NYCHA STANDARD PROCEDURE MANUAL

SP 002:12:1, NYCHA PRIVACY POLICY

TABLE OF CONTENTS

NEW YORK CITY HOUSING AUTHORITY STANDARD PROCEDURE

SUBJECT	ADMINISTERING DEPARTMENT	APPROVED DATE	APPROVED BY	INDEX NO.
NYCHA PRIVACY POLICY	LAW	Issued June 7, 2012 Revised December 23, 2014 Date: 2/13/17	David Farber Executive Vice-President for Legal Affairs and General Counsel Michael Kelly General Manager and Chief Operating Officer	002:12:1

I. PURPOSE

The purpose of this Standard Procedure is to provide instructions to New York City Housing Authority (NYCHA) employees, consultants, and contractors/vendors regarding the handling, safeguarding, and disclosure of Personally Identifiable Information (PII) and the use of NYCHA's resources. This procedure also establishes the role of the Chief Privacy Officer.

II. POLICY

All NYCHA employees, consultants, and contractors/vendors must protect the confidentiality of PII obtained from employees, public housing residents/applicants, Section 8 participants/applicants, and third parties such as employers, contractors/vendors, and government agencies.

Some relevant statutes, regulations and guidance regarding NYCHA's confidentiality obligations include N.Y. Pub. Hous. Law § 159, N.Y. Pub. Off. Law § 96, the federal Violence Against Women Act, the federal Privacy Act (5 U.S.C. § 552a), PIH-2015-06, and OMB M-07-16.

III. APPLICABILITY

This Standard Procedure applies to:

A. All NYCHA employees, consultants, and contractors/vendors at all NYCHA departments/offices/developments in their handling of PII.

B. PII found in various places, including, but not limited to, resident, applicant, or employment applications (electronic or paper); NYCHA owned or operated database systems (e.g., Siebel, Maximo, Primavera, and HRdb); and database systems licensed to NYCHA (e.g., Lexis-Nexis and Westlaw).

C. PII found in any form (including, but not limited to, paper, electronic documents, email, backup tapes, images, audio, video, CD/DVD, microfilm) created, collected, accessed,

used, handled, stored, managed, or disposed of during the course of conducting NYCHA business.

IV. DEFINITIONS

A. Personally Identifiable Information (PII)

PII is defined in OMB-07-16 as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, and biometric records etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

PII includes, but is not limited to:

1. An individual's name (first name or first initial and last name), social security number, e-mail address, phone number, address, driver license number or state ID number, passport number, alien registration number, financial account number, or biometric information such as DNA, fingerprint, and photographic facial images.

2. Any combination of one of the items identified in paragraph IV.A.1. with any of the following items:

   a. Date of birth

   b. Place of birth

   c. Last four digits of social security number

   d. Mother's maiden name

   e. Sexual orientation

   f. Criminal history

   g. Citizenship or immigration status

   h. Ethnic or religious information

   i. Income and/or credit history

   j. Tax return

   k. Asset statement

3. Any number, code, or combination of numbers and codes, such as account number, security code, access code, or password allowing access to or use of an individual's financial or credit account.

4. Individually identifiable information created and collected as part of research projects.

5. Health information such as medical records (in hard copy or electronic form).

B. Sensitive PII

HUD defines sensitive PII as "PII" that when lost, compromised, or disclosed without authorization could substantially harm an individual. Examples of sensitive PII include social security or driver license numbers, medical records, and financial account numbers such as credit or debit card numbers." PIH-2015-06.

V. SAFEGUARDING PERSONALLY IDENTIFIABLE INFORMATION

A. Responsibilities for Safeguarding PII

1. All NYCHA employees, consultants, and contractors/vendors must:

   a. Maintain the confidentiality of PII

   b. Abide by applicable laws , NYCHA's policies, procedures, and guidelines regarding the handling and safeguarding of PII in:

      (1) This Standard Procedure

      (2) Standard Procedure 003:78:1, *Public Access to NYCHA Records*

NOTE:	Violation(s) of this procedure and Standard Procedure 003:78:1, *Public Access to NYCHA Records*, may result in disciplinary action, up to and including termination. Employment actions may be conducted under the advice and guidance of the Human Resources and Law Departments.

   c. Notify immediately your supervisor if you inadvertently gain access or distribute any PII outside of your normal job duties. Refer to Section VII. of this procedure for guidance regarding handling breaches of PII.

