Service Chapter: Administrative Procedures 448-01
Effective Date: October 16, 2024

Overview

Definitions regarding safeguarding practices, protected information and access and disclosure of information are being added.

Description of Changes

1. Definitions 448-01-10 - Change

New definitions will be added in alphabetical order.

2. Communications 448-01-15-35 - Repeal

Information from this section has been moved to ‘Handling Confidential Information 448-01-25-10-01’.

3. Handling Confidential Information 448-01-25-10-01 – New

This is a new section addressing how to handle confidential information and incorporates policies from repealed sections mentioned in this manual letter.

4. Improper Disclosure Reporting 448-01-25-10-15- Change, Title Change

The title of this section has been changed to ‘Improper Disclosure and Data Loss Reporting’ Policy in this section has been rewritten to provide up-to-date information.

5. Securing System and Workspace Information 448-01-25-15-15- Repeal

Information from this section has been moved to ‘Handling Confidential Information 448-01-25-10-01’.

6. Emailing Confidential Information 448-01-25-15-17- Repeal

Information from this section has been moved to ‘Handling Confidential Information 448-01-25-10-01’.

Policy Section Updates

1. Definitions 448-01-10 – Change

Federal Tax Information (FTI) - consists of return information provided from Internal Revenue Services (IRS) records. FTI includes taxpayer identity information, filing status, family size, Modified Adjusted Gross Income (MAGI), and tax year to which information relates. FTI excludes information provided by the taxpayer or their legal representative (even if it is a copy of their tax return or W-2), information obtained from public information files, and information from a source other than the IRS, such as state wage data. If the Department independently verifies FTI provided by the IRS or a secondary source (i.e., SSA, BFS) with the taxpayer or a third-party source (linked to the taxpayer), the verified information is no longer FTI as long as the IRS source information is replaced or overwritten with the newly provided information.

Improper Disclosure - Exposure of information to an unauthorized person. Improper disclosure occurs when PII, FTI or individually identifiable information is disclosed to another person who does not have a need to know.

Mandated Reporter - An individual who holds a professional position (as of licensed social worker, physician, teacher, or counselor) that requires him or her to report to the appropriate state agency cases of child abuse that he or she has reasonable cause to suspect. - Keep

Need-to-Know - means access to information by Economic Assistance and Medicaid program workforce members, whose official duties or responsibilities require them to have access to the information. Accept

Individually Identifiable Information – means information collected from an individual that is created or received by the Department and relates to:

a. The past, present, or future assistance or services applied for or received by an individual under any program administered by or under the supervision and direction of the Department, that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; or

b. A report or any other information obtained, concerning an applicant or a provider of or an individual applying for or receiving assistance or services under any program administered by or under the supervision and direction of the Department.

Personally Identifiable Information (PII) or refers to information that can be used to distinguish or trace an individual's identity. This could be information that identifies a person directly, or when combined with other personal or identifying information that is linked or linkable to a specific individual (indirect).

Protected Health Information (PHI) – means individually identifiable health information including demographic and genetic information created or received by a health care provider, health plan, or health care clearinghouse that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care; and identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual. The confidentiality of PHI is protected under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). PHI falls under the category of personally identifiable information (PII).

Return - means any tax or information return, estimated tax declaration, or refund claim (including amendments, supplements, supporting schedules, attachments, or lists) required by or permitted under the IRC and filed with the IRS by, on behalf of, or with respect to any person or entity."

Return Information – means:

- **a.** Information that IRS obtained from any source or developed through any means that relates to the potential liability of any person under the IRC for any tax, penalty, interest, fine, forfeiture or other imposition or offense;
- **b.** Information extracted from a return, including names of dependents or the location of business;
- **c.** The taxpayer's name, address, and identification number;
- **d.** Information collected by the IRS about any person's tax affairs, even if identifiers, such as name, address and identification number are deleted;
- **e.** Status of whether a return was filed, under examination or subject to other investigation or processing, including collection activities; and
- **f.** Information contained on transcripts of accounts.

Safeguarding Information – The act of protecting confidential information entrusted to the Department by applicants, participants, members and other agencies.

