Office of Child Support
POLICY SHEET

SUBJECT

Email and Fax Policy **PS# 22-02**

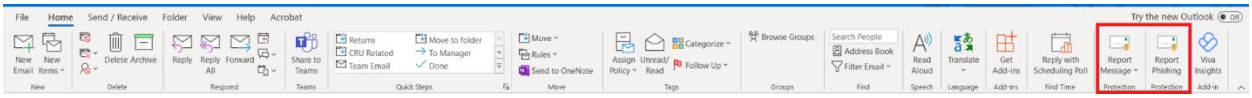
SUMMARY

It is Office of Child Support (OCS) policy to safeguard information in its possession, including but not limited to Federal Tax Information (FTI), Personal Identifiable Information (PII), Federal Parent Locator Service (FPLS) information and Private Health Information (PHI). To ensure that FTI information, either from the IRS directly or received through FPLS, is not inadvertently disclosed, it is OCS policy to not fax or email this information. PHI may be emailed using encryption.

PROCEDURES

To ensure the security of OCS' case files which contain federal tax information (FTI), personally identifiable information (PII), and personal health information (PHI), OCS staff must conform with the following requirements surrounding emailing and faxing information of this nature:

- Keep personal case information such as customer name or external case number out of the subject line. It should contain a generic label. Include the external case number in the message body to make it easier to identify the case if we get an email reply.
- Record all email correspondence in ACCESS using the CONT screen with code "E" for email.
- All email correspondence should be imaged to the case in its original format so it can be accessed.
- Emailing or faxing documents containing FTI or FPLS information is prohibited.
- When emailing Protected Health Information to an external entity, it must be encrypted.
- Suspected phishing scam emails should be reported directly through Microsoft Outlook by clicking on the appropriate buttons at the top right corner of the classic ribbon while in your mailbox or while in the specific email message.



- Additional information regarding phishing and scam emails can be found here.

Incident Response Procedure

Should an unauthorized disclosure via email or fax occur, the following procedures must be followed **IMMEDIATELY** after the disclosure occurring:

Health Insurance Portability and Accountability Act (HIPAA) & Social Security Numbers (SSN) – If there is a violation of the AHS HIPAA Standards & Guidelines, the AHS Consumer Privacy and Information Rule, or an unauthorized disclosure of an SSN that is not considered FTI or FPLS has occurred, you should talk to your supervisor about the event and notify CSP and our OCS HIPAA Liaison. You will complete the AHS Privacy/Security Event Report Form and submit it as soon as possible as specified in the form. If there is an emergency situation involving the disclosure of electronic health information and/or the security of AHS computer systems, call the phone numbers listed on the form. The AHS Privacy/Security Officer will make sure that affected parties receive proper written notice. At times, OCS may be asked to assist with the notification process. For SSN breaches, the notification shall include a description of the following:

- a description of the incident in general terms,
- the type of personal information that was disclosed to unauthorized parties,
- the steps taken to prevent future security breaches,
- a toll-free telephone number that the customer may call for further information and assistance, and
- information for the customer on how to monitor free credit reports and account activity.

Federal Tax Information (FTI) – Unauthorized disclosure of federal tax information in any form, i.e., data breaches, data incidents, information spillage, fax, email, or paper form, must be reported to your supervisor within one clock hour based on the IRS Incident Response Procedures and the OCS Incident Response Procedures. The supervisor shall notify CSP of the unauthorized disclosure of FTI within one clock hour of learning of the breach. CSP will review and report the breach to the IRS Office of Safeguards no later than 24 hours after the identified issue. Staff found responsible for the unauthorized disclosure of FTI are in violation of federal law. The penalties for such a violation include criminal penalties, punishable by fines, imprisonment or both; civil damages; and disciplinary action resulting in immediate dismissal for the most egregious offenses.

The Office of Safeguards will coordinate with OCS regarding appropriate follow-up actions required. Once the incident has been addressed, OCS shall conduct a post-incident review to ensure the incident response policies and procedures provide adequate guidance. Any identified deficiencies in the incident response policies and procedures shall be resolved and trained as soon as reasonably possible.

Federal Parent Locator Service Information (FPLS) – The FPLS is made up of two databases, the Federal Case Registry (FCR) and the National Directory of New Hires (NDNH). FPLS requests shall be made solely to locate a parent for the purpose of establishing paternity, securing child support (or where applicable, to locate a parent in a parental kidnapping case), establishing or enforcing a child custody or visitation order, and for other purposes specified in federal law and regulations.

FPLS data may be disclosed to authorized persons and entities only. As used in subsection (a) of the Social Security Act §453 the term "authorized person" means—

(1) any agent or attorney of any State or Indian tribe or tribal organization (as defined in subsections (e) and (l) of section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b)), having in effect a plan approved under this part, who has the duty or authority under such plans to seek to recover any amounts owed as child and spousal support or to seek to enforce orders providing child custody or visitation rights (including, when authorized under the State plan, any official of a political subdivision);

(2) the court which has authority to issue an order against a noncustodial parent for the support and maintenance of a child, or to issue an order against a resident parent for child custody or visitation rights, or any agent of such court;

(3) the resident parent, legal guardian, attorney, or agent of a child (other than a child receiving assistance under a State program funded under part A) (as determined by regulations prescribed by the Secretary) without regard to the existence of a court order against a noncustodial parent who has a duty to support and maintain any such child;

(4) a State agency that is administering a program operated under a State plan under subpart 1 of part B, or a State plan approved under subpart 2 of part B or under part E; and

(5) an entity designated as a Central Authority for child support enforcement in a foreign reciprocating country or a foreign treaty country for purposes specified in section 459A(c)(2).

