Commonwealth of Massachusetts

DEPARTMENT OF HOUSING &
COMMUNITY DEVELOPMENT

Charles D. Baker, Governor ◆ Karyn E. Polito, Lieutenant Governor ◆ Jennifer D. Maddox, Undersecretary

PHN 2020-18
Attachment A
Tips for protecting PII

Manage Access to Personally Identifiable Information (PII)

- Collect only the PII that is needed for the purposes for which it is collected.

- Use the minimum amount of confidential information (such as Social Security numbers) to the minimum necessary to support business operations (e.g., last four digits). Store the information in approved information repositories.

- Only share or discuss sensitive PII with those persons who have a need to know for purposes of their work.

- When discussing sensitive PII on the telephone:
  - confirm that you are speaking to the right person before discussing the information,
  - inform him/her that the discussion will include sensitive PII

- Never leave messages containing sensitive PII on voicemail.

- Only discuss sensitive PII with authorized personnel in a private and secure environment.
  - Be sure there are not unauthorized personnel, contractors, or guests nearby who may overhear your conversation.
  - Treat notes and minutes from such meetings as confidential unless you can verify that they do not contain sensitive PII.
  - Record the date, time, place, subject, chairperson, and attendees at any meeting involving sensitive PII.

- Do not disclose PII data to any unauthorized persons.

•

Protect Electronic Transmissions of Sensitive PII via Fax, Email, etc.

- Use disclaimer statements when transferring information to internal and external parties.

- Ensure email correspondences are sent to your intended recipient before hitting the “Send” button

- Before faxing PII,
  - coordinate with the recipient so that the PII will not be left unattended on the receiving end
  - the fax is in a controlled area on both ends
  - use only individually controlled fax machines, not central receiving centers

- When faxing sensitive PII,
  - use the date stamp function,
  - confirm the fax number,
  - confirm the fax was received,
  - ensure that none of the transmission is stored in memory on the fax machine,
  - ensure all paper waste is disposed of properly, (e.g., shredded).
  - when possible, use a fax machine that uses a secure transmission line.

- If possible, Encrypt information containing PII when transmitting via an unsecured information system (e.g. electronic mail, Internet, or electronic bulletin board)

- Do not place PII on unprotected shared drives, multi-access calendars, the Intranet, or the Internet.

- Do not use unsecure networks when sending or receiving PII. Examples of unsecured networks include:
  - public wifi hotspots at coffee shops, libraries, etc.

- Permanently delete all copies of temporary upload files containing PII after completing data uploads.

Protect Hard Copy Transmissions of Files Containing Sensitive PII

- Clearly label all files containing sensitive PII documents and removal media (example: For Official Use Only)

- Lock up all hard copy files containing sensitive PII in secured file cabinets and do not leave unattended.

- Protect all electronic media (USB drives, CDs, etc.) that contain sensitive PII and do not leave unattended. This information should be maintained either in secured file cabinets or in computers that have been secured.

- Obtain supervisor approval before removing records about individuals with sensitive PII from usual work facilities where the information is authorized to be stored and used. The removable media containing sensitive PII information includes, but may not be limited to, data on:
  - Thumb drives
  - External USB drives
  - CD / DVD
  - Laptop computers
  - Desktop computers

- Keep accurate records of where PII is stored, used, and maintained

- Periodically audit all sensitive PII holdings to make sure that all such information can be readily located.

- Secure digital copies of files containing sensitive PII. Protection includes encryption, implementing enhanced authentication mechanisms such as two-factor authentication and limiting the number of people allowed access to the files

- Store sensitive PII only on workstations located in areas that have restricted physical access.

- When using mail:
  - use sealable opaque envelopes.
  - mark the envelope to the person’s attention

- do not use translucent envelopes to mail sensitive PII.
- wrap the documents in a way that others cannot see the contents (e.g. include an extra sheet of blank paper or use two envelopes – one inside the other)

Records Management – Retention and Disposition

- Follow applicable records management laws, regulations, and schedules applicable to the records.
- Do not maintain records longer than required per records management schedules.
- Dispose of sensitive PII appropriately – use shredders for hard copies and permanently erase (not just delete) electronic records.