2. Communications 448-01-15-35 – Repeal

~~State and county social service offices correspond electronically via fax, e-mail and phone with applicants, recipients, other agencies and each other. Electronic correspondence, fax and email, must be retained for three years based on policy at Case File Destruction 448-01-40-45-10.~~

~~Program policies allow for counties to communicate with applicants and recipients. Counties are not required to communicate via e-mail or to provide applicants and recipients with their e-mail address, however, if an applicant or recipient requests a worker's or county's e-mail address, the state's open records law requires it be provided.~~

~~If a county does provide an e-mail address to applicants and recipients, it is recommended that the county have one e-mail address for the county where applicants and recipients send their information. This will allow for another worker to receive information when a worker is out on leave.~~

~~When accepting information via e-mail, care must be used to ensure the e-mail is from the applicant or recipient.~~

~~If a household reports a change via e-mail on a weekend, holiday or after hours, the change is considered reported on the next working day.~~

~~Should the applicant or recipient report information via e-mail, refer to program policies. All Economic Assistance and Health Care Coverage programs consider changes reported via e-mail as signed by the household with the exception of SNAP.~~

~~Faxing and emailing of FTI received through a computer match, UFO, BENDEX and IVES interface is prohibited.~~

~~Disclosing FTI received through a computer match, UFO and BENDEX IVES interface, over the phone, including over VoIP networks (telephone services operated over a computer network, ex. Avaya) is prohibited.~~

~~Collaborative Computing Devices (ex. Whiteboards, cameras, microphones) that may be used to communicate must:~~

1. ~~Provide an explicit indication of use to all users present at the device.~~

   ~~Ex: Teams meeting or Zoom meeting, if the meeting is being recorded a message should be displayed on the screen to advise all participants of the recording.~~

2. ~~Prohibit remote activate of collaborative computing devices.~~

~~Upon discovery of an inadvertent disclosure of FTI by email, fax, or phone, contact Economic Assistance central office at (701) 328 – 2332 to report an inadvertent disclosure.~~

3. Handling Confidential Information 448-01-25-10-01 – New

This policy identifies requirements to safeguard confidential information from unauthorized access, disclosure, alteration, and destruction. Its primary aim is to maintain the confidentiality, integrity, and availability of all confidential information. The policy applies to all employees, contractors, and third-party vendors who access, handle, or manage the integrated eligibility system or confidential information.

Securing System Devices and Workspace:

1. Workspace Security:
    - When leaving your workspace, activate the password-protected screen saver or log off your computer.
    - Secure confidential information by placing it in a secure area and avoid leaving it in view of unauthorized personnel.
    - Ensure monitors are positioned to prevent unauthorized viewing or turn them off.
2. Remote and Telework Security:
    - When teleworking, ensure the use of a Virtual Private Network (VPN) and Multi-Factor Authentication (MFA).
    - Telework and Alternative Work Site Wireless Network Connection:
        a) Avoid using wireless network connections when possible.
        b) If using a wireless network connection:
            1. Check encryption of router; turn on encryption if off. Encryption level must be of the same standard as Federal Information Processing Standards (FIPS)-validated or National Security Agency (NSA)-approved encryption.
            2. Only access secure websites (i.e. those that begin with “https”).
            3. A wireless intrusion detection system must be employed.
            4. Update login credentials on Wi-Fi router to increase complexity and uniqueness.
            5. Update the complexity and uniqueness of passwords for all other devices not approved by DHS IT, NDIT or Human Service Zone authorized contractors that are connected to wireless network (Alexa, Google Home, e-readers, tablets, etc.).
                - Any internet connected device can be used as an access point to all other devices connected to the wireless network.
                - If possible, disconnect all other devices from the wireless network.
3. Password Management:

- Do not share passwords with co-workers and keep them secure.
- Change passwords regularly and use complex, unique combinations.

