Haywood County, North Carolina

Personally Identifiable Information (PII) Policy

For U.S. Department of Housing and Urban Development
CDBG-DR Programs

Last update: June 2025

Table of Contents

Revision History

Version Number	Date Updated	Summary of Changes
1.0	June 1, 2025	First version

Personally Identifiable Information (PII) Policy

Personal Identifiable Information (PII) is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public web sites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.

Haywood County handles two different types of PII: Sensitive PII and non-sensitive PII. The differences between sensitive PII and non-sensitive PII are primarily based on an analysis regarding the "risk of harm" that could result from the release of the PII. The federal statute at 2 CFR 200.83 (Protected PII) and 2 CFR (Public PII) generally conform to the sensitive and non-sensitive definitions in use by Haywood County.

Sensitive PII is information that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples of sensitive PII include, but are not limited to, social security numbers (SSNs), driver's license, state identification numbers, passport identification numbers, credit and debit card numbers, bank account numbers, birthdates, marital status, spouse and parent names, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, tax and financial information, and computer passwords.

Non-sensitive PII, on the other hand, is information that if disclosed, by itself, could not reasonably be expected to result in personal harm. Essentially, it is stand-alone information that is not linked or closely associated with any sensitive or non-sensitive PII. Examples of non-sensitive PII include information such as first and last names, business addresses, business telephone numbers, general educational credentials, gender or race. However, depending on the circumstances, a combination of these items could potentially be categorized as sensitive PII.

Table 1 provides the specific types of PII defined in North Carolina General Statute. These types of PII should not be shared by Haywood County staff, contractor staff, program developers, or coordinating parties in possession of this information under any circumstances. Haywood County shall endeavor to limit the collection of this information unless there is no alternative available to execute its programs and activities.

Table 1 - State-Defined PII

PII Description	NC General Statute Source
Social Security/Tax ID Number	NCGS 75-66, NCGS 14-113.20
Driver's License, State ID Card, Passport #	NCGS 75-66, NCGS 14-113.20
Checking Account #	NCGS 75-66, NCGS 14-113.20
Savings Account #	NCGS 75-66, NCGS 14-113.20
Credit Card #	NCGS 75-66, NCGS 14-113.20
Debit Card #	NCGS 75-66, NCGS 14-113.20
PIN Code	NCGS 75-66, NCGS 14-113.20

PII Description	NC General Statute Source
Digital Signature	NCGS 75-66, NCGS 14-113.20
Info used to access financial resources	NCGS 75-66, NCGS 14-113.20
Biometric data	NCGS 75-66, NCGS 14-113.20
Fingerprints	NCGS 75-66, NCGS 14-113.20
Passwords	NCGS 75-66, NCGS 14-113.20
Electronic ID numbers, electronic mail names or addresses, internet account numbers, internet identification names	NCGS 14-113.20
Parent's legal surname prior to marriage	NCGS 14-113.20

The Haywood County Personally Identifiable Information (PII) Policy provides guidance for compliance in handling, protecting PII, and the procedure to follow in the event of an inadvertent disclosure. These governing guidelines may include federal law, OMB guidance, United States Department of Housing and Urban Development (HUD) policies, and any relevant state and local requirements.

As part of authorized grant activities, Haywood County staff, contractor staff, program developers and other individuals or groups may have in their possession personally identifiable information (PII) relating to program participants, staff, subgrantee and partner organizations and their staff. This information is generally found in personnel files, participant data sets, performance reports, program evaluations, grant and contract files, and other sources. Federal law, OMB guidance, federal, state law, and state and local policies require that PII and other sensitive information be protected. To ensure compliance with these policies/regulations, PII and sensitive data developed, obtained or otherwise associated with federal funding must be secured and protected at all times.

This policy applies to all HUD CDBG-DR program or contractor staff, vendors, program developers, and any other individuals or groups involved in the handling and protecting of personally identifiable information per governing guidelines (“Covered Persons”).

As a condition of administering CDBG-DR programs as a “covered person,” all covered persons must:

1) Take the steps necessary to ensure the privacy of all PII obtained from participants and/or other individuals and to protect such information from unauthorized disclosure.

2) Ensure that PII used during the performance of activities funded by federal funds has been obtained in conformity with applicable Federal and state laws governing the confidentiality of information.

3) Acknowledge that all PII data obtained through their program activity shall be stored in an area that is physically safe from access by unauthorized persons at all times and be managed with appropriate information technology (IT) services and designated locations. Accessing, processing and storing of PII data on personally owned equipment at unapproved off-site locations (e.g. non-grantee managed IT services such as private e-mail) is strictly prohibited, except as expressly authorized by Haywood County.

