



Family & Social Services Administration

Privacy Compliance Policies

Version 1.0

Effective: December 31, 2012

Contents

Introduction—Privacy Compliance Policies	1
Section 1: Use and Disclosure Policy.....	2
Section 2: FSSA Privacy Office	6
Section 3: Business Unit Privacy Policies & Procedures.....	7
Section 4: Privacy/Security Liaisons.....	9
Section 5: Incident Management & Breach Reporting Policy.....	11
Section 5.1: Central Response and Reporting Management.....	12
Section 5.2: Privacy/Security Incident Staff Notification Requirements	13
Section 5.3: Privacy/Security Incident Investigation.....	16
Section 5.4: Privacy/Security Incident Determination.....	20
Section 5.5: Breach Notification	24
Section 5.6: Mitigation & Corrective Actions.....	27
Section 5.7: Notice to HHS.....	31
Section 6: E-mail Policy	33
Section 6.1: E-mail Rules.....	34
Section 6.2: E-mail Security.....	37
Section 6.3: Using a Scanner to Scan/Send Client Personal Information	40
Section 7: Laptop & Portable Device Policy	41
Section 8: Fax Policy.....	49
Section 9: Computer & Paper & Media Disposal	52
Section 10: Training Requirements.....	54
Section 11: Staff Protection from Retaliatory Acts.....	55
Section 12: Sanctions for Policy Violation.....	56
Section 13: Retention Policy	57
Section 14: Definitions	58
Section 15: Citations & Authorities.....	68
Section 16: Policy Administration	69

Introduction—Privacy Compliance Policies

Purpose

The purpose of these Privacy Compliance Policies and Procedures is to establish the rules and procedures to be followed by the Family & Social Services Administration (FSSA) and its personnel to ensure the confidentiality, security, and integrity of a [client's personal information](#) in FSSA's [safekeeping](#).

Application

These Privacy Compliance Policies apply to all FSSA divisions, bureaus, sections, facilities (including State Operated Facilities, or SOF's), and program areas and all FSSA personnel ([workforce members](#)). These Policies apply to all forms of client personal information, including electronic and paper, and as may be included in verbal communications.

Background

By the very nature of its business, FSSA creates, obtains, uses, and maintains a significant amount of client personal information, including [health information](#), on individuals who are the beneficiaries of FSSA's services. This includes client personal information on former beneficiaries and those applying for services, as well as personal information on persons associated with current and former beneficiaries and those applying for services (e.g., parent and guardian information).

FSSA is obligated under both federal and Indiana state laws and regulations to protect the confidentiality and integrity of a client's personal information in its safekeeping. This is a substantive responsibility that the agency takes very seriously. It is also a complex responsibility given the scale and scope of the agency and the population we serve.

Premise

FSSA has many [business units](#) that operate under both agency-wide policies and procedures and policies and procedures unique to each unit. Agency-wide policies establish a set of rules applicable to all components of the agency and all agency personnel. These rules are necessary to ensure consistency among the various FSSA business units and staff with respect to the ongoing protection of client personal information, and the agency's ongoing compliance with the various federal and state laws and regulations applicable to the agency as whole.

Section 1: Use and Disclosure Policy

Purpose

This policy establishes FSSA's general use and disclosure policy regarding all [client personal information](#) in FSSA's [safekeeping](#).

Policy

FSSA staff may only access, use, and [disclose](#) client personal information as authorized and permitted by the applicable business unit's policies and procedures. Any access to, use of, or disclosure of client personal information not authorized or permitted by such policies and procedures is strictly prohibited and constitutes a violation of these Privacy Compliance Policies.

FSSA staff may not disclose a client's personal information to anyone except to:

1. The individual to whom the personal information belongs.
 - 1.1. The individual has a right to see and get a copy of their client personal information.
2. The individual's Authorized Representative as identified in the individual's case file and subject to any limitations identified in the case file (e.g., the individual may have indicated that their Authorized Representative may only receive notices on their behalf).
3. The individual's parent or legal guardian if the individual is an unemancipated minor.
4. The individual's parent or legal guardian if the individual is a dependent adult and such is indicated in their file.
5. The individual's designated agent under a valid power-of-attorney, subject to the limitations, if any, in the power-of-attorney.
6. Persons or organizations authorized in writing by the individual to receive their client personal information:
 - 6.1. A signed and valid authorization form must be on file for the individual.
 - 6.2. The types of client personal information that may be disclosed under the authorization must be limited to the client personal information so identified on the authorization form.
 - 6.3. Each division and business unit has an authorization form in place specific to that division or business unit. The appropriate form applicable to the division or business unit is the form that must be signed by the individual in order for the division/business unit to disclose the client personal information.
7. Co-workers who are authorized by the business unit's policies to see and use the client personal information.
8. Other FSSA business units that have a lawful purpose to see and use the client personal information, as defined in the originating business unit's policies; such disclosures may be subject to a valid Memorandum of Understanding between the business units.