4. Information Storage and Disposal:
   - Save information to network drives to ensure backup.
   - Shred or burn sensitive information according to office procedures.
   - Close all programs and shut down your computer properly at the end of each day.
5. Virus and Malware Protection:
   - Report any virus activity immediately to the information technology department.
6. Access to computer, mobile device and associated electronic device operating system must be limited to DHS IT, NDIT or Human Service Zone authorized contractors to prevent changes to device configuration.
7. Computers, including laptop computers, and associated electronic devices must contain remote wipe and/or kill switch functionality to remove sensitive information. If a device cannot be remotely wiped, the device must be configured to purge all data automatically after 4 consecutive unsuccessful attempts are made to gain access.
8. All non-agency owned devices must be reported to the Office of Safeguards 45 days prior to usage unless remote access is through a virtual desktop infrastructure (VDI) environment.
   - VPN login to agency network
   - MFA authentication to validate identity
   - VDI components segregated from personal components
9. Mobile devices, excluding laptop computers, must:
   - Contain remote wipe and/or kill switch functionality to remove sensitive information. If a device cannot be remotely wiped, the device must be configured to purge all data automatically after 10 consecutive unsuccessful attempts are made to gain access.
   - Require encryption at rest.
   - Wireless personal area networks must be disabled that allow connection to a computer via Bluetooth or neat field communication (NFC) for data synchronization.
   - Access to digital camera,global positioning system (GPS) and universal serial bus (USB) interface must be disabled to the extent possible.
   - If computer, mobile device, and associated electronics are lost or stolen, staff must immediately report to their supervisor and DHS EA Central Office at (701) 327-2332 or send an email to the EA Assistant Director.

10. Collaborative Computing Devices (ex. Whiteboards, cameras, microphones) that may be used to communicate must:

    1. Provide an explicit indication of use to all users present at the device.

       Ex: Teams meeting or Zoom meeting, if the meeting is being recorded a message should be displayed on the screen to advise all participants of the recording.

    2. Prohibit remote activity of collaborative computing devices.

11. Electronic Device Management:
    - Encrypt all devices containing sensitive information. Ensure devices are listed with the appropriate office and kept secure.
    - Avoid downloading or printing sensitive information. If unavoidable, secure and destroy printed materials properly.

12. Monitoring and Compliance:
    - Inspect telework and alternative work site locations annually for compliance with safeguard requirements.

13. Adhere to the Acceptable Use of IT Resources Policy as stated in the Human Resources Manual and Human Service Zone Manual.

14. Wireless Network and Device Security
    - Network Security:
      a) Avoid using wireless networks when possible. When necessary, ensure router encryption meets FIPS or NSA standards.
      b) Access secure websites and use a wireless intrusion detection system.
      c) Update router and device passwords regularly and limit the number of connected devices.

Controlling Access to Areas with Federal Tax Information (FTI)

1. Access Control:
   - Maintain an authorized list of personnel with access to areas containing FTI.
   - Control physical access and ensure cleaning and maintenance personnel are accompanied by authorized staff in restricted areas.
   - Prohibit and document "piggybacking" or "tailgating" into restricted areas. Report unauthorized access attempts.
2. Safeguarding FTI:
   - Use Minimum Protection Standards for systems with access to FTI.

- Ensure that physical and environmental risks are minimized by positioning your work environment to prevent unauthorized access and damage.
- FTI must not be downloaded or stored on any computer, mobile device or associated electronic device. If downloaded or stored, computers, mobile devices and associated electronic devices must have agency-approved security access control devices installed.
- FTI must not be printed. If printed, FTI must be protected by securing in a locked drawer or other secure container and access to work area must be restricted behind a locked door. All printed FTI must be destroyed by either burning or shredding.
    1. Burning – material must be burned in a manner that produces enough heat to burn the entire document, leaving only ash.
    2. Shredding - use crosscut shredders which produce particles that are 1 mm x 5 mm (0.04 in. x 0.2 in.) in size (or smaller). If shredding deviates from the above specifications, FTI must be safeguarded until it is rendered unreadable through additional means, such as burning.

