




HUMAN SERVICES
DEPARTMENT

Susana Martinez, Governor
Brent Earnest, Secretary
Mary Brogdon, Director

General Information Memorandum

ISD-GI 17 -36

TO: ISD/MAD Employees
FROM: Mary Brogdon,  Director, Income Support Division
RE: Security Procedures for Handling Internal Revenue Service (IRS) Information
DATE: October 3, 2017

This memorandum provides guidance to ISD central and field offices concerning security procedures for tracking and handling Federal Tax Information (FTI) from the IRS, this includes but is not limited to Income Eligibility Verification Systems (IEVS) and Modified Adjusted Gross Income (MAGI) information.

Attachments:

- Internal Revenue Code 7213
- Internal Revenue Code 7213(a)
- Visitor Access (Sign In) Log
- IEVS FTI Key Assignment
- IRS Safeguard County Office Self Inspection Report
- Acknowledgement of Receipt and Discussion of IEVS GI
- ISD 801 Required IEVS Poster
- ISD202 Eligibility Review Interview Notice
- Internal Revenue Code 6103 (a) and (b)
- Internal Revenue Code 7431
- Restricted Area Access (Sign In) Log
- FTI Tracking Log
- Law Enforcement Sign In Log
- HSD File Encryption Procedure
- ISD-IPP 15-02

Definition of Federal Tax Information

FTI 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 Code and filed with the IRS by, on behalf of, or with respect to any person. Examples of returns include forms filed on paper or electronically, such as Forms 1040, 941, 1099, 1120 and W-2.

As outlined in the Internal Revenue Code (IRC), Section 6103, IRS tax returns and return information is confidential. The complete definition for tax returns and return information can be found in the ISD New Employee training materials — IRS Confidentiality.

For the purposes of the ISD, FTI includes IRS returns and return information provided by the IRS electronically via any computer-based information or eligibility system utilized by the Department and subsequently any computer display or screen containing return information provided by the IRS. Any screen prints from such displays are also considered FTI and are to be safeguarded by the same means as the electronic displays.

New Mexico ISD does not authorize the reproduction or printing of any screen that contains FTI.

I. Background:

Section 1137 of the Social Security Act requires that any State program funded under part A of title IV and any Medicaid program under title XIX of the Act must participate in the Income and Eligibility Verification System process. New Mexico's title IV-A (TANF) program is New Mexico Works established under the New Mexico Works Act of 1997.

At any time an employee of the Human Services Department/Income Support Division (HSD/ISD) utilizes FTI, that employee is bound to recipient(s) confidentiality laws set forth in federal and state regulations. Caseworkers utilize FTI on a daily basis to verify recipient(s) financial eligibility. This information is available through ISD's computer software (ASPEN) interfaces with the New Mexico Department of Labor with WDX and the Social Security Administration with BENDEX, WTPQ and SDX.

Another source of FTI that the state must utilize is the IRS personal tax information. The IRS provides information to the Department about reported unearned income that ISD is unable to identify by using such programs as WDX, WTPQ or SDX. FTI is bound by normal security procedures already taken by the New Mexico HSD and in addition has additional rigorous security requirements. This data set of FTI must never be disclosed to contractors.

Section IX of IRS Publication 1075 requires that state agencies receiving and using IRS FTI train employees, at least annually, of the provisions contained in §7213(a) and §7431 of the Internal Revenue Code (IRC). These sections of the IRC have been attached to this memorandum for your information and records. The provisions provide for criminal and civil penalties for the willful unauthorized disclosure, inspection or solicitation of federal tax return information.

II. Training:

A. The IRS requires that HSD personnel receive annual training that includes HSD's policies and procedures for utilizing FTI, as well as awareness training on criminal and civil penalties for unauthorized disclosure and inspection of IRS return and return information. This GI serves as part of annual awareness training of the Department's policies and procedures regarding FTI. This GI must be read as part of an overall FTI

/Affordable Care Act awareness training that is to be viewed by all ISD, ITD, and MAD employees at the time of hire and on an annual basis thereafter. Each staff member must sign an acknowledgement of receipt and understanding of this GI. Annual training consists of the following components:

1. ISD, ITD, and MAD staff must view a film produced by the IRS, "Disclosure Awareness". HSD staff can view "Disclosure Awareness" on the HSD Learning Management System (LMS) that is accessible from their desktop computers. The video must be viewed prior to receiving certification of completion for the course.
2. All staff must review a presentation on LMS. The presentation defines FTI, covers penalties (both civil and criminal), and outlines office policies and procedures for viewing, handling, and destroying (if necessary) FTI. The employee must sign an acknowledgement that they have received IRS Employee Awareness Training. This presentation will be updated annually to reflect any changes in IRS.

B. Training certification will be kept on record by both OHR and each local office.

III. Security Constraints:

- A. IRS FTI provides ISD leads to possible information about income or resources.
 1. The state agency must seek its own verification for the source indicated by that lead.
 2. The caseworker can take no action to reduce or terminate benefits based solely on FTI data.
 3. The caseworker shall not disclose to any collateral contact that the lead information came from an IRS source.
- B. FTI data retains its identity and if recorded elsewhere remains tax return information and must be secured accordingly.
 1. The name of the payor, account numbers, amount of income and like information from the IRS report must not appear in the notice to recipient(s).
 2. Making print screens containing FTI is strictly prohibited. Any notes containing tax return data must be secured each evening to locked files. Transcription of FTI data is strictly prohibited. Do not copy or document any portion of FTI data into any electronic format including, but not limited to, e-mail correspondence, facsimile, text or Word document, Excel spreadsheet, or in any comment or remarks field in ASPEN.
 3. If print screens are made in error, the HSD staff member must follow the FTI destruction procedures :
 - a. Complete the FTI tracking log.
 - b. Place the created FTI and the FTI Tracking Log in the IEVS cabinet (locked cabinet in locked room).
 4. Referrals to OIG must not note or explain that the initial information about unreported income or resources came from an IRS report.
 5. If FTI is commingled with non-tax return information, the commingled information assumes the identity of tax return information and must be safeguarded accordingly.