4) Sign a disclosure acknowledging the confidential nature of the data and must comply with safe and secure management of the data if that person has access to PII. These disclosures must be kept on file with the program manager for monitoring review at the request of Haywood County.

5) Acknowledge their understanding of the confidential nature of the data and the safeguards with which they must comply in their handling of such data, as well as the fact that they may be liable to civil and criminal sanctions for improper disclosure.

6) Limit access to any program and grant activity PII to only those employees of the grant recipient who need it in their official capacity to perform duties in connection with the scope of work in the grant agreement.

7) Process data in a manner that will protect the confidentiality of the records/documents and is designed to prevent unauthorized persons from retrieving such records by computer, remote terminal or any other means.

8) Encrypt all PII and other sensitive data transmitted via email or stored on CDs, DVDs, portable storage devices, such thumb drives, etc. to ensure that PII is not transmitted to unauthorized users.

9) Retain all PII data in accordance with required record retention requirements. Thereafter, all PII data must be destroyed, including the degaussing of magnetic tape files and deletion of electronic data.

10) With regard to personally identifiable information handled during the intake of applications for assistance by Haywood County employees or contractors, this procedure must be followed, as may be amended or modified and approved by Haywood County. This procedure will be reviewed and revised by Haywood County, as needed.

11) Agree to fully cooperate in any review, investigation or inquiry that occurs in the event of a disclosure of PII.

The data collected from applicants for direct assistance may contain personal information on individuals. Unauthorized disclosure of such personal information may result in personal liability with civil and criminal penalties. The information collected may only be used for limited official purposes:

- Program staff may use personal information throughout the award determination and closeout process to ensure compliance with Program requirements, reduce errors, and mitigate fraud and abuse.
- Independent auditors, when hired by the Program to perform a financial or programmatic audit of the Program may use personal information in determining program compliance with all applicable HUD and federal regulations, including the Stafford Act, CDBG-DR requirements and State and local law.
- Haywood County may disclose sensitive personal information of an applicant to those with duly authorized power of attorney for the applicant or for whom the applicant has provided written consent to do so.
- Haywood County may disclose PII when required by federal or state laws and regulations, such as to the North Carolina Joint Legislative Commission on Governmental Operations.
- Haywood County may need to disclose limited PII when determining applicant eligibility and the verification of benefits received using third-party services as well as internal and external parties.

- Haywood County may need to disclose PII to the State Bureau of Investigation (SBI), such as unredacted documentation, after a determination of Fraud, Waste, and Abuse (FWA) has been rendered.
- Haywood County may need to disclose PII to state and local elected officials and their staff as well as other stakeholders to ensure quality program delivery.

Organizations assisting in executing the CDBG-DR Program must comply with all federal and state law enforcement and auditing requests. This includes, but is not limited to, HUD, FEMA, FBI, NC Office of the Comptroller, third-party services engaged by Haywood County for certain eligibility verifications, and the HUD Office of the Inspector General.

CDBG requirements (applicable to CDBG-DR and CDBG-MIT) at 24 CFR 570.490(c)(2) provides that the State shall provide citizens with reasonable access to records regarding the past use of CDBG funds and ensure that units of general local government provide citizens with reasonable access to records regarding the past use of CDBG funds consistent with State or local requirements concerning the privacy of personal records.

DEFINITIONS

Business: A sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit. The term includes a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution. Business shall not include any government or governmental subdivision or agency.

Disclosing party: Any employee, Subrecipient, contractor and staff, vendor or any other person in possession of PII that transmits, publishes whether in written or oral format, or otherwise releases the PII of another without express permission or authorization by the person or entity identified in the PII.

Personal Identifiable Information (PII): As established in 2 CFR 200.79, information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

PII disclosure: An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach. Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.

Personal information: A person's first name or first initial and last name in combination with identifying information as defined in state statute G.S. 14-113.20(b). Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records.

POC: Point of Contact. This is the person designated by a Subrecipient, contractor or vendor as the primary point of contact for interaction and communications.

Protected consumer: An individual (i) who is under the age of 16 at the time a request for the placement of a security freeze is made pursuant to state statute G.S. 75-63.1 or (ii) who is incapacitated or for whom a guardian or guardian ad litem has been appointed.

Protected consumer security freeze: A security freeze placed on a protected consumer's credit report or on a protected consumer's file pursuant to state statute G.S. 75-63.1.