Email and Confidential Information Handling

Emails containing confidential information must adhere to the following:

1. Emailing FTI received through any interface is prohibited.
2. Ensure the subject line does not include any client-identifying information.
3. Include the following email disclaimer:

----------Confidentiality Statement----------
This transmission is intended only for the use of the individual to whom it is addressed and may contain information that is made confidential by law. If you are not the intended recipient, you are hereby notified any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please respond immediately to the sender and then destroy the original transmission as well as any electronic or printed copies. Thank you.

4. Emails sent containing confidential information must be encrypted.
5. Double-check that the email is being sent to the correct source.
6. When accepting information through email, care must be taken to ensure the email does not contain any suspicious activity. Immediately report suspicious activity to the ND IT Department.

Faxing and Confidential Information Handling

1. Faxing FTI received through any interface is prohibited.
2. Ensure the subject line does not include any client-identifying information.
3. Include the following disclaimer:

----------Confidentiality Statement----------
This transmission is intended only for the use of the individual to whom it is addressed and may contain information that is made confidential by law. If you are not the intended recipient, you are hereby notified any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please respond immediately to the sender and then destroy the original transmission as well as any electronic or printed copies. Thank you.

4. Double-check that the fax is being sent to the correct source.

4. Improper Disclosure and Data Loss Reporting - 448-01-25-10-15 – Change, Title Change

Purpose
This policy outlines the procedures for addressing improper disclosures and potential data loss of confidential information. **Confidential information includes:**

- Individually Identifiable Information
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Federal Tax Information (FTI)

Scope

This policy applies to all employees, contractors, Human Service Zone employees, and any other agents of Health and Human Services (HHS) who handle or have access to confidential information within the integrated eligibility verification system (SPACES).

Improper Disclosure
Improper Disclosure refers to the unauthorized sharing or access of confidential information by individuals lacking proper authorization or a legitimate need to know.

Data Loss
Data Loss refers to the unintended deletion, corruption, or unavailability of data, making it inaccessible or unusable. Causes can include human error, hardware failure, software corruption, malware, natural disasters, and theft or loss.

Responsibility and Reporting

Individuals with access to client information are responsible for reporting any improper disclosure of confidential information they encounter in the workplace to their immediate supervisor. This obligation not only helps protect the integrity of the organization but also safeguards the privacy rights of program participants.

Failing to report improper disclosures can lead to serious consequences, including legal ramifications for both the individual and the organization.

After a report is received the following steps will be taken:

1. **Investigation:** HHS will investigate to determine if an improper disclosure has occurred.
2. **Notification:** Relevant entities and affected individuals will be notified as appropriate.
3. **Mitigation:** The HHS will work with impacted individuals to minimize potential harm.
4. **Compliance:** Actions will be taken to address compliance issues and prevent future incidents.

Notification of Improper Disclosure

Step 1:

The team member who has reason to believe that an improper acquisition, access, use, or disclosure of confidential information has occurred must report the incident promptly to their immediate supervisor.

Step 2:

The team member's supervisor must electronically submit an Improper Disclosure Report. If unable to submit the report through the online form, the team member must email Bianca Bell, Economic Assistance (EA), Assistant Director at bibell@nd.gov. , including "Notice of Improper Disclosure" in the subject line.

Improper Disclosure reports must include:

- Point of contact for follow-up
- Name of the person who discovered or received the improper disclosure
- Date and time the incident occurred
- Date and time the incident was discovered
- Description of the incident and data involved
- The potential number of individuals affected
- Address where the incident occurred
- IT resources involved (e.g., laptop, server, mainframe)
- Copies of all associated documents (emails, notices, client reports, etc.)
- Potential number of FTI or SSA records involved

- ****DO NOT INCLUDE** any FTI or SSA data in the incident report.**

Upon discovery of a potential improper disclosure or security incident involving FTI or SSA data, the supervisor must report the incident to the Economic Assistance central office at (701) 328-2332 or email the EA Assistant Director within 24 hours of discovery.

Note: Immediate notification is the most critical factor, even if all information is not available.

Reporting to Improper Disclosure/ Data Loss to Relevant Authorities
HHS is responsible for reporting to the appropriate authorities when required. Below is an overview of HHS's responsibilities by federal agency.