IV. Penalties:

- A. HSD Confidentiality:** Returns and return information, including all information from FTI reports, are considered confidential information. As such, this information is protected from disclosure in HSD's Code of Conduct. Any willful, or by reason of gross negligence, unauthorized disclosure, inspection, or solicitation of returns or return information is a violation of HSD's Code of Conduct. Any violation of HSD's Code of Conduct shall be cause for disciplinary action which could result in dismissal.
- B. Penalties for Willful Unauthorized Disclosure, Inspection or Solicitation of Tax Returns or Return Information:** All applicant/recipient information collected and used by ISD is subject to the department's rule of confidentiality. IRS tax return information is subject to additional security precautions required by the IRS. Willful unauthorized disclosure, inspection of tax returns or return information subjects the offender to certain criminal and civil penalties as indicated in the Internal Revenue Codes subsections 7213(a) and 7431.
1. **Criminal Penalties involving State Employees:**
 - a. Willful unauthorized disclosure of a return or return information is a felony upon conviction, punishable by fine "in any amount not exceeding \$5,000, or imprisonment of not more than five years, or both, together with the cost of prosecution."
 - b. Willful unauthorized inspection of return information is punishable upon conviction by fine "in any amount not exceeding \$1,000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution."
 - c. Receipt of any item of material value in exchange for any return or return information is a felony upon conviction, punishable by "in any amount not exceeding \$5,000, or imprisonment of not more than five years, or both, together with the cost of prosecution."
 2. **Civil Damages:** Any person who knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer, for other than authorized use, may be subject to civil action for damages in a district court of the United States. If found liable the defendant shall pay to the plaintiff the greater of: \$1,000 for each act of unauthorized inspection or disclosure, or the sum of: actual damages; plus punitive damages (in the case of gross negligence); plus the cost of the action.

V. Identification of Personnel in ISD Offices

- A. Issuance and wearing of Identification Badges and Visitor Logs:**
1. All ISD employees will be issued photo identification badges within 30 days from the date of hire. ISD employees are required to wear identification badges at all

times while conducting business on behalf of ISD. The identification badge should be easily visible and worn above the waist.

2. Visitors, defined as any individual including, but not limited to, family members of employees, vendors, and any State of New Mexico employee who does not work in the building he or she is entering, must enter the building through the main entrance to sign-in with the security guard or receptionist.
3. Any person in a secured area who is not wearing a badge should be referred to security or the County Director, as appropriate.
4. Visitors who are not authorized to view confidential information and/or are not conducting official business should not be able to view or access any confidential information while visiting an ISD office. All ISD employees are responsible for making sure that confidential information is protected from unauthorized access by a visitor in the building.
5. If anyone not employed at each individual county office (to include HSD employees from another office) are to be taken past a cypher locked door, with an escort, then the persons must sign the Restricted Area Access Log. The Restricted Area Access Log should be past the cypher locked door and not in the lobby.

B. Return of Identification Badges and Building Keys upon Separation

1. Upon notification of an employee's anticipated separation, the immediate supervisor will collect the building keys and employee identification badge. The supervisor will provide the badge and key to the employee each day until the last day of employment.
2. If the building entrance key is not returned by the employee, the building entrance(s) must be rekeyed or locks replaced. If the identification badge is used for entry to the building in lieu of a key and not returned, it must be disabled. If employee entry is by a cipher lock code pad, and a generic code is used, the code must be changed. If each staff member has a distinct code, the departing member's code must be disabled.

VI. Procedures:

A. County Director (CD) or Designee Responsibility:

1. Must ensure that staff is trained in accordance with this guidance and the security procedures are followed accordingly.
2. Ensure confidential information is protected from unauthorized access by a visitor in the building (i.e. workstation computer monitors are not visible from the hallway).
3. Ensure each filing cabinet, notebook, or any other items that might contain FTI must display the label, "Inspection or Disclosure Limitations", informing anyone coming in contact with the FTI of the criminal and civil penalties associated with unauthorized inspection or disclosure.
4. Store created FTI and FTI Tracking Logs in a locked file cabinet;
5. Return 100% of the created FTI and the FTI Tracking Logs to ISD central office within 45 days of receipt of the electronic IEVS report. Place in a double envelope and send the package certified mail using a tracking system to:

***HSD/ISD
Policy and Program Development Bureau
Attn: Suzanne Duran-Vigil - IEVS Coordinator
PO Box 2348
Santa Fe, NM 87504-2348***

6. All previous years "IEVS Transmittals" and "IEVS Removal Log" shall be returned to ISD Central Office at the above address.
7. Complete the "IRS Safeguard County Office Self Inspection Report".
8. Complete the "IEVS FTI Key Assignment Verification".
9. Retain five years "Visitor Access Logs/Restricted Area Access Logs" per IRS Pub. 1075.
10. Post required IEVS poster near all network printers/copiers used by ISD employees.

B. Caseworker Responsibility:

1. If the information ***has been*** previously reported by the recipient and handled appropriately by ISD:
 - a. no further case action is necessary; and
 - b. the worker records the time spent reviewing the case, indicates no action required on the electronic Tally Sheet for the categories of eligibility (COE) reviewed and closes the screen containing the FTI.
2. If the information ***has not been*** previously reported and acted upon:
 - a. the worker sends the "Eligibility Review Interview" notice (ISD202) to the recipient(s) scheduling an appointment that does not identify the specifics of the income/resource or the source of the information;
 - b. the interview does have to be face to face, and the caseworker cannot release any information regarding IEVS via the telephone.
 - c. if the recipient(s) ***does not*** keep the appointment or contact ISD to reschedule, the worker will follow the instructions in IPP 15-02, within three days of the missed appointment, to close the case;
 - d. if the recipient(s) keeps the appointment, or reschedules and keeps the appointment:
 - i. the caseworker evaluates the information indicated by the lead and takes appropriate action within 10 days of the ISD county office receiving the verification;
 - ii. the caseworker may tell the recipient(s) at interview that the information requested came from an IRS lead;
 - e. if the recipient(s) keeps the appointment, or reschedules and keeps the appointment and the caseworker suspects fraud:
 - i. the caseworker must first verify the information is correct using collateral contacts or documentation;
 - ii. the caseworker should refer the case to the Office of Inspector General (OIG); and

- iii. supply OIG with only the collateral contact and documentation provided by the recipient. IRS or IEVS data cannot be cited as the lead source on any of the documentation sent to OIG.
3. Any information provided by the recipient or collateral contacts in response to the agency inquiry is not tax return information and is afforded the standard protection of the HSD practice and procedures regarding confidentiality, and is not subject to the stricter IRS rules.
4. if the recipient calls to get information regarding the ISD 202, the caseworker ***will not*** provide any information over the phone. The caseworker will inform the recipient that the information could only be discussed in person and they will need to attend the appointment.

C. CSED Responsibility per MOU:

1. Complete safeguard inspection of ITD and DoIT at an 18 month interval or as required by IRS.
2. Provide copies of the inspection schedules and reports to ISD as updated.