Section 1: Use and Disclosure Policy

FSSA Privacy Compliance Policies & Procedures

9. Other state agencies that have a lawful purpose to see and use the client personal information, as defined in the originating business unit's policies and subject to a valid Memorandum of Understanding between FSSA and the other state agency being in place.
 - 9.1. Client personal information may not be disclosed to other state agencies absent a valid Memorandum of Understanding being in place; other state agencies are not necessarily covered under the same federal and state laws and regulations as FSSA.
10. Contractors that are authorized to see and use the client personal information, subject to a written [Business Associate](#) Agreement with FSSA that allows the disclosure. The terms of the Business Associate Agreement must be approved by the FSSA Privacy Officer.
11. Providers who provide services to FSSA clients and have a direct treatment relationship with the individual (e.g., physicians, hospitals, mental health centers, physical therapists, etc.).
 - 11.1. If there is no existing or anticipated direct treatment relationship in place, client personal information cannot be disclosed to a provider simply because they are a provider.
 - 11.2. Note that minimum necessary does not apply with respect to disclosing client medical information and benefits coverage to providers.
12. Legitimate research organizations subject to a valid Data Use Agreement between FSSA and the research organization that includes an appropriate Institutional Review Board waiver.
13. The FSSA Privacy Officer/HIPAA Compliance Officer as may be necessary to investigate and manage improper disclosures of client personal information.
14. As otherwise required by law and permitted under the applicable state and federal regulations.
 - 14.1. The FSSA Privacy Officer can provide guidance regarding other permitted disclosures.

Disclosures for legislative inquiries: Disclosures of any client personal information to Legislators or their staff requires the completion of the "AUTHORIZATION TO ACT ON CONSTITUENTS'S Behalf Form" (State Form # 54530 (12-10)) by the client or their personal representative. Any alternate authorization forms must be approved by the FSSA Privacy Officer prior to the disclosure.



54530_HIPAA
Legislative Form.pdf

Minimum Necessary: All uses and disclosures of client personal information by FSSA, including FSSA's own use of client personal information, will be limited to the minimum information necessary to fulfill the purpose of the use or disclosure as defined in the business unit's policies, with the exception of disclosures to the individual or others as identified in policy statements 2 – 5 and 11 above.

Verification: When a client or their representative calls in we are required by federal regulations to verify their identity before disclosing any client personal information. Have them tell you¹:

¹ A business unit may require alternative identity verification procedures based on the unit's requirements.

Section 1: Use and Disclosure Policy

FSSA Privacy Compliance Policies & Procedures

1. Case Number or RID Number
2. Client's full name
3. Client's date of birth
4. Last four digits of the client's Social Security Number
5. If a representative is calling:
 - a. If it is an Authorized Representative, be sure a valid AR form is on file
 - b. If it is a parent or guardian:
 - i. For unemancipated minors, they are the legal parent (rights have not been terminated) or guardian as identified in the case file;
 - ii. For dependent adults, they are the legal parent or guardian as identified in the case file.
 - c. If another type of representative (e.g., have power-of-attorney, the client's attorney, etc.), that supporting documentation is in the case file.

If there is any doubt about the client's identity, ask for additional identifying information (e.g., full SSN, complete address, etc.).

If you are on the phone with a client or in a face-to-face interview and there are others on the call or at the interview (who are not verified as the client's Authorized Representative or parent/guardian), obtain the client's verbal permission to discuss the client's personal information in front of the others and document that permission in the case notes.

Additional Restrictions: Disclosure of certain client personal information may be further limited under applicable business unit policy (e.g., the Division of Mental Health & Addiction has more restrictive disclosure policies for certain members of its service population) and other FSSA policies.

Individual Responsibility: It is each FSSA staff member's responsibility to ensure that client personal information is only used and disclosed in accordance with this policy and in accordance with the staff member's business unit's policy. When in doubt, ask your supervisor for guidance and/or seek clarification with the FSSA Privacy Officer.

