Resolution 2026-11

HAVRE DE GRACE HOUSING AUTHORITY

A Resolution of the Board of Commissioners
Approving and Adopting the Privacy Policy

WHEREAS the U.S. Department of Housing and Urban Development ("**HUD**") performed a comprehensive compliance review of the Havre De Grace Housing Authority ("**HDGHA**") and set forth the findings in the report dated June 13, 2025 (the "**Report**"); and

WHEREAS the Report included Finding PH 15, which required HDGHA to adopt and implement a privacy policy to implement administrative, technical, and physical safeguards to protect applicant and participant information; and

WHEREAS the Privacy Policy, attached as **Exhibit A**, sets forth the requirements for collecting, managing access to, handling, and securing confidential information and documents, including paper and electronic records, containing personally identifiable information about residents and applicants.

NOW THEREFORE, BE IT RESOLVED by the Board that:

1. The Privacy Policy attached as **Exhibit A** is hereby approved and adopted.

2. The Executive Director, or designee, is authorized to perform all appropriate acts and execute all appropriate documents to carry out this resolution consistent with its terms for implementation of the Records Policy.

Passed, adopted and approved by the Board on July 13, 2026.

Michele Ball
Michele Ball, Chair

George N. Kasnic
George Kasnic, Vice Chair

Sharon Jacobs
Sharon Jacobs, Commissioner

Carrie A. Parsons
Carrie Parsons, Commissioner

Dawn Nowak, Commissioner

EXHIBIT A

PRIVACY POLICY

HAVRE DE GRACE HOUSING AUTHORITY

PRIVACY POLICY

This Privacy Policy governs the way that information regarding residents and applicants is managed and maintained by staff of the Havre De Grace Housing Authority ("**HDGHA**"). The Privacy Act of 1974 requires federal agencies to manage and maintain information in systems electronic and paper records that have safeguards to protect against the misuse of the information. The obligations under the Privacy Act are extended to public housing agencies and other third parties that are required to maintain documents pertaining to information required by the U.S. Department of Housing and Urban Development ("**HUD**"). Notice PIH 2015-06 (April 23, 2015) sets forth the responsibilities of public housing agencies for safeguarding personally identifiable information required by HUD.

A. General Requirements

Personally Identifiable Information ("**PII**") is defined as information which can be used to distinguish or trace an individual's identity, such as their name, social security number, driver's license numbers, medical records, and financial account numbers such as credit or debit card numbers.

Confidential Information consists of PII and other information about the resident's tenancy in the public housing program. HDGHA staff are legally and ethically obligated to protect PII and other confidential information from unauthorized disclosure or misuse. For instance, HDGHA staff are prohibited from discussing or otherwise disclosing any resident's PII or other confidential information PII with other staff without an authorized legitimate business reason. **Furthermore, HDGHA staff are strictly prohibited from disclosing any resident's PII or other confidential information with any other resident.** Confidential information including PII must be handled securely and shall not be disclosed to third parties without the written consent from the resident to disclose such information or as required by law.

In addition to the requirements set forth hereunder, staff shall comply with the HDGHA Record Retention and Disposal Policy. Incidents of unauthorized use or disclosure shall be reported promptly to the Executive Director.

B. Limit Collection of and Manage Access to PII

HDGHA staff are obligated to limit the collection of PII and manage access to PII to prevent unauthorized disclosure. HDGHA staff shall comply with the following requirements.

(1) HDGHA staff must only collect and maintain PII that is needed for the purpose for which it is collected.

(2) HDGHA copies of files containing PII and other confidential information must be locked up in secure file cabinets or secure closet and must not be left unattended.

(3) All data storage devices such as thumb drives, CDs, and the like that contain PII must not be left unattended. These devices must be maintained in secured file cabinets or locked drawers.

(4) Do not distribute or release PII to contractors, or other third parties unless you receive authorization to release or distribute such information.

(5) Prior to discussing PII on the telephone, confirm that you are speaking to the right person before discussing the information and inform the person that the discussion will include PII.

(6) Never leave messages containing PII on voicemail.

(7) Do not discuss PII if unauthorized personnel, contractors, or guests are nearby and may be able to overhear the conversation.

(8) Hold meetings in a secure space (i.e., no unauthorized access or eavesdropping possible) if PII will be discussed and ensure that the room is secured after the meeting.

(9) Treat notes and minutes from such meetings as confidential unless you can verify that the notes and minutes do not contain sensitive PII.

(10) HDGA staff must secure digital copies of files containing PII to include implementing encryption where possible, enhanced authentication mechanisms such as two-factor authentication, and limiting the number of people who are allowed access to the files.

(11) HDGHA must store PII only on workstations that can be secured, such as workstations located in areas that have restricted physical access.

C. Protecting Electronic Transmissions of PII via fax, email, etc.

HDGHA must make appropriate arrangements to ensure the protection of PII that is transmitted electronically.

(1) When faxing PII, HDGHA staff shall use the date stamp function, confirm the fax number, verify that the intended recipient is available, and confirm that he/she has received the fax. Additionally, HDGHA staff shall ensure that none of the transmission is stored in memory on the fax machine, that the fax is in a controlled area, and that all paper waste is disposed of properly (e.g., shredded).

(2) Before faxing PII, HDGHA staff must coordinate with the recipient so that the PII will not be left unattended on the receiving end.

(3) PII should be encrypted when transmitting the information electronically, e.g. by email.

(4) HDGHA shall not place PII on shared drives, multi-access calendars, the Intranet, or the Internet.

D. Protecting Hard Copy Transmissions of Files Containing PII

HDGHA staff shall protect hard copies of documents with PII in files that are transmitted.

(1) HDGHA staff shall not remove tenant records with PII from HDGHA offices unless staff obtains approval from a supervisor. Staff must present sufficient justification, as well as evidence of information security, when submitting the request.

(2) HDGHA shall not use interoffice or translucent envelopes to mail PII. Instead the documents with PII shall only be sent in sealable opaque solid envelopes and the envelope shall be addressed to the person's attention.