D. Central Office:

1. ISD receives an electronic report with IRS tax return information. The Information Technology Division (ITD) runs the report from data provided by IRS from personal income tax returns. Central office has requested only certain information from the IRS report that would help ISD establish eligibility for active categories of assistance including TANF, General Assistance and Education Works cash assistance programs, Medicaid categories that have resource limits and SNAP cases not receiving the above listed categories. These reports are subject to the confidentiality requirements of the HSD, as well as the much higher security requirements of the IRS;
2. Maintain the IEVS Computer Matching Agreement with IRS.
3. Ensure annual training has been completed by ITD per CSED MOU.
4. Collect Acknowledgement of Receipt and Discussion of IEVS GI.
5. Collect and destroy per approved IRS standards, created FTI and the FTI Tracking Logs.
6. Prepare an annual Safeguard Security Report (SSR).
7. Compile the IEVS program cost savings report.
8. Retain necessary FTI Tracking Logs and previous years IEVS Transmittals for five years.

Please review this memorandum with all appropriate staff. Any questions concerning IEVS procedures should be directed to Suzanne Duran-Vigil at 505-827-7289 or SuzanneP.Duran-Vigi@state.nm

INTERNAL REVENUE CODE SEC. 7213

UNAUTHORIZED DISCLOSURE OF INFORMATION

(a) RETURNS AND RETURN INFORMATION

(1) FEDERAL EMPLOYEES AND OTHER PERSONS – It shall be unlawful for any officer or employee of the United States or any person described in section 6103(n) (or an officer or employee of any such person), or any former officer or employee, willfully to disclose to any person, except as authorized in this title, any return or return information [as defined in section 6103(b)]. Any violation of this paragraph shall be a felony punishable upon conviction by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution, and if such offense is committed by any officer or employee of the United States, he shall, in addition to any other punishment, be dismissed from office or discharged from employment upon conviction for such offense.

(2) STATE AND OTHER EMPLOYEES—It shall be unlawful for any person [not described in paragraph (1)] willfully to disclose to any person, except as authorized in this title, any return or return information [as defined in section 6103(b)] acquired by him or another person under subsection (d), (i)(3)(B)(i), (1)(6), (7), (8), (9), (10), (12), (15) or (16) or (m)(2), (4), (5), (6), or (7) of section 6103. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(3) OTHER PERSONS – It shall be unlawful for any person to whom any return or return information [as defined in section 6103(b)] is disclosed in a manner unauthorized by this title thereafter willfully to print or publish in any manner not provided by law any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(4) SOLICITATION – It shall be unlawful for any person willfully to offer any item of material value in exchange for any return or return information [as defined in 6103(b)] and to receive as a result of such solicitation any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(5) SHAREHOLDERS – It shall be unlawful for any person to whom return or return information [as defined in 6103(b)] is disclosed pursuant to the provisions of 6103(e)(1)(D)(iii) willfully to disclose such return or return information in any manner not provided by law. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

INTERNAL REVENUE CODE SEC. 7213A.

UNAUTHORIZED INSPECTION OF RETURNS OR RETURN INFORMATION

(a) PROHIBITIONS

(1) FEDERAL EMPLOYEES AND OTHER PERSONS – It shall be unlawful for

(A) any officer or employee of the United States, or

(B) any person described in section 6103(n) or an officer willfully to inspect, except as authorized in this title, any return or return information.

(2) STATE AND OTHER EMPLOYEES – It shall be unlawful for any person [not described in paragraph (1)] willfully to inspect, except as authorized by this title, any return information acquired by such person or another person under a provision of section 6103 referred to in section 7213(a)(2).

(b) PENALTY

(1) IN GENERAL – Any violation of subsection (a) shall be punishable upon conviction by a fine in any amount not exceeding \$1000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution.

(2) FEDERAL OFFICERS OR EMPLOYEES – An officer or employee of the United States who is convicted of any violation of subsection (a) shall, in addition to any other punishment, be dismissed from office or discharged from employment.

(c) DEFINITIONS – For purposes of this section, the terms “inspect” “return” and “return information” have respective meanings given such terms by section 6103(b).

INTERNAL REVENUE CODE SEC. 7213A.

UNAUTHORIZED INSPECTION OF RETURNS OR RETURN INFORMATION

(a) PROHIBITIONS

(1) FEDERAL EMPLOYEES AND OTHER PERSONS – It shall be unlawful for

(A) any officer or employee of the United States, or

(B) any person described in section 6103(n) or an officer willfully to inspect, except as authorized in this title, any return or return information.

(2) STATE AND OTHER EMPLOYEES – It shall be unlawful for any person [not described in paragraph (1)] willfully to inspect, except as authorized by this title, any return information acquired by such person or another person under a provision of section 6103 referred to in section 7213(a)(2).

(b) PENALTY

(1) IN GENERAL – Any violation of subsection (a) shall be punishable upon conviction by a fine in any amount not exceeding \$1000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution.

(2) FEDERAL OFFICERS OR EMPLOYEES – An officer or employee of the United States who is convicted of any violation of subsection (a) shall, in addition to any other punishment, be dismissed from office or discharged from employment.

(c) DEFINITIONS – For purposes of this section, the terms “inspect” “return” and “return information” have respective meanings given such terms by section 6103(b).



HUMAN SERVICES
DEPARTMENT

Susana Martinez, Governor
Brent Earnest, Secretary
Marilyn Martinez, Director

IEVS FTI KEY ASSIGNMENT VERIFICATION

I acknowledge that I have received the following key(s). I understand that these key(s) are used to access areas, rooms or containers used to secure FTI. I agree not to allow or contribute to the duplication of any unauthorized copies. It is my understanding that all keys assigned to me are to be returned if I change positions or leave the employment of this agency.

DATE KEY(S) ASSIGNED:

ASSIGNED KEY(S) NUMBERS:

EMPLOYEE WHO ASSIGNED KEY:

EMPLOYEE WHO RECEIVED KEY:

EMPLOYEE'S SIGNATURE:

SUPERVISOR'S SIGNATURE:

DATE KEY RETURNED:

EMPLOYEE WHO RECEIVED RETURNED KEY:

EMPLOYEE'S SIGNATURE:

SUPERVISOR'S SIGNATURE:



IRS SAFEGUARD COUNTY OFFICE SELF INSPECTION REPORT

County Office:	Person Interviewed:	Date Interviewed:
----------------	---------------------	-------------------

1. Are the IRS printouts kept in locked storage when not in actual use by eligibility staff? Yes No

Within this office, where is this storage located _____

2. Is access to the IRS printouts strictly controlled? Yes No

Who is responsible for monitoring this?