No personal use: It is a **direct violation of this policy for a FSSA staff member to use any client personal information in FSSA's safekeeping for personal reasons or personal gain.** In addition, any use of client personal information in FSSA's safekeeping for a staff member's personal reasons or personal gain may subject the staff person to significant civil and criminal penalties under state and federal law, as well as sanctions under FSSA and state policy.

Social Media: At no time may a FSSA staff member post any client personal information or make any references to clients on any social media account or page, including but not limited to Internet forums, weblogs, social blogs, micro blogs, wikis, podcasts, photo pages, and other permutations. Examples of social media include, but are certainly not limited to Facebook, Twitter, LinkedIn, Plaxo, Google+, Yelp, Yammer, MySpace, and YouTube.

Doing so is a **direct violation of these Privacy Compliance Policies** and may subject the staff member to sanctions in accordance with state and FSSA policy, as well as criminal and civil penalties.

Section 1: Use and Disclosure Policy

FSSA Privacy Compliance Policies & Procedures

Note: this does not mean you cannot post information about your family or friends who may be FSSA clients provided the posting in no way states or infers that the person is a client and receives benefits; additionally, you are prohibited from accessing any FSSA information regarding your family or friends.

Training Materials, Policy Documents, and Other Guidance: Client personal information is prohibited from being used in any training materials, policy and procedure documents, provider and user guides, training web pages or applications, or other guidance materials prepared by a FSSA division/business unit. This includes examples and any other permutations in which client personal information is presented or displayed. Exceptions to this policy require written permission of the FSSA Privacy Officer.

Test Data: Client personal information is prohibited from being used for information system testing under any scenario or condition. Exceptions to this policy require written permission and risk acceptance by the applicable Division Director and written concurrence by the FSSA Privacy Officer.

Guidance: The FSSA Privacy Officer can provide additional guidance on use and disclosure rules.

Procedures

Each FSSA business unit will develop/update its policies and procedures to further identify permitted and not permitted uses and disclosures of client personal information, including applicable minimum necessary provisions.

Section 2: FSSA Privacy Office

Purpose

It is a regulatory requirement (reference §164.530(a) of the HIPAA Privacy Rule) that FSSA designate a Privacy Officer responsible for the development and implementation of the privacy policies and procedures of the agency.

Policy

FSSA shall designate a Privacy Officer (also referred to as the HIPAA Compliance Officer) responsible for the development and promulgation of agency's privacy policies and procedures, and assuring FSSA's ongoing compliance with the various federal and state privacy laws and regulations applicable to FSSA.

The FSSA Privacy Officer is in-charge of and responsible for the FSSA Privacy Office, including any staff assigned to the Privacy Office. The Privacy Officer may delegate certain responsibilities and authorities to Privacy Office staff, at his or her sole discretion.

The FSSA Privacy Officer is responsible for and is authorized to oversee, direct, and control the agency's response, in collaboration with FSSA management, to any and all known or suspected [privacy/security incidents](#), including the associated actions of contractors involved in any such privacy/security incidents.

The FSSA Privacy Officer shall serve as the agency's primary point of contact regarding privacy complaints, interactions with the US Department of Health and Human Services/Office of Civil Rights and/or the Indiana Attorney General's Office regarding privacy compliance matters, contractor notifications to FSSA of known or suspected security and/or privacy incidents, and similar items.

The FSSA Privacy Officer shall collaborate with FSSA management, including division management, on the development and implementation of Business Unit Privacy Policies & Procedures (reference Section 3), the appointment of Privacy/Security Liaisons (reference Section 4), and other privacy and security matters.

The FSSA Privacy Officer will coordinate with the Indiana Office of Technology (IOT) and the FSSA Division of Technology Services (DTS) for implementation of any required technical standards.

The FSSA Privacy Officer's other responsibilities are identified throughout these Privacy Compliance Policies.

Procedures

The FSSA Privacy Officer will prepare procedures applicable to the Privacy Officer's duties and responsibilities as identified throughout these Privacy Compliance Policies.

Section 3: Business Unit Privacy Policies & Procedures

Purpose

These Privacy Compliance Policies and Procedures apply to all FSSA divisions, bureaus, sections, facilities, and program areas (collectively and individually, “business units”) and all FSSA personnel.