Social Security Administration
The EA Assistant Director must notify the SSA Regional Office or SSA Systems Security Contact within one hour of identifying the improper disclosure/ data loss. If no response, they must contact the SSA Network Customer Service Center (NCSC) at 877-697-4889.
For incident involving cyberattacks the EA Assistant Director must notify the United States Computer Emergency Readiness Team (US-CERT) within one hour of discovering an incident via email or through the DHS CISA Incident Reporting System.

- US-CERT Email: soc@us-cert.gov
- US-CERT Reporting System: [CISA Incident Reporting] (https://www.us-cert.gov/forms/report)
- For assistance with incident reporting or technical questions, contact the Security Operations Centers (SOC) at 888-828-0870.

Internal Revenue Services
For any suspected improper disclosure of FTI, the EA Assistant Director must notify the local Treasury Inspector General for Tax Administration (TIGTA) Field Division Office immediately, but no later than 24 hours after becoming aware of the incident.

- TIGTA Field Division Office: (713) 209-3711
- Hotline Number: 800-589-3718
- TIGTA Website: [TIGTA Website] (https://www.treasury.gov/tigta)
- Mailing Address:

  Treasury Inspector General for Tax Administration
  Ben Franklin Station
  P.O. Box 589
  Washington, DC 20044-0589

Simultaneously with notifying TIGTA, the EA Assistant Director must send an encrypted email to the Office of Safeguards at safeguardreports@irs.gov, using the subject "Data Incident Report."

For all other authorities, the EA Assistant Director will consult with internal partners including HHS Legal to determine steps for notification. This includes incidents involving data pertaining federal computer matching agreements. The EA Assistant Director will collaborate with Federal partners on follow-up actions, notifications, prior to any state-level actions.

Compliance with Regulations:

North Dakota HHS and state policies for privacy incident response are defined in the following sources:

- NDIT Security Incidence Response Policy: RS.SP-1
- NDCC 51-30-02: Notice to Attorney General and Consumers
- NDCC 51-30-03: Notice to Owner or Licensee of Personal Information
- NDCC 51-30-05: Method of Notice
- IRC § 6103
- Privacy Act

Additionally, information related to individuals applying for or receiving assistance under Economic Assistance and Medicaid programs administered by the Department is considered confidential under NDCC 50-06-15.

Review and Updates

This policy will be reviewed annually to ensure compliance with applicable laws and guidelines, and updates will be made as necessary.

5. Securing System and Workspace Information 448-01-25-15-15- Repeal

~~Federal and State regulations require information stored in the computer systems and at your workspace be kept secure. The following requirements must be followed to ensure the security of this information:~~

- ~~When leaving your workspace for any reason, secure your computer by activating the password-protected screen saver or logging off~~
- ~~When leaving your workspace, place confidential information in a secure area.~~
- ~~Do not share passwords with co-workers.~~
- ~~Keep passwords secure~~
- ~~Position your monitor so it cannot be easily viewed or turn it off to avoid displaying sensitive information to unauthorized personnel.~~
- ~~Do not leave confidential information where unauthorized personnel can view it.~~
- ~~Ensure your workspace is secure before leaving during an evacuation or emergency, such as fire, tornado, or flood.~~
- ~~Save information to an appropriate network drive if available. Information stored in the network is backed-up.~~
- ~~Shred or burn sensitive information in accordance with office procedures.~~

- Promptly report any virus activity to your computer technician.
- Close all programs and properly shut down your computer at the end of each day.
- If you are working at home or use a dial-up environment, you are prohibited from using a recording, taking pictures of, or capturing screen shots of any FTI or SSA provided information, including but not limited to cell phones, tablets, laptops, video cameras, security cameras, family members with access to workstations that could view personally identifiable information (PII).

- Each time an e-mail containing client information (e.g. name, social security number) is sent, it must include one of the following disclaimers and the subject line of the email should not include client identifying information:

  - General Disclaimer

---------Confidentiality Statement---------
This transmission is intended only for the use of the individual to whom it is addressed and may contain information that is made confidential by law. If you are not the intended recipient, you are hereby notified any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please respond immediately to the sender and then destroy the original transmission as well as any electronic or printed copies. Thank you.