 Name: _____ Title: _____

3. Who maintains the keys to the FTI locked cabinet? _____

4. Is the IEVS FTI Key Assignment Verification Form completed and up to date? Yes No

5. Is the office building itself kept secure during working hours? Yes No

Describe the type of building security: _____

6. Is the building kept secure after working hours? Yes No

Who is responsible for monitoring this?

 Name: _____ Title: _____

7. Is federal tax information incorrectly commingled with other information? Yes No

8. Are the labels, "Inspection or Disclosure Limitations" on each filing cabinet, notebook or any other item that might contain FTI? Yes No

9. Did the reviewer personally observe safes or other secure storage containers or areas? Yes No

10. Is the responsibility for these safes or other secure storage containers or areas clearly assigned? Yes No

11. Are employees aware of the IRS security procedures and instructions? (Reviewer should briefly interview two employees.) Yes No

12. Are logs kept when the tax information is received by the county office? (logs should be viewed) Yes No

13. Disposal: Are logs kept when the tax information is sent back to Santa Fe Central Office for appropriate disposal? (view logs for appropriate entry) Yes No

CERTIFICATION		
<i>I certify the above responses are true to the best of my knowledge</i>		
<i>Signature of office Reviewer</i>	<i>Title</i>	<i>Date</i>

**DISTRIBUTION: ORIGINAL - SENT TO CENTRAL OFFICE
 COPY - KEPT IN FIELD OFFICE FOR 5 YEARS**



HUMAN SERVICES
DEPARTMENT

Susana Martinez, Governor
Brent Earnest, Secretary
Mary Brogdon, Director

Acknowledgement of Receipt and Discussion of IEVS GI 17-###

I, _____ acknowledge that I have reviewed and read the annual IEVS GI for handling the IEVS report for the tax year TY 15. I acknowledge that I have met with other county office staff members, either in a unit meeting or a general staff meeting and have discussed and understand my responsibilities and duties in the handling of the IEVS report.

Printed Staff Member Name

Printed Supervisor Name

Staff Member Signature Date

Supervisor Signature Date

County Office



IRS PENALTIES APPLY TO YOU!!

UNAUTHORIZED INSPECTION of returns or return information: It is unlawful to inspect any information (except as authorized by this title). **PENALTY** – Any violation shall be punishable upon conviction by a fine in any amount exceeding \$1,000 or imprisonment for not more than 1 year **OR** both, together with the cost of prosecution. IRC Section 7213A

UNAUTHORIZED DISCLOSURE of information, returns and return information: It is unlawful to disclose to any person, except as authorized in this title, any return or return acquired by him or another person. **PENALTY** – Any violation shall be a **FELONY** punishable by a fine in any amount exceeding \$5,000 or imprisonment of not more than 5 years **OR** both. IRC Section 7213

CIVIL DAMAGES FOR UNAUTHORIZED INSPECTION OR DISCLOSURE of returns and return information: In general, any individual who knowingly or by reason of negligence inspects or discloses any return or return information with respect to a taxpayer in violation of IRC Section 6103, such taxpayer may bring civil action for damages against such person. IRC Section 7431.

For more information, please refer to IRS Publication 1075

Report an unauthorized access or disclosure of tax information to:

IEVS Coordinator at 505-827-7274

Treasury Inspector General (TIGTA) Denver Field Office 1-303-291-6102

OR

TIGTA National Hotline 1-800-589-3718

AND

Email a Data Incident Report to the IRS Office of Safeguards Inspections at
SafeguardsReports@IRS.gov



INCOME SUPPORT DIVISION
CENTRAL ASPEN SCANNING AREA
P.O. BOX 830
BERNALILLO NM 87004
PHONE NUMBER: (800) 283-4465
FAX NUMBER: (855) 804-8960



Case Number:
Date: June 13, 2016

Eligibility Review Interview Notice Income Support Division

Dear :

The New Mexico Human Services Department has received information that you may have income or resources that were not considered when determining your eligibility for benefits. This information may or may not affect your benefits. An appointment has been set for you to come in and discuss this information with your caseworker.

Your appointment is scheduled for:

Date: June 20, 2016
Time: 3:30 PM
Location: Office Name
Caseworker: Suzanne Duran-Vigil

Please be ready to discuss information concerning the following income or resources when you come in for your interview about Unearned Income.

- | | |
|--|--|
| <input type="checkbox"/> Bank Account Interest | <input type="checkbox"/> Private Pensions or Annuities |
| <input type="checkbox"/> Credit Union Account Interest | <input type="checkbox"/> Social Security Income |
| <input type="checkbox"/> Child Support | <input checked="" type="checkbox"/> Stocks and Bonds |
| <input type="checkbox"/> Sale of Property | <input type="checkbox"/> Gambling Winnings |

If you are unable to make the appointment and have not contacted your caseworker to reschedule by June 01, 2016, your benefits may be reduced or your case closed.

If you have any questions you may contact your local ISD Office. ISD Offices are open from 8:00am to 5:00pm Mondays through Fridays except on State Government observed holidays.

Eligibility Worker Name



**INTERNAL REVENUE CODE SEC. 6103.
CONFIDENTIALITY AND DISCLOSURE OF RETURNS AND RETURN
INFORMATION.**

(a) General rule Returns and return information shall be confidential, and except as authorized by this title—

(1) no officer or employee of the United States,

(2) no officer or employee of any State, any local law enforcement agency receiving information under subsection (i)(7)(A), any local child support enforcement agency, or any local agency administering a program listed in subsection (l)(7)(D) who has or had access to returns or return information under this section, and

(3) no other person (or officer or employee thereof) who has or had access to returns or return information under subsection (e)(1)(D)(iii), paragraph (6), (12), (16), (19), (20) or

(4) (21) of subsection (l), paragraph (2) or (4)(B) of subsection (m), or subsection (n), shall disclose any return or return information obtained by him in any manner in connection with his service as such an officer or an employee or otherwise or under the provisions of this section. For purposes of this subsection, the term “officer or employee” includes a former officer or employee.

(b) Definitions For purposes of this section—

(1) Return The term “return” means any tax or information return, declaration of estimated tax, or claim for refund required by, or provided for or permitted under, the provisions of this title which is filed with the Secretary by, on behalf of, or with respect to any person, and any amendment or supplement thereto, including supporting schedules, attachments, or lists which are supplemental to, or part of, the return so filed.