The agency-wide policies also provide a framework for the development and promulgation of policies and procedures by and unique to each business unit. The purpose of this policy and its supporting procedures is to establish the requirement that all FSSA business units are responsible to develop and promulgate subsidiary privacy policies and procedures that are unique to the needs of the business unit.

Policy

Each business unit will establish subsidiary privacy policies and procedures that are unique to the needs of the business unit, reflecting the unit’s business procedures and interactions with individual [clients](#) and incorporating, as necessary, federal or state laws and regulations specifically applicable to the business unit.

FSSA business units may establish privacy policies and procedures that are more restrictive than these Privacy Compliance Policies; and, in certain cases, may be obligated to do so under federal or state laws and regulations specifically applicable to the business unit.

However, in no case may a business unit establish privacy policies and procedures that are less restrictive, contrary to, or otherwise circumvent these agency-level Privacy Compliance Policies and Procedures without the express, written permission of the FSSA Privacy Officer. Exceptions may be granted, but only where a solid business and legal case can be made for the exception.

Procedures

The following provides additional guidance for this policy.

1. Certain business units that are subsidiaries of a parent business unit (e.g., First Steps is a subsidiary of the Division of Disability & Rehabilitative Services) may adopt the parent business unit’s privacy policies and procedures and not develop its own, provided the subsidiary does not have any privacy requirements that are unique to its business function. The parent business unit management team and the Privacy Officer must approve these exceptions.
2. Business unit privacy policies and procedures are to be submitted to the Privacy Officer for review and approval.
 - 2.1. The Privacy Officer’s approval is limited to ensuring the privacy policies and procedures are not less restrictive, contrary to, or otherwise circumvent these Privacy Compliance Policies and Procedures; are not contrary to applicable federal and state laws and regulations; and, meet generally accepted privacy best practices.
 - 2.2. The Privacy Officer may make specific recommendations regarding business unit privacy policy and procedure content.

Section 3: Business Unit Privacy Policies & Procedures

FSSA Privacy Compliance Policies & Procedures

- 2.3. The Privacy Officer will maintain a central log of all business unit specific privacy policies and procedures.
3. Business unit privacy policies and procedures should be a supplement to these Privacy Compliance Policies and Procedures. For example, a business unit may insert supplemental privacy policies and procedures (by way of links) into these Privacy Compliance Policies and Procedures; or, provide a reverse cross-reference to these Privacy Compliance Policies and Procedures within the business unit's privacy policies and procedures.
4. Business units should also consider integrating their privacy policies and procedures with other, relevant policies and procedures in order to provide a consolidated and uniform set of policies and procedures for their staff and business operations.

Section 4: Privacy/Security Liaisons

Purpose

The purpose of this policy is to ensure each FSSA division, state operated facility, and business unit, as appropriate, has a designated staff member assigned to serve as the Privacy/Security Liaison for that division, state operated facility, or business unit.

The scale and scope of FSSA requires Privacy and Security coordination between the FSSA Privacy Officer and the FSSA business units on a number of fronts, including, but not limited to, management of privacy/security incidents, business unit specific privacy and security policy and procedure development, and providing a knowledgeable resource to assist staff with privacy/security related questions and issues.

Policy

Each FSSA division will assign an appropriately qualified staff member to serve as the division's Privacy/Security Liaison. Each state operated facility (hospital) will assign an appropriately qualified staff member to serve as the facility's Privacy/Security Liaison.

At a minimum, each division and state operated facility will have a designated Privacy/Security Liaison. As determined by each division in collaboration with the FSSA Privacy Officer, additional Privacy/Security Liaisons may be designated for the various bureaus, sections, program areas, and offices within the division. The Privacy/Security Liaisons will be responsible to:

1. Ensure all staff members within their assigned area are familiar with and understand FSSA's Privacy Compliance policies and procedures.
2. Ensure all staff members within their assigned area complete any and all required privacy and security training as promulgated by the FSSA Privacy Officer, including both initial and refresher training.
3. Develop and document privacy and security policies and procedures as applicable to their assigned area (as business unit-specific policies and procedures that are a subsidiary of FSSA's Privacy Compliance Policies and Procedures, as described in Section 3), as directed by and in collaboration with division management.
4. Collaborate as necessary with the FSSA Privacy Officer regarding the development of business unit-specific privacy and security policies and procedures.
5. Ensure all staff members within their assigned area are familiar with and understand any business unit-specific privacy policies and procedures, and are trained on same.
6. Coordinate with the FSSA Privacy Officer on privacy/security incidents as further described elsewhere in these Privacy Compliance Policies (following the associated policies and procedures).
7. Report on their activities to the FSSA Privacy Officer on a regular basis (as deemed necessary and appropriate by the FSSA Privacy Officer).