Protected Personal Identifiable Information: As established in 2 CFR 200.82, an individual's first name or first initial and last name in combination with any one or more types of information, including, but not limited to, Social Security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical or financial records, and educational transcripts. Protected PII does not include information that is required by law to be disclosed. Protected PII and Sensitive PII are often used interchangeably.

Reporting party: Haywood County employee or staff member of a program developer, contractor or vendor that reports a suspected disclosure and that is not the disclosing party.

Security freeze: Notice placed in a credit report, at the request of the consumer and subject to certain exceptions, that prohibits the consumer reporting agency from releasing all or any part of the consumer's credit report or any information derived from it without the express authorization of the consumer.

Sensitive Information: Any unclassified information whose loss, misuse or unauthorized access to or modification of could adversely affect the interest or the conduct of federal programs or the privacy to which individuals are entitled under the Privacy Act.

Sensitive PII and Non-Sensitive PII: There are two types of PII, sensitive PII and non-sensitive PII. The differences between sensitive PII and non-sensitive PII are primarily based on an analysis regarding the "risk of harm" that could result from the release of the PII.

1. Sensitive PII is information that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples of sensitive PII include, but are not limited to, social security numbers (SSNs), driver's license, state identification numbers, passport identification numbers, credit and debit card numbers, bank account numbers, birthdates, marital status, spouse and parent names, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, tax and financial information, and computer passwords.

2. Non-sensitive PII, on the other hand, is information that if disclosed, by itself, could not reasonably be expected to result in personal harm. Essentially, it is stand-alone information that is not linked or closely associated with any sensitive or non-sensitive PII. Examples of non-sensitive PII include: information such as first and last names, business addresses, business telephone numbers, general educational credentials, gender, or race. However, depending on the circumstances, a combination of these items could potentially be categorized as sensitive PII.

Stakeholder: An individual, organization, or entity with an interest in the facts and circumstances of a participant (individual, household, or business entity) in Haywood County's recovery and mitigation programming. Examples of stakeholders include elected officials and elected official staff, local government officials and local government staff, other state agency officials, contractors or vendors working with or for Haywood County in the delivery of recovery programs, other verified property owners, other verified household occupants, lien holders on affected properties, mortgagees or lenders with an interest in affected property, and individuals that have a signed Communication Designee (CD) form or Limited Power of Attorney (POA). Media inquiries and non-stakeholder citizens are not

considered stakeholders.

Substitute notification: Providing notification of suspected or actual disclosure of PII to the public via a webpage, broadcast media (local access channel and/or radio), social media (Haywood County Facebook and Twitter), robocall or Telecommunication Device for the Deaf (TDD).

DISCLOSURE OF INFORMATION TO STAKEHOLDERS

In the delivery of recovery programming, Haywood County may have access to sensitive PII and non-sensitive PII for participating households, individuals, or businesses. Certain individuals, organizations, or entities may have an interest in the ongoing recovery effort for participating households, individuals, or businesses (hereafter Stakeholders). Examples of Stakeholders include elected officials and elected official staff, local government officials and local government staff, other state agency officials, contractors or vendors working with or for Haywood County in the delivery of recovery programs, other verified property owners, other verified household occupants, lien holders on affected properties, mortgagees or lenders with an interest in affected property, and individuals that have a signed Communication Designee (CD) form or Limited Power of Attorney (POA). Media inquiries and non-Stakeholder citizens are not considered Stakeholders. PII and non-sensitive PII information is not to be shared with such non- Stakeholder entities. Haywood County staff are reminded to forward media inquiries to the External Affairs team for proper escalation.

These Stakeholders may from time-to-time request information or inquire about the status of the ongoing recovery. Stakeholders may be entitled to information related to the general eligibility of an application for assistance, general recovery or program status, “next steps” in the recovery activity, general construction status updates, and other information related to the progress of the recovery activity. These updates are not considered a PII and do not pose a risk of revealing the identity or causing harm to a participating household, individual, or business.

While general information is allowable and does not constitute disclosure of a PII, sensitive PII must never be disclosed in the course of sharing allowable information with a Stakeholder. Refer to Table 1 above for specific examples of information that must not be disclosed, even to Stakeholders. Table 2 provides a set of examples of what is and is not allowable to disclose to a Stakeholder.