(2) Return information The term “return information” means—

(A) a taxpayer’s identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, over assessments, or tax payments, whether the taxpayer’s return was, is being, or will be examined or subject to other investigation or processing, or any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with respect to the determination of the existence, or

USC Title 26, IRC 6103(a) and (b)

possible existence, of liability (or the amount thereof) of any person under this title for any tax, penalty, interest, fine, forfeiture, or other imposition, or offense,

(B) any part of any written determination or any background file document relating to such written determination (as such terms are defined in section 6110 (b)) which is not open to public inspection under section 6110,

(C) any advance pricing agreement entered into by a taxpayer and the Secretary and any background information related to such agreement or any application for an advance pricing agreement, and

(D) any agreement under section 7121, and any similar agreement, and any background information related to such an agreement or request for such an agreement, but such term does not include data in a form which cannot be associated with, or otherwise identify, directly or indirectly, a particular taxpayer. Nothing in the preceding sentence, or in any other provision of law, shall be construed to require the disclosure of standards used or to be used for the selection of returns for examination, or data used or to be used for determining such standards, if the Secretary determines that such disclosure will seriously impair assessment, collection, or enforcement under the internal revenue laws.

(3) Taxpayer return information The term “taxpayer return information” means return information as defined in paragraph (2) which is filed with, or furnished to, the Secretary by or on behalf of the taxpayer to whom such return information relates.

(4) Tax administration The term “tax administration”—

(A) means—

(i) the administration, management, conduct, direction, and supervision of the execution and application of the internal revenue laws or related statutes (or equivalent laws and statutes of a State) and tax conventions to which the United States is a party, and

(ii) the development and formulation of Federal tax policy relating to existing or proposed internal revenue laws, related statutes, and tax conventions, and

USC Title 26, IRC 6103(a) and (b)

(B) includes assessment, collection, enforcement, litigation, publication, and statistical gathering functions under such laws, statutes, or conventions.

(5) State

(A) In general The term "State" means—

(i) any of the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands,

(ii) for purposes of subsections (a)(2), (b)(4), (d)(1), (h)(4), and (p), any municipality—

(I) with a population in excess of 250,000 (as determined under the most recent decennial United States census data available),

(II) which imposes a tax on income or wages, and

(III) with which the Secretary (in his sole discretion) has entered into an agreement regarding disclosure, and

(iii) for purposes of subsections (a)(2), (b)(4), (d)(1), (h)(4), and (p), any governmental entity—

(I) which is formed and operated by a qualified group of municipalities, and

(II) with which the Secretary (in his sole discretion) has entered into an agreement regarding disclosure.

(B) Regional income tax agencies For purposes of subparagraph (A)(iii)—

(i) Qualified group of municipalities The term "qualified group of municipalities" means, with respect to any governmental entity, 2 or more municipalities—

(I) each of which imposes a tax on income or wages,

(II) each of which, under the authority of a State statute, administers the laws relating to the imposition of such taxes through such entity, and

(III) which collectively have a population in excess of 250,000 (as determined under the most recent decennial United States census data available).

(ii) References to State law, etc. For purposes of applying subparagraph (A)(iii) to the subsections referred to in such subparagraph, any reference in such subsections to State law, proceedings, or tax returns shall be treated as references to the law, proceedings, or tax returns, as the case may be, of the municipalities which form and operate the governmental entity referred to in such subparagraph.

(iii) Disclosure to contractors and other agents

Notwithstanding any other provision of this section, no return or return information shall be disclosed to any contractor or other agent of a governmental entity referred to in subparagraph (A)(iii) unless such entity, to the satisfaction of the Secretary—

(I) has requirements in effect which require each such contractor or other agent which would have access to returns or return information to provide safeguards (within the meaning of subsection (p)(4)) to protect the confidentiality of such returns or return information,

(II) agrees to conduct an on-site review every 3 years (or a mid-point review in the case of contracts or agreements of less than 3 years in duration) of each contractor or other agent to determine compliance with such requirements,

(III) submits the findings of the most recent review conducted under sub-clause (II) to the Secretary as part of the report required by subsection (p)(4)(E), and

(IV) certifies to the Secretary for the most recent annual period that such contractor or other agent is in compliance with all such requirements. The certification required by subclause (IV) shall include the name and address of each contractor and other

USC Title 26, IRC 6103(a) and (b)

agent, a description of the contract or agreement with such contractor or other agent, and the duration of such contract or agreement. The requirements of this clause shall not apply to disclosures pursuant to subsection (n) for purposes of Federal tax administration and a rule similar to the rule of subsection (p)(8)(B) shall apply for purposes of this clause.

(6) Taxpayer identity

The term “taxpayer identity” means the name of a person with respect to whom a return is filed, his mailing address, his taxpayer identifying number (as described in section 6109), or a combination thereof.

(7) Inspection

The terms “inspected” and “inspection” mean any examination of a return or return information.

(8) Disclosure

The term “disclosure” means the making known to any person in any manner whatever a return or return information.

(9) Federal agency

The term “Federal agency” means an agency within the meaning of section 551 (1) of Title 5, United States Code.

(10) Chief executive officer

The term “chief executive officer” means, with respect to any municipality, any elected official and the chief official (even if not elected) of such municipality

(11) Terrorist incident, threat, or activity

The term “terrorist incident, threat, or activity” means an incident, threat, or activity involving an act of domestic terrorism (as defined in section 2331 (5) of Title 18, United States Code) or international terrorism (as defined in section 2331(1) of such title).

INTERNAL REVENUE CODE – SEC 7431

IRC SEC. 7431 CIVIL DAMAGES FOR UNAUTHORIZED INSPECTION OR DISCLOSURE OF RETURNS AND RETURN INFORMATION.

(a) In general

(1) Inspection or Disclosure by employee of United States

If any officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against the United States in a district court of the United States.

(2) Inspection or disclosure by a person who is not an employee of United States

If any person who is not an officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103 or in violation of section 6104 (c), such taxpayer may bring a civil action for damages against such person in a district court of the United States.

(b) Exceptions No liability shall arise under this section with respect to any inspection or disclosure-

- (1) which results from good faith, but erroneous, interpretation of section 6103, or
- (2) which is requested by the taxpayer.

(c) Damages In any action brought under subsection (a), upon a finding of liability on the part of the defendant, the defendant shall be liable to the plaintiff in an amount equal to the sum of –

(1) the greater of –

(A) \$1,000 for each act of unauthorized inspection or disclosure of a return or return information with respect to which such defendant is found liable, or

(B) the sum of –

- (i) the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure, plus
- (ii) in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus

(2) the cost of the action.