2. NYCHA employees, consultants, and contractors/vendors may not access or distribute PII:

   a. Regarding residents, applicants, and employees unless required as part of NYCHA job duties

b. For personal reasons

c. Outside of NYCHA or NYCHA's systems, including NYCHA's Virtual Private Network (VPN) or authorized remote access, unless advance written approval is granted by a Department/Office Director

B. Rules for Handling PII

When handling PII, all NYCHA employees, consultants, and contractors/vendors must comply with the following:

1. Collect only what is necessary to accomplish the intended NYCHA business purpose
2. Provide minimum necessary access
3. Disclose only the minimum information necessary
4. Safeguard information in transit
5. Secure physical equipment and resources
6. Safeguard information in storage
7. Dispose of information securely when no longer needed

NOTE:	All NYCHA employees, consultants, and contractors/vendors must comply with the rules regarding the handling, storing, and disposing of PII in Standard Procedures/General Memoranda (GMs) including, but not limited to: • S.P. 003:04:1, *Baseline Information Security Policy* • S.P. 040:05:2, *Enterprise Income Verification (EIV) System Access and Security for Public Housing and Housing Choice Voucher Programs* • GM 3699, *Records Retention – Housing Developments* • GM 3718, *Tenant Folder* • NYCHA Privacy Breach Response Handbook • NYCHA Human Resources Manual

8. Visit the Privacy and Information Technology Security Portal on the Intranet on a regular basis. http://connect/PRI and http://connect/IT/Pages/IT-Security.aspx

VI. DISCLOSURE OF PERSONALLY IDENTIFIABLE INFORMATION

NYCHA may be required to release information, including PII, if requested by HUD, other federal, state, or local authority, or if required by law. PII may also be requested in a subpoena, search warrant, or other court order, or by researchers seeking access to resident data to support their studies. The Law Department reviews such requests on a case-by-case basis and determines the scope of information to be shared.

NYCHA may share PII with government agencies or entities under an agreement, such as a Memorandum of Understanding (MOU). In addition, NYCHA may disclose PII as part of the City's web-based system that enables authorized users to access multiple data sources through a single point of entry. The Law Department reviews such proposed disclosures on a case-by-case basis and determines the scope of data sharing, if any.

All NYCHA employees, consultants, or contractors/vendors must:

A. Consult with NYCHA's Law Department for further details and instructions before releasing any PII.

B. Comply with NYCHA policies regarding the release of PII.

C. Forward all of the City's web-based system requests or other data requests to the Law Department for review and determination of data to be disclosed, if any. In addition, consult the Law Department before disclosing NYCHA data to a researcher.

VII. REPORTING A PRIVACY INCIDENT

A privacy incident is a violation or imminent threat of a violation of privacy laws, principles, policies, and practices. It includes loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar terms referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII whether physical or electronic. Examples of a privacy incident include, but are not limited to, lost or missing Tenant Folder(s); a locked cabinet containing PII has been forced open; or PII is accidentally faxed to the wrong fax number.

All NYCHA employees, consultants, or contractors/vendors must follow the NYCHA Data Breach Reporting Policy in response to a privacy incident or suspected breach as dictated in the NYCHA Privacy Breach Response Handbook.

All employees, consultants, and contractors/vendors must report any suspected or confirmed privacy incident or breach to a supervisor. The supervisor must then report to the Chief Privacy Officer the suspected or confirmed privacy incident or breach of PII. If there are any questions regarding the NYCHA Privacy Policy, the supervisor may contact the Chief Privacy Officer at Privacy@nycha.nyc.gov.

Consult the NYCHA Privacy Breach Response Handbook for further instructions.

VIII. REVIEW/REVISION HISTORY PAGE

NYCHA PRIVACY POLICY

SP 002:12:1

Review/ Revision	Review/ Revision Date	Sections Amended
1.	12/23/14	Banner
2.	12/23/14	Throughout document replaced "Personally Identifiable Information" with PII.
3.	12/23/14	V. Safeguarding Personally Identifiable Information
4.	12/23/14	VI. Disclosure of Personally Identifiable Information
5.	12/23/14	VII. Reporting Personally Identifiable Information Breach
6.	2/13/17	Banner
7.	2/13/17	II. Policy
8.	2/13/17	IV. Definitions
9.	2/13/17	V. Safeguarding Personally Identifiable Information
10..	2/13/17	VI. Disclosure of Personally Identifiable Information
11.	2/13/17	VII. Reporting A Privacy Incident
12.	3/7/18	V. Safeguarding Personally Identifiable Information