Table 2 - Example Disclosure Breakdown to Stakeholders

May Disclose to Stakeholders	May Not Disclose
General Eligibility	Household Income
Application Status	The Amount or Value of an Award or Assistance Received
Application "Next Steps"	Social Security Number or Tax ID Number (Including Partial IDs)
Construction Status	Email Address and/or Phone of Primary Applicant

May Disclose to Stakeholders	May Not Disclose
Recovery Project or Activity (i.e. rehabilitation vs. reconstruction)	Criminal History or Incarceration Status
	Medical Information and/or Information Related to a Disability

	Date of Birth
	Citizenship Status
	Protected Class Status (ex: Ethnicity, Race, Religious Affiliation, Sex (including Gender Identity and Sexual Orientation), National Origin, Familial Status, etc.)
	Parent's and Spouse's Birth Surnames

POST-DISCLOSURE PROCESS

The loss of PII can result in substantial harm to individuals, including identity theft or other fraudulent use of the information. Because Haywood County employees, program developers and contractors/vendors may have access to personal identifiable information and other sensitive data concerning individuals, all have a special responsibility to protect that information from loss and misuse. All Haywood County departments are obligated to ensure that the responsibilities under this policy are communicated and enforced. This procedure applies to the actual or potential disclosure of sensitive PII, whether by an employee, a Subrecipient, a contractor or a vendor, including disclosures with an associated loss of state-owned property. Examples of a suspected or actual disclosure of PII includes, but are not limited to:

- A laptop or portable storage device containing PII is lost or stolen
- An email containing PII is inadvertently sent to the wrong person
- A box of documents with PII is lost or stolen during transport
- An unauthorized third party overhears agency employees discussing PII about an individual seeking employment or assistance via an CDBG-DR program
- A user with authorized access to PII discloses it for personal gain or to embarrass an individual
- An IT system housing PII is accessed by a malicious actor
- PII that should not be widely disseminated is posted inadvertently on a public website

Individuals with access to Haywood County's data and information systems should not wait for confirmation that a disclosure has occurred before reporting to the Finance Director or appropriate personnel. Such a delay may undermine Haywood County's and/or the program developer's ability to investigate the potential disclosure, protect the PII from continued disclosure or to mitigate or reduce the risk of harm to potentially affected individuals. In addition, any delay may reduce the likelihood that Haywood County can recover a lost or stolen device or physical document.

Haywood County, program developer's, and businesses (including contractors for program developer's and vendors) are subject to provisions of the North Carolina General Statutes. Specifically, they are subject to the North Carolina Identity Theft Protection Act, N.C.G.S. § 75-60 *et seq.*, and may be subject to other provisions. Procedures herein shall be consistent with the requirements of the Identity Theft Protection Act and the State's guidelines and procedures as outlined by the North Carolina Department of Justice. *See* "Security Breach Information." NC DOJ, *https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-your-business-from-id- theft/security-breach-information/*.

Procedures:

In the event of an actual or potential inadvertent disclosure of sensitive personal identifying information, a disclosing party must take several steps. The overall objective of each step is to mitigate the harm caused by the disclosure. The disclosing party must be transparent and immediately and accurately determine the scope of the disclosure.

Any person who believes that he or she may have inadvertently disclosed sensitive PII or, becomes aware of an actual or potential disclosure or security breach, the person must notify Haywood County as soon as practicable; the only delay considered reasonable is if requested by law enforcement to avoid harm to a criminal investigation or national security. In addition, if a person hears about or is alerted to the potential disclosure of sensitive PII, that person must alert the appropriate personnel, as discussed below, even if that person is not the disclosing party.

I. NOTICE REQUIREMENTS

Timing

1) *Notice – Haywood County*. Immediately after a Haywood County employee learns that an unauthorized or inadvertent disclosure occurred, *or may have occurred*, notice must be given to the Finance Director and the employees direct supervisor.

   In the event of an actual or potential disclosure or security breach of PII for an *individual*, the following persons should be notified: Kristian Owen, Finance Director contract point of contact.