(d) Period for Bringing Action Notwithstanding any other provision of law, an action to enforce any liability created under this section may be brought, without regard to the amount in controversy, at any time within 2 years after the date of discovery by the plaintiff of the unauthorized inspection or disclosure.

(e) Notification of Unlawful Inspection and Disclosure If any person is criminally charged by indictment or information with inspection or disclosure of a taxpayer's return or return information in violation of –

(1) paragraph (1) or (2) of section 7213 (a),

(2) section 7213A (a), or

(3) subparagraph (B) of section 1030(a)(2) of Title 18, United States Code, the

Secretary shall notify such taxpayer as soon as practicable of such inspection or disclosure.

(f) Definitions For purposes of this section, the terms “inspect”, “inspection”, “return” and “return information” have the respective meanings given such terms by section 6103 (b).

(g) Extension to information obtained under section 3406 For purposes of this section –

(1) any information obtained under section 3406 (including information with respect to any payee certification failure under subsection (d) thereof) shall be treated as return information, and

(2) any inspection or use of such information other than for purposes of meeting any requirement under section 3406 or (subject to the safeguards set forth in section 6103) for purposes permitted under section 6103 shall be treated as a violation of section 6103.

For purposes of subsection (b), the reference to section 6103 shall be treated as including a reference to section 6311 (e).



New Mexico Human Services Department
Information Technology Division

HSD File Encryption Procedure

Revision History

Revision Number	Revision Date	Summary of changes	Author
Draft	7/18/14	Draft	M. Ricklin
Version 1	2/23/15	Final approved version	M. Ricklin
1	4/17/17	Reviewed; no changes	M. Ricklin

INTRODUCTION

AUTHORITY

The Human Services Department (HSD) Information Technology Division's (ITD) Information Security Officer (ISO) or other designated management official, shall develop, implement and maintain a coordinated information security program for ITD including the adoption of managerial, operational, and technical security controls. The procedures are in alignment with applicable federal and state laws, Executive Orders, regulations, standards, and guidance.

PURPOSE

The purpose of this document is to provide HSD staff with the steps required for encrypting work folders and files on their workstations or laptops.

SCOPE

This procedure applies to HSD staff responsible for protecting the confidential information associated with their daily work activities. Confidential information may include Personally Identifiable Information (PII), Protected Health Information (PHI), Federal Tax Information (FTI), or information associated with personnel files or HSD operations.

BACKGROUND

ITD periodically scans the HSD network to search and report on unprotected confidential information. This is done to assure HSD is meeting the federal requirements for protection of data. Confidential information may only be accessed on a need-to-know basis, and must be protected from unlawful or accidental disclosure.

RELATION TO DIRECTIVES AND PROCEDURES

This procedure is driven by the requirements of the ITD Access Directive and the ITD System & Communications Directive. This procedure helps to satisfy the guidance of the directives pertaining to *Information Sharing (AC-21)*, and *Protection of Information at Rest (SC-28)*.

USER NOTES

- Encryption is a form of file protection which makes the content of a file unreadable. When you encrypt the file, the data within is manipulated by an encryption key and algorithm, which converts the data to unreadable content. The information is recovered using the corresponding decryption key and algorithm.
- The Encrypting File System (EFS) on Microsoft Windows is a feature that provides file system level encryption. The technology enables files to be transparently encrypted to protect confidential data from attackers with physical access to the computer.
- Encryption can be enabled by users on a per-file or per-folder basis. Encrypting a folder will encrypt the sub-folders within, as well as all the files within each sub-folder. A folder with many files will require time to complete the process. You can still work on other activities outside of the folder during the encrypting process. Once a folder is set up with EFS, any other files you create in or copy to that folder will be encrypted as well.
- Once a user is logged on successfully, access to their EFS encrypted files requires no additional authentication, as the decryption happens transparently. The encryption is tied to the logon credentials. Thus, any compromise of the user's computer password automatically leads to access to the files.
- E-mailing a file that you had previously encrypted with EFS on your workstation or laptop *fails to secure the file*. It becomes **unencrypted** and the recipient will be able to read the file. If you need to send a confidential file by e-mail, it must be individually encrypted. Note however that ISD and CSED policy prohibits transfer of FTI via email.
- Copying a file that you had previously encrypted with EFS on your workstation or laptop, to a shared server drive, *fails to secure the file*. It will become **unencrypted** and accessible to all staff that can access the share.

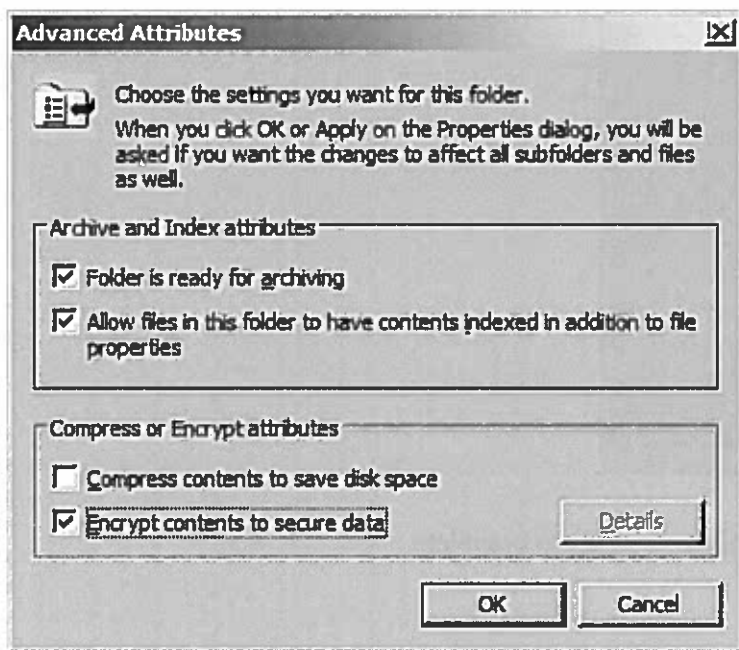
FOLDER ENCRYPTION STEPS	
	Use these steps to enable encryption at the folder level, which will encrypt all sub-folders and files within a folder on your workstation or laptop. You will not require a password to access your folders or files.
1	Right-click on the folder chosen for encryption, and click on Properties
2	Click Advanced
3	Check "Encrypt Contents to Secure Data", then click OK
4	Click Apply
5	Click "Apply changes to this folder, subfolders and files", and then click OK
6	A pop-up message will indicate the files are encrypting and the processing time remaining
7	All files created or copied to this folder are now encrypted and only accessible to the owner of the encrypted folder. The encryption is tied to your logon credentials.
INDIVIDUAL FILE ENCRYPTION STEPS	
	For individual files requiring shared access, use these steps to encrypt the files. For example, for files requiring protection on a shared server or as an e-mailed attachment.
1	Open the Word or Excel document (Word or Excel only; these steps are not applicable to Project, Power Point, or Visio files)
2	On the File tab, select "Protect Document" (or "Protect Workbook" for Excel files)
3	Select "Encrypt with Password"
4	Enter a strong password, one that you will not forget (If you forget the password you will lose access to the file content. No one can recover an encrypted file when the password is lost.)
5	Re-enter the password
6	When you save the file it can only be opened with the unique password.
7	The encrypted file can now be placed onto a shared drive or as an email attachment if needed. Use a separate communication channel to provide the password. Note: ISD and CSED policy prohibits transfer of FTI via email.