  - Drug and Alcohol Disclaimer

---------Confidentiality Statement---------
This transmission is intended only for the use of the individual to whom it is addressed and may contain information that is made confidential by law. If you are not the intended recipient, you are hereby notified any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please respond immediately to the sender and then destroy the original transmission as well as any electronic or printed copies. Thank you.

This notice accompanies a disclosure of information concerning a client in alcohol or drug treatment, made to you with the consent of such a client. This information has been disclosed to you from records protected by Federal confidentiality rules (42 C.F.R Part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 C.F.R. Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.

- Any suspicious activity must be reported to the Information Technology Services Division in the Department.

~~Controlling Access to Areas Containing Federal Tax Information (FTI)~~

~~The director or designee shall maintain an authorized list of all personnel who have access to information system areas where these systems contain FTI. This shall not apply to those areas within the facility officially designated as publicly accessible.~~

~~Each agency shall control physical access to the information systems that display FTI information or where FTI is processed to prevent unauthorized individuals from observing the display output.~~

~~Each agency shall position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.~~

- ~~Whenever cleaning and maintenance personnel are working in restricted areas containing FTI, the cleaning and maintenance activities must be performed in the presence of an authorized employee if the area includes access to casefiles or computers where FTI is housed.~~

- ~~Allowing an individual to "piggyback" or "tailgate" into a restricted locations should be prohibited and documented in agency policy. The agency must ensure that all individuals entering an area containing FTI do not bypass access controls or allow unauthorized entry of other individuals.~~

- ~~Unauthorized access should be challenged by authorized individuals (e.g., those with access to FTI). Security personnel must be notified of unauthorized piggyback/tailgate attempts.~~

~~Safeguarding Federal Tax Information (FTI): Telework and Alternative Work Site Locations~~

~~FTI remains subject to the same safeguard requirements and the highest level of attainable security in a telework or alternative work site location as required in a traditional work site location.~~

~~In addition to the traditional work site safeguard requirements, the following safeguard requirements are required.~~

- ~~Access to FTI remotely requires:~~
  - ~~Virtual Private Network (VPN) login to agency network~~
  - ~~Multi-Factor Authentication (MFA) authentication to validate identity~~
- ~~Use of personal computers, mobile devices, and associated electronics (printers, scanners, fax, etc.,) are prohibited unless:~~

- Authorized by your supervisor.
- The devices have a written security risk assessment completed by DHS IT, NDIT or Human Service Zone authorized contractors.
- The devices have been configured to comply with all IRS safeguard requirements.
- All non-agency owned devices must be reported to the Office of Safeguards 45 days prior to usage unless remote access is through a virtual desktop infrastructure (VDI) environment
  - VPN login to agency network
  - MFA authentication to validate identity
  - VDI components segregated from personal components

- Computers, mobile devices, and associated electronics that receive, process, store or transmit FTI must contain the highest level of protection practical.
- Computers, mobile devices, and associated electronics must employ encryption mechanisms to ensure that FTI may not be accessed if the computer, mobile device, or associated electronics are lost or stolen.
- All computers, mobile devices and associated electronics must be listed with the appropriate office (state office, county office or Human Service Zone office) for inventory purposes and updated annually.
- Only agency-approved security access control devices and agencyapproved software will be used on computers, mobile devices, and associated electronics.
- All computers, mobile devices and associated electronics receiving, processing, or transmitting FTI must be kept in a secured area under the immediate protection and control of an authorized employee or locked up.
- **FTI must not be downloaded or stored** on any computer, mobile device or associated electronic device. If downloaded or stored, computers, mobile devices and associated electronic devices must have agency-approved security access control devices installed.
- **FTI must not be printed.** If printed, FTI must be protected by securing in a locked drawer or other secure container and access to work area must be restricted behind a locked door. All printed FTI must be destroyed by either burning or shredding.
  - Burning – material must be burned in a manner that produces enough heat to burn the entire document, leaving only ash.