2) *Notice –Business (contractor to program developer or Subrecipient).* Any business, providing services for the administration of CDBG-DR that becomes aware of PII being disclosed must immediately notify its contractual partner (program developer or the Subrecipient) and Haywood County. The following persons should be notified in the manner defined below:

Content

It is Haywood County policy to offer a 12-month period of credit monitoring service to all individuals affected by a PII breach, at no expense to the affected party. A template notification of PII breach, along with an attachment including information related to steps an individual may take to safeguard their identity, are included as Appendix A in this policy. The template and notification may be modified to reflect the facts and circumstances of the real or suspected PII breach. All reports of actual or potential PII disclosure should contain the following information:

- General description of the disclosure or breach
- The type of personal information disclosed
- A narrative describing the efforts taken to avoid further disclosure or unauthorized access to information
- Telephone number where people can call for more information
- Provide advice for impacted or affected persons to include:
  - Checking affected accounts
  - Sign-up for free credit monitoring services
  - Notify the credit bureaus to request fraud alerts
  - Consider a security freeze to prevent establishment of new credit accounts
  - Monitoring their credit
- Contact information for the major consumer reporting agencies, the Federal Trade Commission and the North Carolina Attorney General's Office

Method of Publication

There are several methods to send the notice of disclosure/security breach. Those methods are:

- By US Mail – though not required, return receipt requested is a best practice
- By Electronic Mail – if there is a valid email address AND the recipient has agreed to receive communications electronically
- By Telephone – by calling the affected person and after verifying the business or agency has reached the correct person
- By Substitute Notice – this method may be used only when
    - The cost of providing the notice exceeds $250,000
    - The number of affected persons is greater than 500,000, or
    - The agency or business had no other way to contact the affected persons
        i. This notice must include posting the notice on the business or agency website
        ii. Emailing affected persons when the business or agency has valid email addresses
        iii. Publishing the notice via major statewide media

II. RECOMMENDED ACTIONS AFTER NOTICE

After Haywood County Employee/Contractor Disclosure

Upon receipt of notice, the Finance Director consults with the legal department to assess what type of disclosure may have occurred. Based on the results of the review, the Finance Director will take the following actions:

1) Actual or potential disclosure of PII through the loss of state-owned property. This procedure applies to the actual or potential disclosure of PII with an associated loss of state-owned property by Haywood County personnel or program developer's contractors. The supervisor of the disclosing party or the supervisor of the reporting party, in addition to the notice requirements discussed above, shall take the actions as stated below, even if the disclosing party or the reporting party reasonably believes the lost, stolen or otherwise misplaced state-owned property may be located in the future.
    a. Advise the program developer and/or Haywood County of the loss of state property and potential disclosure of PII
        i. Request that IT immediately prohibit access to state servers, databases and other proprietary information by changing password access to the lost property
        ii. Ensure that any communications (emails. faxes, etc.) to the owner of the lost state property are diverted to a secure email address or fax number
    b. The Finance Director and supervisory/managerial personnel notified of potential disclosure completes SBI-78 (see Appendix B)
    c. The Finance Director convenes a meeting with Haywood County's Legal Counsel to determine most effective and efficient method to mitigate the harm caused by any potential disclosure
    d. The Finance Director, in conjunction with Haywood County's Legal Counsel, drafts additional correspondence to the person whose PII may have been disclosed

2) Where there is an actual or potential disclosure of PII by Haywood County personnel or program developer's contractors, but no associated loss of state-owned property, the supervisor of the disclosing party or the supervisor of the reporting party shall, in addition to providing notice as discussed above, immediately take the actions as stated below.

    Program Developer's supervisory personnel shall meet with the disclosing party or the reporting party to determine all relevant information regarding the disclosure of PII related to any CDBG-DR Program and they advise the Finance Director of the facts, including but not limited to the

following:

a. What information was potentially disclosed and when?
b. How was the disclosure made (e.g., via email, facsimile, letter, telephone call, videoconference, voicemail, etc.)?
c. What actions were taken to prevent disclosure of the PII prior to its inadvertent disclosure?
d. What actions were taken to recall the disclosed information after its inadvertent disclosure?

3) Take corrective action that includes, but is not limited to:
   a. Disciplinary action. After review by the Finance Director, Haywood County employees that are found to have been involved in a suspected or actual disclosure of PII may be subject to disciplinary action up to and including termination of employment. Further, employees may also be subject to criminal penalties under N.C.G.S. §75-60, *et seq.*, the applicable sections of 2 C.F.R.§200 and the federal Privacy Act, where applicable. In this event, the Finance Director will coordinate with the County Manager.
   b. Recertification. After a suspected or actual disclosure by a Haywood County employee, the disclosing party should read and recertify that the party has read and understood this PII policy. Both the employee involved in the suspected or actual disclosure and the employee's supervisor shall execute the certification form. The recertification shall be submitted to the Finance Director.
   c. Training. After review by the Finance Director, any Haywood County employee, or program developer's contractor found to have been involved in a suspected or actual disclosure of PII shall receive additional PII training.