FOLDER ENCRYPTION SCREEN SHOTS

1. Right Click on the folder and select Properties



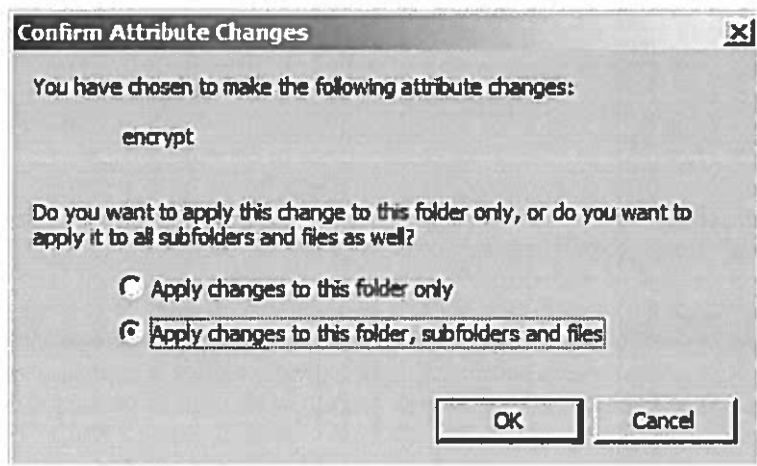
2. Click Advanced
3. Check "Encrypt Contents to Secure Data" and click OK



4. Click "Apply"



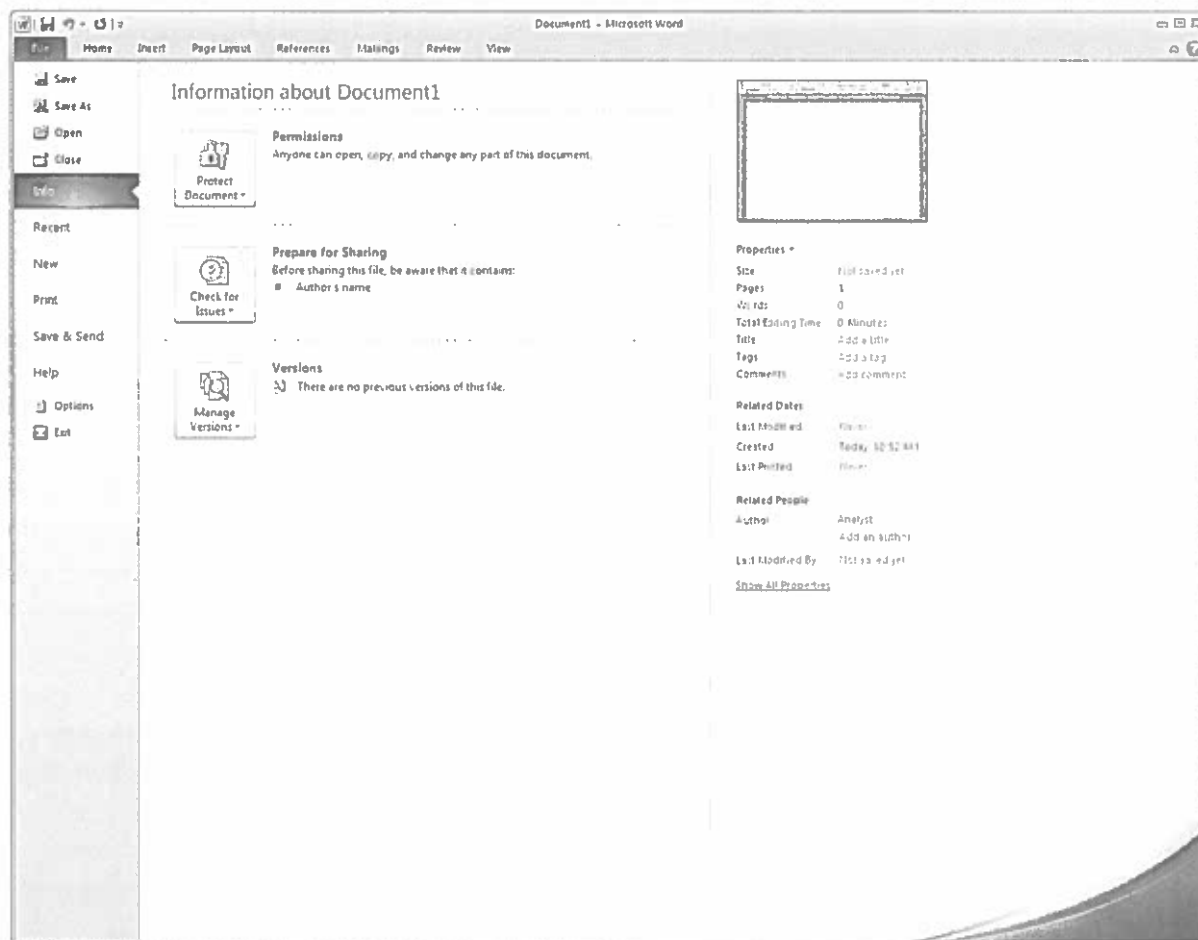
5. Click "Apply changes to this folder, subfolders and files", and click OK



