

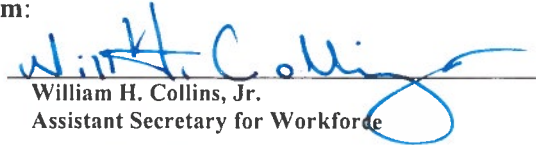
NORTH CAROLINA DEPARTMENT OF COMMERCE  
DIVISION OF WORKFORCE SOLUTIONS

**DWS POLICY STATEMENT NUMBER: PS 10-2014**

**Date: September 30, 2014**

**Subject: Electronic File Storage and Protecting Personally  
Identifiable Information**

**From:**

  
William H. Collins, Jr.  
Assistant Secretary for Workforce

**Purpose:** To provide guidance on the use of electronic file storage, protecting Personally Identifiable Information (PII) and retrieval of workforce and other federal funds' participant, program and financial documents; and to rescind Policy Statement No. 09-2013.

**Background:** Local Workforce Development Areas and the North Carolina Division of Workforce Solutions (DWS) must maintain many forms of documentation and data for federal funds purposes. These documents and data may be stored electronically and must have the ability to be retrieved as per guidance in this Policy Statement.

**Rescinded**

US Department of Labor (USDOL) Training and Employment Guidance Letter (TEGL) No. 39-11 provides additional "Guidance on the Handling and Protection of Personally Identifiable Information."

**Action:** Local Workforce Development Areas and DWS offices using electronic file storage and retrieval systems must meet the minimum requirements as outlined in Attachment 1 of this Policy Statement to maintain and protect information. Effective July 1, 2015, all participant and program related documents will be scanned in and stored in NCWorks Online. In addition to NCWorks Online data, all customer information must be protected as outlined in this Policy Statement and referenced TEGL.

It is expected that all boards, their representatives and DWS staff will take necessary steps to protect Personally Identifiable Information data collected from individuals and employers. This includes redacting any unnecessary personal identifiable data when using for verification.

**Effective Date:** Immediately

**Expiration:** Indefinite

**Contact:** Field Services Program Staff

**Attachment 1:** North Carolina Guidance for Workforce Investment Act and Other Federal Funds Electronic Image Storage

**Attachment 2:** Personally Identifiable Information (PII) Factsheet

# Rescinded

**NORTH CAROLINA  
GUIDANCE FOR WORKFORCE INVESTMENT ACT (WIA)  
AND OTHER FEDERAL FUNDS ELECTRONIC IMAGE STORAGE**

At a minimum, Electronic Storage and Retrieval Systems must:

- Ensure the integrity, accuracy, authenticity, and reliability of the records kept in an electronic format;
- Be capable of retaining, preserving, retrieving, and reproducing the electronic records;
- Be able to update/convert the records as new technology develops;
- Organize documents in a manner consistent with applicable Division of Workforce Solutions policies;
- Ensure that financial and program records maintain a completeness of documentation, are organized by Program Year, and are sufficient for a complete audit trail;
- Have adequate disaster recovery plans, including proper anti-virus protection, tamper proof secondary/supplementary data storage facilities such as regular backup in an external hard drive, and stored in a safe location;
- Ability to convert paper originals stored in electronic format back into legible and readable paper copies; and
- Have adequate records management practices in place.

**Rescinded**

Before implementing the use of an Electronic Storage and Retrieval System, the following requirements must be met:

1. Electronic Data Storage and Retrieval Policies, Procedures and/or Guidelines in place.
2. Adequate computer hardware necessary for implementation, including scanners.
3. Established Data Element Validation and Participant file structure as outlined in current DWS policy.
4. Appropriate electronic document storage and retrieval software to include capacity to scan and retrieve documents in universally accepted file formats such as PDF.
5. Adequate organization server storage capacity which complies with record retention and access regulations as outlined by the Workforce Investment Act of 1998, Public Law 105-220, Section 185.
6. Adequate security measures, for example, password protected assigned access.
7. Documented compliance with vendor recommendations regarding security and login identification and conformity with all software vendor licensing guidelines.
8. Appropriate licensure for software including adequate user licenses as recommended by vendor.
9. Appropriate archiving procedures for storing outdated and/or no longer useful documents.
10. Access capability for DWS and federal officials for data validation, monitoring, and auditing as needed.
11. A notification system to contact impacted individuals if data is compromised.

## Personally Identifiable Information (PII) Factsheet

US DOL Training and Employment Guidance Letter No. 39-11 states:

Definitions.

- Personally Identifiable Information (PII) – Federal Office of Management and Budget defines PII 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.<sup>1</sup>
- 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.
- Protected PII and non-sensitive PII - the U.S. Department of Labor has defined two types of PII, protected PII and non-sensitive PII. The differences between protected 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. Protected PII is information that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples of protected PII include, but are not limited to, Social Security numbers (SSNs), credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse name, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, financial information and computer passwords.
2. Non-sensitive PII 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 protected or unprotected PII. Examples of non-sensitive PII include information such as first and last names, e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race. However, depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII.

To illustrate the connection between non-sensitive PII and protected PII, the disclosure of a name, business e-mail address, or business address most likely will not result in a high degree of harm to an individual. However, a name linked to a Social Security number, a date of birth, and mother's maiden name could result in identity theft. This demonstrates why protecting the information of our program participants is so important.

When uploading verifying documentation in NCWorks Online, be sure to redact information that is not being used for verification. If storing documents electronically in NCWorks Online, use the tools provided to redact the sensitive parts of the document such as driver's license number or the first five digits of the Social Security number.

Example: When using a driver's license to verify date of birth, redact all other information, i.e., driver's license number and address. When using a driver's license to verify residence and date of birth, redact driver's license number.

USDOL Training and Employment Guidance Letter No. 39-11 provides additional "Guidance on the Handling and Protection of Personally Identifiable Information."

<sup>1</sup>OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007), available at <http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf>

# Rescinded