If FPLS information is used for other purposes or disclosed improperly (in any form- i.e., data breaches, data incidents, information spillage, fax, email, or paper form), the unauthorized use or disclosure must be reported to your supervisor immediately, but no later than one hour after the identified issue. The supervisor will notify CSP to report the unauthorized disclosure to the Federal Office of Child Support Services and/or the IRS Office of Safeguards if the disclosed data is FTI.

Unauthorized use or disclosure of State Workforce Agency information obtained through the FPLS can result in criminal penalties, as well as civil. The penalty for each act of unauthorized access to, disclosure of, or use of information in the National Directory of New Hires includes an administrative penalty (up to and including dismissal of employment) and a fine of $1000. Unauthorized disclosure of FTI obtained through the FPLS is a violation of federal law which includes penalties for such a violation include criminal penalties, punishable by fines, imprisonment or both; civil damages; and disciplinary action resulting in immediate dismissal for the most egregious offenses.

RATIONALE

Much of the information received by the Office of Child Support in the course of operations is considered protected information by various laws, regulations, policies and procedures.

HIPAA requires that AHS implement procedures to carry out the HIPAA Privacy Rule. AHS calls these procedures the AHS HIPAA Standards & Guidelines. AHS staff must know how these Standards & Guidelines apply to their work and how to follow them.

Internal Revenue Code (I.R.C.) § 6103(l)(6) allows the Internal Revenue Service (IRS) to disclose federal return information to federal, state and local child support enforcement agencies for purposes of, and to the extent necessary in, establishing and collecting child support obligations from, and locating, individuals owing such obligations. This return information consists of taxpayer's social security number (or numbers, if the individual involved has more than one such number), address, filing status, amounts and nature of income, and the number of dependents reported on any return filed by, or with respect to, the individual taxpayer owing such obligations.

I.R.C. § 6103(l)(6)(B) authorizes further disclosures of return information by any federal, state or local child support enforcement agency with respect to any individual to whom child support obligations are sought to be established or enforced, to any agent of such agency which is under contract with such agency to carry out the purposes of, and to the extent necessary in, establishing and collecting child support obligations from, and locating, individuals owing such obligations. The information that can be disclosed is limited to the address, social security number (or numbers) of such individual, and the amount of any reduction under I.R.C. § 6402(c) (relating to offset of past-due support against overpayments) in any overpayment otherwise payable to such individual.

As a condition for receiving federal return information, recipient agencies are required by Federal Safeguards Requirements pursuant to I.R.C. § 6103(p)(4) to establish and maintain, to the satisfaction of the IRS, safeguards designed to prevent unauthorized access, disclosure, and use of all return information and to maintain the confidentiality of that information. These requirements are outlined in IRS Publication 1075. IRS Publication 1075 and AHS Policy Sheet 5.26 outline the process and requirements surrounding background checks for staff accessing FTI.

The Social Security Number Protection Act (9 V.S.A. § 2440(d)) says that the state and any state agency, political subdivisions of the state, and agent or employee of the state, may not collect a social security number from an individual unless authorized or required by law to do so; use the social security number for any purpose other than the purpose set forth in the statement required under subdivision (3) of this subsection; intentionally communicate or otherwise make available to the general public a person's social security number; or print an individual's social security number on any materials that are mailed to the individual, unless a state or federal law, regulation, or grant agreement requires that the social security number be on the document to be mailed. A social security number that is permitted to be mailed under this subdivision may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on an envelope, without the envelope having been opened.

9 V.S.A. § 2440(e) further states that social security numbers may be disclosed to another governmental entity if disclosure is necessary for the state to perform its duties and responsibilities including necessary administrative purposes and internal verifications. Social security numbers disclosed pursuant to a court order, warrant or subpoena or in response to a valid discovery request pursuant to rules applicable to a court or administrative body that has jurisdiction over the disclosing entity is allowed.

26 U.S.C. §§ 7213(a)(2) and (b)(2) states that unauthorized use or disclosure of federal tax information obtained through the FPLS could result in criminal penalties and dismissal from employment.

42 U.S.C. § 653(1)(2) states that the penalty for each act of unauthorized access to, disclosure of, or use of information in the National Directory of New Hires shall include an administrative penalty (up to and including dismissal of employment) and a fine of $1000.

Date	Action	Description
04/14/2022	Created	
08/15/2023	Revised	Applied standard formatting and updated all hyperlinks
/08/25/2023	Revised	Updated FPLS information to provide additional details and to clarify reporting for potential breach occurrences; removed requirement to contact the Treasury Inspector General for Tax Administration (TIGTA) based on Security and Privacy Alert Memo from IRS Office of Safeguards, effective 8/21/23
08/30/2023	Revised	Updated the hyperlink to feature the recently updated OCS Incident Response Procedure
09/06/2023	Revised	Updated hyperlink to resources regarding email phishing spam reporting based on updated ADS Policy released 9/6/23
12/29/2023	Revised	Updated reference reporting potential FPLS breaches to be directed to OCSS and/or IRS Office of Safeguards
01/04/2024	Revised	Updated hyperlinks throughout document