6. Pop up indicates files are encrypting and remaining time to complete.

INDIVIDUAL FILE ENCRYPTION SCREEN SHOTS

1. Open the Word or Excel document
2. On the File tab, select Info, and select “Protect Document”



3. Select “Encrypt with a Password”, then enter your file password. This step will be repeated to complete the process.



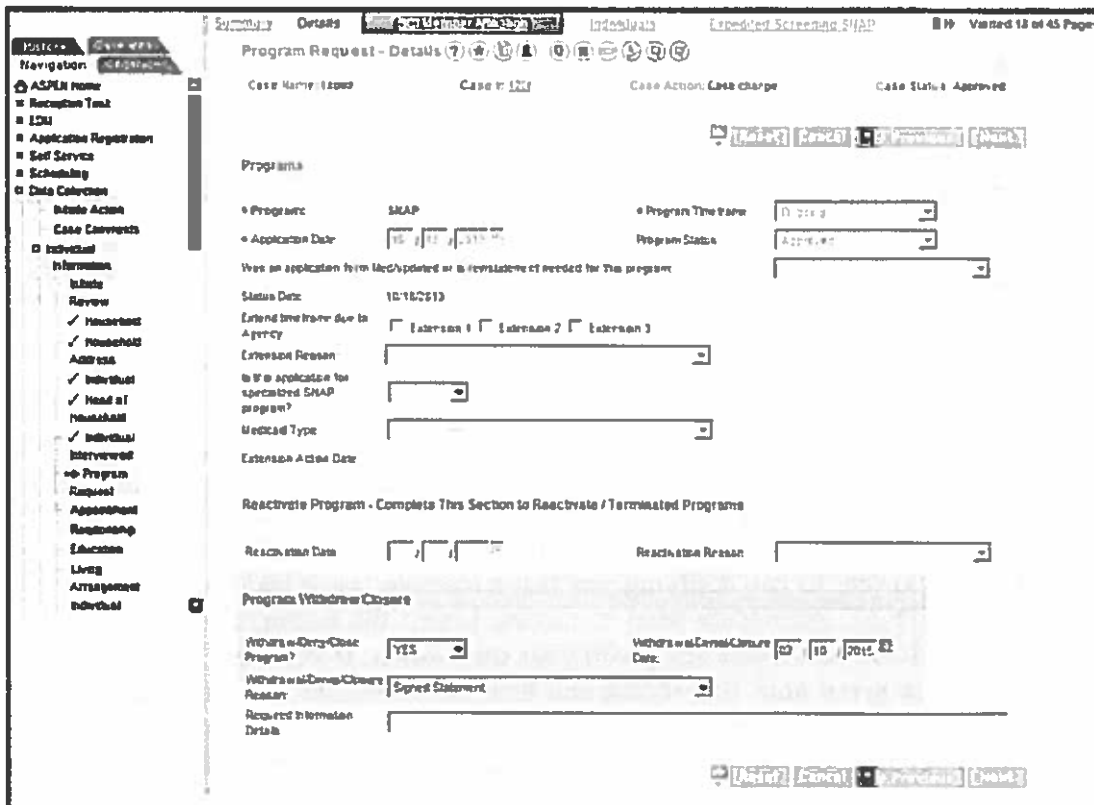
General Information Memorandum

ISD-IPP 15-02

TO: ISD Employees
FROM: *MM* Marilyn Martinez, Acting Director, Income Support Division
RE: IEVS ISD 202/ ISD 201 Closures
DATE: February 11, 2015

This IPP is to clarify the process for closing cases that failed to attend the appointment requested by ISD 202 (IEVS processing). The ISD employee must send a manual notice ISD 201 and suppress the regular notice from going out.

1. Via left navigation: Data Collection > Individual Information > Program Request Screen terminate the case using the “Deny/Withdraw/Close” section. Always close the case based on “signed statement”, see screen shot below.



2. Run EDBC and certify the closure for all programs.
3. Suppress the NOCA immediately, see screen shot below.

View Pending Correspondence Pending Correspondence Detail Visited 54 of 56

View Pending Correspondence

Search Criteria

Case: Application: Vendor: Individual ID:

Case # Application or Vendor or Individual # 1200

Search Results

Document Description	Request Date	Generate Date
ISD 1210 - Notice of Case Action	02/10/2015	02/10/2015

4. Via left navigation: Correspondence > Generate Manual, issue a manual ISD 201, Notice to Client. The notice must contain the language below, make sure to personalize only the highlighted areas. NOTE: when using the Notice to Client do not use hard returns.

ISD 201 - Notice to Client

Additional Info

Case Name Case # Case Action Case Status: App Denied

Letter

Enter the correct language here

Due Date

The New Mexico Human Services Department has received information that you may have income or resources that were not considered when determining your eligibility for benefits. An appointment notice was sent to you notifying you that a meeting was scheduled for [insert date and time from the ISD 202 previously sent] to discuss [insert the matter, i.e., your gambling earnings from the ISD 202 previously sent] with your caseworker. If you were unable to attend this meeting, you were given until [insert date and time from the ISD 202 previously sent] to contact your caseworker to reschedule this appointment. You were informed that if you did not reschedule your appointment by [insert date from the ISD 202 previously sent], your benefits

would be reduced or your case would be closed. You failed to attend this meeting, or to contact your caseworker to reschedule. Your [insert COE closing, i.e., TANF/SNAP/Medicaid] will be closed effective [insert date from the Eligibility Summary Screen], per 8.100.130.12 NMAC.

El Departamento de Servicios Humanos de Nuevo México ha recibido información que es posible que tienes ingresos o recursos que no fueron considerados al determinar su elegibilidad para los beneficios. Un aviso de cita fue enviado a usted que le notifica que una reunión estaba programada para [insert date and time from the ISD 202 previously sent] para discutir [insert the matter, i.e., your gambling earnings from the ISD 202 previously sent] con su trabajador de casos. Si usted no pudo asistir a esta reunión, que se les dio hasta [insert date and time from the ISD 202 previously sent] para ponerse en contacto con su trabajador de casos para reprogramar la cita. Se le informó que si no reprogramar su cita por [insert date from the ISD 202 previously sent], sus beneficios se reducirán o su caso se cerrará. Usted no pudo asistir a esta reunión, o ponerse en contacto con su trabajador de casos para reprogramar. Su [insert COE closing, i.e., TANF/SNAP/Medicaid] se cerrará efectiva [insert date from the Eligibility Summary Screen], por 8.100.130.12 NMAC.

5. Case comments....case comments....case comments.....

DO NOT INDICTATE IRS OR IEVS ON THE MANUAL NOTICE OR ASPEN CASE COMMENTS!

If you have questions regarding this IPP please contact Brandi E. Sandoval at (505) 827-7274
brandi.sandoval@state.nm.us