FSSA Privacy & Security Office
Incident Notification Procedures

Notification Summary Table

Entity	Notice Timing	Incident Status	Comment	Page#
CMS Emergency Disconnect (federal data exchange)	Immediate—driven by FSSA	Suspected or Confirmed	Emergency disconnect of exchange if security issue suspected with the data exchange	2
CMS (federal data exchange)	1 hour	Suspected or Confirmed	Applies to PHI/PII received from Federal Data Services Hub	2-3
Social Security Administration (SSA)	1 hour	Suspected or Confirmed	Multiple SSA points of contact to notify	3-4
Office of Child Support Enforcement (federal data exchange)	1 hour	Suspected or Confirmed	Applies to OCSE National Directory of New Hires (NDNH) data	5
Department of Workforce Development	2 hours	Suspected or Confirmed	Applies to data exchanges when FSSA is a requesting agency as defined under 20 CFR 603.21(e)	6
ISDH data exchanges with FSSA	2 hour verbal notification followed by written notice within 24 hours	Confirmed	Applies to individually identifiable data provided to FSSA by ISDH via data exchange	7
IRS (FTI data)	24 hours	Suspected or Confirmed	Multiple IRS points of contact to notify	8-9
Attorney General	2 days	Suspected or Confirmed	Applies to SSN disclosures	10
Individual—SSN or other IC 4-1-11 personal information	Within 30 days	Confirmed		10
HHS/OCR	60 days from end of calendar year for breaches involving <500 individuals; Contemporaneous with notice to individual for breaches involving 500+ individuals	Confirmed	Applies to PHI breaches	11
Individual—PHI	Within 60 days	Confirmed		11

FSSA Privacy & Security Office
Incident Notification Procedures

Background:

These FSSA Privacy & Security Office Incident Notification Procedures supplement the FSSA Privacy & Security Compliance Policies and Procedures and, in particular, Sections 5.4, 5.7 and 5.8 thereof.

CMS emergency disconnect of the system-to-system connection with CMS (for federal data exchange):

If there is a suspected security incident or event that may warrant an emergency disconnect of the Connecting Entity's system-to-system connection with CMS:

Notify CMS IT Service Desk:

410-786-2580; 800-562-1963
Or, by email to CMS_IT_Service_Desk@cms.hhs.gov

Upon resolution of the incident, an "after action report" will be presented to the CMS ISSO in order to reestablish the connection.

CMS (Centers for Medicare & Medicaid Services) regarding federal exchange data under ACA:

Within one (1) hour of discovery of suspected or confirmed incidents notify:

1. Email CMS IT Service Desk at cms_it_service_desk@cms.hhs.gov

2. If unable to report incidents to the CMS IT Service Desk, contact the CMT IT Service Desk by phone: 800-562-1963 or 410-786-2580

3. Complete and submit to the CMS IT Service Desk the CMS ACA Security and Privacy Incident Report using the CMS ACA Security and Privacy Incident Report template:

   

   ACA_Incident_Report_Template_v2_11.d

4. Submit electronic after-action reports to the CMS Information Systems Security Officers (ISSOs) after the incident is resolved.

Incident = An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Breach = The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where (1) a person other than an authorized user accesses

personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized.

Reference: OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* and the Computer Matching Agreement between CMS and FSSA/DFR.

Social Security Administration—SSA Data DFR Eligibility Systems and Voc Rehab

Within one (1) hour of discovery of suspected or confirmed breach or loss of PII or a security incident which includes SSA-provided data, notify:

1. **US-CERT** (United States Computer Emergency Readiness Team): 888-282-0870; www.us-cert.gov, click on "Report an Incident"

2. **SSA System Security Contact:** Jennifer Rutz
   Director, Office of Information Security
   Division of Compliance and Oversight
   Suite 3383 Perimeter East Building
   6201 Security Boulevard
   Baltimore, MD 21235
   410-966-8253
   Jennifer.Rutz@ssa.gov

3. **SSA Chicago Regional Office:** Latrice Ivy
   Data Exchange Coordinator, CDIPS
   600 W. Madison, 10th Floor
   Chicago, IL 60661
   312-575-4693
   Latrice.Ivy@ssa.gov

4. If unable to make contact with the SSA System Security Contact or the SSA Chicago Regional Contact within one hour after attempting to make contact, call the SSA National Network Service Center (NNSC) 877-697-4889 (select "Security and PII Reporting" from options list).

5. As the final option, in the event SSA contacts and NNSC both cannot be reached, contact SSA's Office of Information Security, Security Operations Center (SOC) toll-free at 1-866-718-6425.

FSSA Privacy & Security Office
Incident Notification Procedures

Use the worksheet, attached as Attachment 6, to the SSA Information Exchange Agreement to gather and organize the incident information and provide the SSA with timely updates as any additional information about the incident becomes available.

Breach = Refers to the actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII or Covered Information, whether physical, electronic, or in spoken word or recording.

Security Breach = An act from outside the organization that bypasses or contravenes security policies, practices, or procedures.

Security Incident = A fact or event which signifies the possibility that a breach of security may be taking place, or may have taken place. All threats are security incidents, but not all security incidents are threats.