Program Developer or Contractor/Vendor Disclosure

Where there is an actual or potential disclosure of an individual person's PII by a program developer or one of its contractors or vendors, the program developer and its contractors or vendors have certain obligations. The program developer must take reasonable measures to safeguard PII deemed relevant by HUD and Haywood County, adhering to applicable federal, state, local and tribal laws regarding privacy and obligations of confidentiality. *See, SRA*, §4.6(d).

Pursuant to the Subrecipient Agreement (SRA), the Subrecipient must comply with 2 C.F.R. §200.303(e), which states the non-federal entity must "take reasonable measures to safeguard protected personally identifiable information and other information the Federal awarding agency or pass-through entity designates as sensitive or the non-Federal entity considers sensitive consistent with applicable Federal, State, local, and tribal laws regarding privacy and responsibility over confidentiality." In this context, protected PII is the same as sensitive PII.

Thus, in the event of a disclosure or breach of and individual's PII by a Subrecipient, its employees, contractors or vendors, the Subrecipient must take following actions:

1) As provided above, immediately notify the Subrecipient's Grant or Program Manager using the PII Disclosure Form (or Subrecipient's approved equivalent) found in Appendix A

2) Take corrective action that includes, but is not limited to:

   a. Actively participate in the review. After a suspected disclosure or breach of PII for an individual, the Subrecipient shall notify its program POC and/or Finance Director. After providing notice, the Subrecipient shall actively participate in the review of the potential disclosure or breach by providing information and submitting documents upon request, consenting to interviews as requested and operating with full

transparency.

b. Disciplinary action. Subrecipients operating under active Subrecipient Agreements (SRA) with NC Office of Recovery and Resiliency (NCORR) that, after a review by the Finance Director of Compliance, are found to have employees, contractors or vendors that were involved in a suspected or actual disclosure of PII may incur disciplinary action up to and including termination of the SRA Agreement. Further, employees may also be subject to criminal penalties under N.C.G.S.
§75-60, *et seq.*, the applicable sections of 2 C.F.R.§200 and the federal Privacy Act, where applicable.

c. Recertification. In the event of a suspected or actual disclosure by a Subrecipient contractor or vendor, the POC for the disclosing entity shall recertify that it has reviewed the Subrecipient's PII policy or, if applicable, this Haywood County, PII policy, with all persons within its organization involved in the suspected or actual disclosure. Both the POC and the person(s) involved in the disclosure shall execute the certification form. The recertification shall be submitted to the Finance Director.

d. Training. After a review by appropriate Haywood County personnel, any Subrecipient, contractor or vendor to a Subrecipient found to have been involved in a suspected or actual disclosure of PII shall receive additional PII technical assistance. This technical assistance shall be considered a mandatory condition to the continuing the contractual relationship under the SRA. Failure to comply with the technical assistance raining requirements may result in further disciplinary action.

BEST PRACTICES

- Individuals with access to PII should be able to quickly and easily report a suspected or actual disclosure while in the office, teleworking or from any remote location. Therefore, it is recommended that Haywood County establish an email address and/or toll-free telephone number dedicated to reporting the disclosure and record the PII Disclosure Report Form (Appendix A) in the Haywood County Salesforce system. Any electronic or oral report should be followed up with a written and executed PII Disclosure Report Form.

- Haywood County should task its program managers with helping individuals participating in its programs with establishing and using enhanced protective measures, such as multi-factor authentication or using complex and frequently expiring passwords.

- Whenever possible, use unique identifiers for participant tracking instead of SSNs. While SSNs may initially be required for performance tracking purposes, a unique identifier could be linked to each individual record. Once the SSN is entered for performance tracking, the unique identifier would be used in place of the SSN for tracking purposes. If SSNs are to be used for tracking purposes, they must be stored or displayed in a way that is not attributable to a particular individual, such as using a truncated SSN.

- Use appropriate methods for destroying sensitive PII in paper files (i.e. shredding) and securely deleting sensitive electronic PII.

- Do not leave records containing PII open and unattended.

- Store documents containing PII in locked cabinets when not in use.

Appendix A: Personally Identifiable Information Sign Off Form

I have reviewed and acknowledge Haywood County's Personally Identifiable Information Policy and agree that all necessary steps will be taken to ensure the privacy and confidential nature of all personally identifiable information to protect such information from unauthorized disclosure.

I further agree that all personally identifiable information will be stored in an area that is physically safe from access by unauthorized persons at all times and be managed with appropriate information technology (IT) services and designated locations. Access to any personally identifiable information through program and grant activity will be restricted to only those individuals who need access in their official capacity to perform duties in connection with the scope of work.