Procedures

Each Privacy/Security Liaison will develop procedures pertinent to their assigned area designed to assure compliance with this policy.

Section 5: Incident Management & Breach Reporting Policy

Purpose

The purpose of this policy and its supporting procedures is to ensure the timely reporting of known or suspected [security and privacy incidents](#) so that appropriate action can be taken in a timely manner to prevent or mitigate any improper disclosures of [client personal information](#).

This policy is organized into several sections with each focusing on a particular policy regarding Incident Management & Breach Reporting:

1. [Section 5.1](#): Central Response and Reporting Management
2. [Section 5.2](#): Privacy/Security Incident Staff Notification Requirements
3. [Section 5.3](#): Privacy/Security Incident Investigation
4. [Section 5.4](#): Privacy/Security Incident Determination
5. [Section 5.5](#): Breach Notification
6. [Section 5.6](#): Mitigation & Corrective Actions
7. [Section 5.7](#): Notice to HHS

Overall, it is the agency's policy for all privacy/security incidents to be reported to the FSSA Privacy Officer, who will centrally manage FSSA's response to ensure response consistency, legal and regulatory compliance, and cost management. The FSSA Privacy Officer, working appropriately with FSSA management, the affected business unit's management and Privacy/Security Liaison, and others as applicable, will investigate the incident, determine whether a [breach](#) has occurred, ensure appropriate mitigation and corrective action procedures are or will be undertaken, and provide or cause to provide appropriate notice when required.

Section 5.1: Central Response and Reporting Management

Purpose

A timely and expert response to known or suspected [privacy/security incidents](#) is vital to managing and mitigating the impact of the incident, with the objective of taking immediate action to stop the incident if it is ongoing; and, to complete an appropriate and structured investigation into the cause and effect of the incident, including ascertaining the potential harm to the individuals (victims) subject to the incident and risk to the agency.

In addition, given the potentially significant costs involved in mitigation activities and providing notice to the victims (as may be required under federal and/or state law), the reporting requirements to both the Office of the Indiana Attorney General and the Department of Health and Human Services, and the potential harm that may be caused by a substantive incident, it is appropriate to centralize management of the incident investigation and mitigation process (including notice). This helps assure a uniform approach, appropriate involvement by all applicable state agencies and departments in the process, and a streamlined notification and reporting process.

Policy

The FSSA Privacy Officer will centrally manage all reported privacy/security incidents, both known and suspected. The Privacy Officer will involve FSSA management, other FSSA divisions, state agencies, and law enforcement as appropriate and needed under the circumstances.

The FSSA Privacy Officer is responsible for oversight, direction, and control of the incident investigation and may delegate, as appropriate under the circumstances, investigation and mitigation activities to other FSSA personnel, including contractors. Such personnel will cooperate with the FSSA Privacy Officer and undertake those assigned activities in a timely and competent manner.

As designated by the FSSA Privacy Officer, Privacy Office staff may oversee, direct, and control privacy/security incident response procedures of behalf of the FSSA Privacy Officer.

Procedures

The FSSA Privacy Office has internal procedures in place to guide its response to reported privacy/security incidents, including incident risk determination and management procedures, documentation procedures, notice development and dissemination procedures, and communication procedures.

These procedures will include reporting of incidents involving Federal Tax Information used by the agency to the Internal Revenue Service and/or the Social Security Administration.

Section 5.2: Privacy/Security Incident Staff Notification Requirements

Purpose

The purpose of this policy and its supporting procedures is to ensure the timely notification of the appropriate [Privacy/Security Liaison](#) by FSSA personnel of a known or suspected [privacy/security incident](#).

Policy

FSSA personnel will promptly notify their assigned Privacy/Security Liaison (PSL) should they learn of or reasonably suspect that a privacy/security incident has occurred. This should notice occur on the same business day that FSSA personnel become aware of the incident. This includes known or suspected privacy/security incidents reported to a staff member by clients and/or FSSA contractors (e.g., Xerox, HP, IPMG, an AAA, Phoenix, RCR, Anthem/Wellpoint, MDwise, etc.).

