement Access to Certain Data**

MPHA shall furnish to a local, state, or federal law enforcement officer, upon the officer's request, the current address, Social Security number, and photograph, if available, of a recipient of assistance if the officer:

a. Provides MPHA with the name of the recipient;

b. Notifies MPHA that recipient is:

    1. Fleeing to avoid prosecution or custody or confinement after conviction, under Minnesota laws, for a felony crime;

    2. Violating a condition of probation or parole imposed under state or federal law;

    3. Not residing at a registered address pursuant to Minn. Stat. § 243.166; or

    4. Has information necessary for the officer to conduct the officer's official duties;

c. Provides that the location or apprehension of the individual is within the officer's official duties; and

d. The request is made in writing and in the proper exercise of the officer's official duties.