_____

Printed Name

_____

Signature

_____

Agency Name

_____

Date

This form may be completed by anyone making a formal report of a suspected or actual disclosure of Personal Identifying Information. Please select a reporting status from the following choices:

( ) Confidentiality and anonymity are not requested.

( ) If you desire to remain anonymous, complete all sections below except for the sections requesting your contact information.

( ) If you desire confidential status, Haywood County may contact you for additional information, but your name will be kept confidential and will not be shared outside Haywood County.

Disclosure reported by:			
Name:		**Name:**	
Email:		**Email:**	
Phone:		**Phone:**	

Summary of the Disclosure:
Do not include PII or classified information. Summarize the facts or circumstances of the theft, loss or compromise of PII as currently known, including:
a. A description of the parties involved in the disclosure
b. The physical or electronic storage location of the information at risk
c. What steps, if any, were immediately taken to contain the disclosure
d. Whether the disclosure is an isolated occurrence or a systematic problem
e. Who conducted the review of the disclosure, if applicable
f. Any other pertinent information

Date and Time of the Disclosure:	
Location of the Disclosure:	

Type of Disclosure:			
Lost Information or Equipment	**Yes No**	**Unauthorized Disclosure** ***(e.g., email sent to incorrect address, oral or written disclosure to unauthorized person, disclosing documents publicly with sensitive information not redacted)***	**Yes No**
Stolen Information or Equipment	**Yes No**	**Unauthorized Access** ***(e.g., an unauthorized employee or contractor accesses information or an information system)***	**Yes No**
Unauthorized Equipment ***(e.g., using an unauthorized personal device, server or email account to store PII)***	**Yes No**	**Unauthorized Use** ***(e.g., employee with agency-authorized access to database or file access and uses information for personal purposes rather than for official purposes)***	**Yes No**

Method of Disclosure			
Laptop or Tablet	**Yes No**	**Smartphone**	**Yes No**
Desktop Computer	**Yes No**	**Hardcopy files**	**Yes No**
External Storage Device *(e.g., portable HDD, USB drive)*	**Yes No**	**External Storage Device** *(e.g., DVD, CD, etc.)*	**Yes No**
IT System *(e.g., Intranet, Shared Drive)*	**Yes No**	**Verbal Disclosure**	**Yes No**
Email Disclosure *(e.g., provide email address, whether personal, secured, private)*			
Other *(describe medium)*			

Report History			
Initial Report to _____	**Yes No**	**Initial Report to Subrecipient**	**Yes No**
Name of Initial Report Recipient			
Title of Initial Report Recipient			
Email of Initial Report Recipient			
Phone of Initial Report Recipient			
Date and Time of Initial Report			

Number of Individuals and Safeguards	
Number of Persons/Entities Potentially Affected by Disclosure?	
Was the Information Unstructured? *(e.g., open-ended fields on a form/survey)*	**Yes No**
Was the Information Encrypted?	**Yes No**
Is There a Duplicate Set of the Potentially Compromised Information?	**Yes No**

Additional Information	
Was the Disclosure Internal *(e.g., within Haywood County Network), External, Both or Unknown?*	
What Countermeasures, If Any, Were Already Enabled When the Disclosure Occurred? *(e.g., HDD encryption, encryption of electronic files, password on smartphone, etc.)*	
What efforts, if any, have already been undertaken to mitigate potential harm? *(e.g., calling or sending email to recipient of unauthorized email containing PII requesting its deletion, contacting webpage developer or DPS DIT requesting removal of unredacted documents, etc.)*	
Is there evidence or information supporting that the information disclosed was intentionally stolen or misused? *(Describe basis for knowledge and how information may have been misused, e.g., evidence of identity theft, hacking, adverse publicity, etc.)*	

Appendix B: PII Breach Notification Template

TO:

« Name»

«Mailing Address»

«Mailing Address»

DATE:

«Date»

PERSONAL INFORMATION COMMUNICATION AND COMPLIMENTARY CREDIT MONITORING OFFER

Dear [Name]:

Haywood County is committed to helping homeowners recover from the impacts of Tropical Storm Fred. While assisting homeowners, the CDBG-DR Program collects personally identifiable information (PII) to help determine program eligibility and determine what program benefits to provide to an eligible household. We are writing to notify you that some of this personal information was received by a third party. Describe the nature of the PII breach, including whether the information leaked was sensitive PII or not. As soon as we learned of this incident, Haywood County took steps to control any potential release of information including contacting homeowners that were involved in the receipt of personal information. Briefly describe the extent of the PII breach.