- Shredding - use cross cut shredders which produce particles that are 1 mm x 5 mm (0.04 in. x 0.2 in.) in size (or smaller). If shredding deviates from the above specifications, FTI must be safeguarded until it is rendered unreadable through additional means, such as burning.

- Access to computer, mobile device and associated electronic device operating system must be limited to DHS IT, NDIT or Human Service Zone authorized contractors to prevent changes to device configuration.
- Computers, including laptop computers, and associated electronic devices must contain remote wipe and/or kill switch functionality to remove sensitive information. If a device cannot be remotely wiped, the device must be configured to purge all data automatically after 4 consecutive unsuccessful attempts are made to gain access.
- Mobile devices, excluding laptop computers, must:
  - Contain remote wipe and/or kill switch functionality to remove sensitive information. If a device cannot be remotely wiped, the device must be configured to purge all data automatically after 10 consecutive unsuccessful attempts are made to gain access.
  - Require encryption at rest.
  - Wireless personal area networks must be disabled that allow connection to a computer via Bluetooth or near field communication (NFC) for data synchronization.
  - Access to digital camera, global positioning system (GPS) and universal serial bus (USB) interface must be disabled to the extent possible.
- If computer, mobile device, and associated electronics are lost or stolen, staff must immediately report to their supervisor and DHS EA Central Office at (701) 327-2332 or send an email to the EA Assistant Director.
- Telework and Alternative Work Site locations must be inspected annually for compliance with IRS required safeguards.
- Telework and Alternative Work Site Wireless Network Connection:
  - Avoid using wireless network connections when possible.
  - If using a wireless network connection
    - Check encryption of router; turn on encryption if off. Encryption level must be of the same standard as Federal Information Processing Standards (FIPS)-validated or National Security Agency (NSA)-approved encryption.
    - Only access secure websites (i.e. those that begin with “https”).

- A wireless intrusion detection system must be employed.
- Update login credentials on Wi-Fi router to increase complexity and uniqueness.
- Update the complexity and uniqueness of passwords for all other devices not approved by DHS IT, NDIT or Human Service Zone authorized contractors that are connected to wireless network (Alexa, Google Home, e-readers, tablets, etc.).
    - Any internet connected device can be used as an access point to all other devices connected to the wireless network.
    - If possible, disconnect all other devices from the wireless network.

6. Emailing Confidential Information 448-01-25-15-17- Repeal

Email containing sensitive and/or confidential information (Protected Health Information, PHI; or Personal Identifiable Information, PII) sent to county social service staff, the state agency, and the Social Security Administration are secure.

Email sent to other entities containing sensitive and/or confidential information (Protected Health Information, PHI; or Personal Identifiable Information, PII) must be encrypted through the Secure Mail process.

In addition, when an email containing client information (e.g. name, social security number) is sent, it must also include one of the following disclaimers. The subject line of the email should not include client identifying information:

- General Disclaimer

----------Confidentiality Statement----------

This transmission is intended only for the use of the individual to whom it is addressed and may contain information that is made confidential by law. If you are not the intended recipient, you are hereby notified any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please respond immediately to the sender and then destroy the original transmission as well as any electronic or printed copies. Thank you.

- Drug and Alcohol Disclaimer

----------Confidentiality Statement----------

~~This transmission is intended only for the use of the individual to whom it is addressed and may contain information that is made confidential by law. If you are not the intended recipient, you are hereby notified any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please respond immediately to the sender and then destroy the original transmission as well as any electronic or printed copies. Thank you.~~

~~This notice accompanies a disclosure of information concerning a client in alcohol or drug treatment, made to you with the consent of such a client. This information has been disclosed to you from records protected by Federal confidentiality rules (42 C.F.R Part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 C.F.R. Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.~~

~~Emailing FTI received through any interface is prohibited.~~

~~Upon discovery of an inadvertent disclosure of FTI by email, contact Economic Assistance central office: (701) 328 – 2332 to report an inadvertent disclosure.~~

~~Refer to 448-01-15-35 for faxing restrictions of FTI~~