Reference: Information Exchange Agreement between SSA and FSSA, Section I.2 and Attachment 6

Associated Issue: Clear identification of the location of SSA data within DFR Eligibility Systems, IRIS, and Claims Tracker (the latter two are Voc Rehab systems)—i.e., how determine if breached?

Incident Reporting:

Notify the SSA Regional Office Contact or the SSA Systems Security Contact if there is a possible or suspected loss of SSA PII. If, for any reason, the responsible State official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact within one hour, the responsible State Agency official or delegate must report the incident by contacting SSA's National Network Service Center (NNSC) toll free at 1-877-697-4889 (select "Security and PII Reporting" from the options list). As the final option, in the event SSA contacts and NNSC both cannot be reached, the Organization is to contact SSA's Office of Information Security, Security Operations Center (SOC) tollfree at 1-866-718-6425.

Office of Child Support Enforcement (NDNH Data)

Within one (1) hour of discovery of a breach or suspected breach (confirmed or suspected incidents) that includes NDNH data, notify:

Linda Boyer
FPLS Information Security Officer
Division of Federal Systems
Office of Child Support Enforcement
Administration for Children and Families
Mary E. Switzer Building
330 C Street SW, 5th Floor
Washington, DC 20201
Phone: 202-401-5410
Fax: 202-401-5533
Email: linda.boyer@acf.hhs.gov

Secondary contact: Danny Markley Danny.Markley@acf.hhs.gov

Reference: Computer Matching Agreement between HHS/ACF/OCSE and FSSA/DFR, Security Addendum, Section IV

Department of Workforce Development Data Exchanges

Reporting of Security Incident to DWD. FSSA, in collaboration with FSSA Privacy Office shall report to DWD any security incident of which the FSSA becomes aware. Successful breaches of security shall be reported by FSSA Privacy Office to the DWD Security Officer by calling (317) 232-7596 within two (2) hours of becoming aware of the breach and in electronic form to PrivacyandSecurityOfficers@DWD.in.gov within twenty-four (24) hours of becoming aware of the breach. If the FSSA Privacy Office is unable to reach the DWD Security Manager at the above phone number, then the FSSA Privacy Office will report successful breaches of security to the Chief Information Officer by calling (317) 234-8371 within the same timeframes indicated above. In the event a successful breach is discovered outside of normal business hours, leaving a voice message at the above listed numbers is sufficient verbal notification; however, FSSA in collaboration with the FSSA Privacy Office shall still comply with the electronic reporting requirement stated above.

The following format should be used when reporting the breach electronically:

- **Name of Agency**
  Incident # (number assigned by reporting entity)

- **Type of Incident –**
  1. Date and Time of Report (Date and time incident was initially reported)
  2. Date and Time of Incident (Date and time incident occurred)
  3. Time potential breach was identified

- **Name and Title of Person Reporting Incident**
  Contact Information (of person reporting incident)

- **Summary of Incident** (Include pertinent information regarding the potential security breach)

- **Description of Personally Identifiable Information Involved** (Include number of participants records involved)

- **Action Taken**

  1. Name of Person(s) Conducting Preliminary Investigation
  2. Contact Information (of individual responsible for Issue Analysis)
  3. Date Investigation started
  4. Action(s) Taken (include dates, times, and names of agencies notified of the Incident)

- **Conclusion**
  Measures taken to address issue, and prevent any reoccurrences

Indiana State Department of Health (ISDH) regarding Data Exchanges

For personally identifiable information, including PHI, provided to FSSA by ISDH as part of a data exchange:

Within two (2) hours of when a breach is confirmed, notify the ISDH Security Manager by phone at 317-233-4945.

Within twenty-four (24) hours of when a breach is confirmed, provide details of the breach to the ISDH Security Manager by email at PrivacyandSecurityOfficers@ISDH.in.gov. Reference the MOU for relevant details.

Reference: Master Memorandum of Understanding between FSSA and ISDH regarding data exchanges. Note, other MOU's may be in place that either have not yet been incorporated into the master or may have financial exchanges requiring a separate MOU—the specific MOU should be referenced for disclosure notice guidance.

Associated Issue: Identification and location of ISDH data; as the exchanges progress some of the ISDH-provided data may become integrated with FSSA systems, data warehouse repositories, etc. Note: the responsibility for addressing breaches of data provided by ISDH (e.g., notice to victims) is FSSA's.

Internal Revenue Service—Federal Tax Information Disclosure

Within twenty-four (24) hours of discovering a possible improper inspection or disclosure of FTI, including breaches and security incidents, perform the following notification procedures:

1. **Call the local TIGTA (Treasury Inspector General for Tax Administration) Field Division Office first: https://www.treasury.gov/tigta/oi_office.shtml**

   If unable to contact the local TIGTA Field Division, contact the Hotline Number:

   - **Hotline:** 800-366-4484
   - **TIGTA Homepage:** http://www.treasury.gov/tigta/index.shtml

   Mailing Address:

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

   Concurrent with contacting the TIGTA, notify the IRS Office of Safeguards:

   Data Incident Report: submit a Data Incident Report to SafeguardReports@IRS.gov using the IRS approved encryption techniques (encrypt file using MS Word encryption, password is standard password—see FSSA Privacy Officer); subject line = Data Incident Report; do not include any FTI in the data incident report.