Based on Haywood County's review, describe anticipated level of risk or harm. We are notifying you of this exposure because we are committed to your privacy and security. For that reason, we have arranged for you to obtain 12 months of credit monitoring services at no cost to you. It is a generally good practice to monitor accounts and any credit reports for any signs of suspicious activity, although the information involved in this event is not the type that would likely be used against you. Attachment 1 includes additional information about your options for monitoring and protecting yourself, regardless of your decision to participate in the complimentary credit monitoring service.

If you have questions about the credit monitoring service, please contact _____ to learn more about how to access this service.

Sincerely,

_____

Attachment 1: Additional Information

Be cautious about using email to provide sensitive personal information, whether sending it or in response to email requests. In addition, be cautious when opening attachments and clicking on links in emails. Scammers sometimes use fraudulent emails or other communications to deploy malicious software or to trick people into sharing personal information, such as account numbers, Social Security numbers, or usernames and passwords. The Federal Trade Commission (FTC) has provided guidance at: https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.

Review financial statements and accounts for signs of suspicious transactions and activities. If any indication of unauthorized accounts or transactions is found, report the possible threat to local law enforcement, your State's Attorney General's office, or the FTC. Contact information for some of those entities is below. If unauthorized charges are discovered, promptly inform the relevant payment card companies and financial institutions.

Fraud Alert Information

Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. To place a fraud alert, please contact any of the agencies listed below. The agency will then contact the other two credit agencies.

Whether or not you enroll in the credit monitoring product offered, you also have the right to place an initial fraud alert on your file at no cost. An initial fraud alert lasts one (1) year and is placed on a consumer's credit file. Victims of identity theft are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Fraud alert messages notify potential credit grantors to verify identification before extending credit in case someone is using personal information without consent. A fraud alert can make it more difficult for someone to get credit fraudulently, however, please be aware it also may delay the ability to obtain credit.

To place a fraud alert, please contact any of the agencies listed below. The agency will then contact the other two credit agencies. Any of the consumer reporting agencies or the FTC may also be contacted for more information regarding fraud alerts. The contact information for the three nationwide credit reporting agencies is:

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Free Credit Report Information

Consumers have rights under the federal Fair Credit Reporting Act. These include, among others, the right to know what is in their credit file; the right to dispute incomplete or inaccurate information; and the right to ask for a credit score. Under federal law, consumers are entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even without any discovery of suspicious activity on initial credit reports, it is recommended to check account statements and credit reports periodically. Remain vigilant for incidents of fraud and identity theft. Victim information can be held for use or shared among a group of thieves at different times. Checking credit reports periodically can help spot problems and address them quickly.

If suspicious activity is discovered on credit reports, or if there is reason to believe there is misuse of information, call local law enforcement agency or state attorney general and file a police report. Get a copy of the report as many creditors need the information it contains to alleviate fraudulent debts. File a complaint with the FTC using the contact information below. Complaints will be added to the FTC's Consumer Sentinel database, where it will be accessible to law enforcement.

Consumers may also contact the FTC or the North Carolina Department of Justice to learn more about steps to protect from identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1.877.FTC.HELP (382.4357)
https://www.consumer.ftc.gov/identity-theft-and-online-security

North Carolina Department of Justice
114 West Edenton Street
Raleigh, NC 27603
1-919-716-6400
https://ncdoj.gov/protecting-consumers/identity-theft/

Security Freeze Information

Consumers have the right to request a free security freeze (aka "credit freeze") on their credit file by contacting each of the three nationwide credit reporting companies through the channels outlined below. When a credit freeze is added to a credit report, third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access credit reports without consent. A credit freeze can make it more difficult for someone to get credit fraudulently, however, please be aware it also may delay the ability to obtain credit. Consumers can also contact any of the consumer reporting agencies or the FTC for more information regarding security freezes.

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com/personal/credit-report-services	www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert

A separate credit freeze must be placed at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, including middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill; and
6) Other personal information as required by the applicable credit reporting agency.

If a credit freeze is requested online or by phone, the credit reporting agencies have one (1) business day after receiving the request to place a credit freeze on the credit report. If a lift of the credit freeze is requested online or by phone, the credit reporting agency must lift the freeze within one (1) hour. If a credit freeze or lift of a credit freeze is requested by mail, the credit agency must place or lift the credit freeze no later than three (3) business days after getting the request.