   Reference Publication 1075, Section 1.8.3 for Data Incident Report content requirements and Section 2.E.2 Encryption Requirements

If the incident involves intrusions, manipulations or compromises of computer networks, as well as external cyber-based actions that interfere with the IRS's ability to conduct electronic tax administration, or any breach that involves unauthorized disclosure within an IT environment, contact TIGTA Electronic Crimes & Intelligence Division at cybercrimes@tigta.treas.gov. See Notification of Impacted Individuals (following) for additional notification requirements.

Notification of Impacted Individuals:

Include the following statement with the initial notification:

"As part of FSSA's continuing investigation into the incident the agency will make a determination as to whether an employee (or other individual under FSSA's control) was directly involved (i.e., maliciously or accidentally caused or committed an unauthorized inspection or disclosure of return information) and, in conjunction with FSSA human resources, determine whether adverse

or disciplinary action is warranted; and, will keep the IRS Office of Safeguards apprised accordingly. Should adverse or disciplinary action be warranted, the agency will provide notice to the impacted individual(s) and work with the IRS Office of Safeguards regarding the notification process."

Background regarding the above inclusion: Pursuant to IRS Interim Guidance – Taxpayer First Act, Section 3002, individuals impacted by the improper inspection or disclosure of their return information (FTI) are to be notified when an agency proposes disciplinary or adverse action against an employee arising from the employee's unauthorized inspection or disclosure of the taxpayer's return or return information. This guidance requires agencies to work cooperatively with the IRS Office of Safeguards regarding the notification procedures once a determination is made to take adverse or disciplinary action against the employee until the IRS provides final guidance on these notification procedures.

Reference: IRS Publication 1075, Section 1.8.5 *Incident Response Notification to Impacted Individuals* and Section 1.8 *Reporting Improper Inspections or Disclosures*. IRS Security and Privacy Alert, February 20, 2020, Interim Guidance – Taxpayer First Act, Section 3002.

Other IRS Notification Requirements: Reference IRS Publication 1075, Section 2.E.6 regarding other notification requirements.

Office of the State Attorney General/Individual for SSN disclosure

Within two (2) business days of the disclosure, notify the Office of the Attorney General in writing of the following:

1. The nature of any release of Social Security Numbers or other personal identifying information
2. Steps taken by the agency or employee to do the following:
    a. Stop the current release
    b. Notify the individuals affected
    c. Prevent future releases

Notice to OAG Identity Theft Unit via pdf form; can be done by sending a secure email to databreach@atg.in.gov.

Within thirty (30) days of the disclosure provide written notice to the individuals affected by the disclosure.

References:

1. IC 4-1-10, release of Social Security Number in violation of IC 4-1-10 (i.e., not permitted by law)
2. IC 4-1-11-5: notice to individual without unreasonable delay (guidance from OAG is 30 days).
3. 10 IAC 5-4-1 Notification to Attorney General

Associated Issue: Timely notification to FSSA Privacy Office by DFR field offices, OMPP, DMHA, DDRS, and business associates (e.g., HP, Xerox, First Data, etc.).

Breach of the Security of the System—IC 4-1-11

This law requires notice to the individual without unreasonable delay upon the breach of the security of a system from which personal information has been disclosed.

Breach = unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a state or local agency. It excludes (1) good faith acquisition of personal information by an agency or employee for purposes of the agency, if the personal information is not used or subject to further unauthorized disclosure; and, (2) unauthorized acquisition of a portable electronic device on which personal information is stored if access to the device is protected by a password that has not been disclosed (*assumes a complex password and assumes the data cannot be otherwise accessed*).

Personal Information = first name or initial and last name and at least one of the following three: (1) Social Security Number, (2) Driver's license number or identification card number, (3) account number, credit card number, debit card number, security code, access code, or password of an individual's financial account. Note: IC 4-1-6 has an expanded definition of Personal Information.

US Department of Health & Human Services/Office for Civil Rights/Individual (PHI Breach)

To the individual: written notice within 60 days after discovery of the breach

- If insufficient or out-of-date contact information for 10 or more individuals, substitute notice is required: (a) conspicuous posting for 90 days on website or conspicuous notice in major print or broadcast media; (b) toll-free number available for 90 days for questions

To the Secretary of HHS (via the OCR Breach Reporting website (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html):

1. For breaches involving less than 500 individuals: not later than 60 days after the end of each calendar year
2. For breaches involving 500 or more individuals: contemporaneous with notice to the individual

To the media for breaches involving 500 or more individuals—reference 45 CFR 164.406 for details

Breach = the acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

Reference: 45 CFR 164 Subpart D (HIPAA Breach Rule)

Associated Issue: Timely notification to FSSA Privacy Office by DFR field offices, OMPP, DMHA, DDRS, and business associates (e.g., DXC, Conduent, Deloitte, etc.).