Alert: If you suspect that your computer has been infected with a virus or other type of malware, or if you've accidentally opened a spam message, immediately contact the IOT Help Desk to report the issue, and then contact your PSL. A virus, if not removed, can cause extensive damage to state systems.

Advisory: FSSA personnel reporting known and suspected privacy/security incidents are protected from any recrimination or retaliatory acts under the state's and FSSA's whistleblower and retaliatory protection policies.

Failure to report a known or suspected privacy/security incident **is a violation of this policy** and may result in personnel sanctions in accordance with state and FSSA policy.

Procedures

1. FSSA personnel are to be on the alert for any known or suspected privacy/security incidents.

Advisory: FSSA prefers that its personnel err on the side of caution and report any suspected privacy/security incident—if you are unsure, contact your assigned PSL or supervisor for guidance. It is better to report an incident that, in the end, is not a privacy/security incident than to risk a real incident going unreported. And, no one will be reprimanded for doing so.

2. FSSA personnel are directed to promptly notify their assigned Privacy/Security Liaison of a known or suspected privacy/security incident.
 - 2.1. Such notice should be in person, by phone, or by e-mail.

Alert: If a Business Associate/Contractor contacts you and reports a privacy/security incident or breach, promptly contact the FSSA Privacy Officer.

Section 5: Incident Management & Breach Reporting Policy

FSSA Privacy Compliance Policies & Procedures

3. If the assigned PSL is not available, the staff person should then immediately notify both their supervisor² and the FSSA Privacy Officer.
 - 3.1. Such notice should be in person, by phone, or by e-mail.
4. The staff person discovering the privacy/security incident should try to capture as much information about the incident as possible—write it down; however, don't delay notice just to capture this information:
 - 4.1. Date and time of when you discovered the incident.
 - 4.2. When the incident occurred (date and time), if known.
 - 4.3. How you discovered the incident.
 - 4.4. The nature of the incident:
 - 4.4.1. *What information* was disclosed or compromised (e.g., name, address, RID#, Case#, SSN, date of birth, medical record, etc.)?
 - 4.4.1.1. Obtain a copy of the information disclosed, if possible;
 - 4.4.2. *To whom* the information was disclosed?
 - 4.4.3. *The volume* of information disclosed (e.g., how many people, how many records, etc.);
 - 4.4.3.1. The names and addresses of the people affected (victims)—may require some investigation or provision of a file if a large number were affected;
 - 4.4.3.2. Which FSSA programs are the victim(s) enrolled in or applying for (e.g., Medicaid, a Waiver program, SNAP, TANF, etc.)?
 - 4.4.4. *How* the incident occurred.
 - 4.4.5. Whether **Social Security Numbers** were disclosed or compromised.
 - 4.4.6. *What actions* were taken to mitigate the incident (if any)?
 - 4.4.7. And, any other information that seems pertinent.
 - 4.5. To whom you reported the incident, include date, time, and method (e.g., in person, by phone).
 - 4.6. Your name and contact information.
5. The FSSA Privacy Officer may contact the staff person for additional information, as needed.
6. If, for whatever reason, the staff person making the notification to the PSL believes that the PSL is not being responsive or timely, the staff person should contact the FSSA Privacy Officer and report the privacy/security incident.

² If the supervisor is the one suspected of causing the privacy/security incident and the staff person is uncomfortable reporting the incident to this same supervisor, the staff person should directly notify the FSSA Privacy Officer.

Section 5: Incident Management & Breach Reporting Policy

FSSA Privacy Compliance Policies & Procedures

Advisory: Disclosures that occur incidental to the use or disclosure of client personal information otherwise permitted by these Privacy Compliance Policies, *et seq*, may not constitute a privacy/security incident, provided such use or disclosure is a by-product of a permissible use or disclosure, cannot be reasonably prevented, and is limited in nature. For example, an Eligibility Specialist's computer screen locks up while displaying client information; the IT person who fixes the problem likely will see the information; this is an incidental disclosure and not a violation or breach. Such incidental disclosures do not need to be reported as privacy/security incidents; when in doubt, seek guidance from your Privacy/Security Liaison or the FSSA Privacy Officer.

Section 5.3: Privacy/Security Incident Investigation

Purpose

The purpose of this policy and its supporting procedures is to establish the requirements and general approach for the investigation of known and suspected privacy/security incidents as reported by FSSA personnel or as otherwise becomes known to FSSA.

Policy

The applicable FSSA Privacy/Security Liaison and the FSSA Privacy Officer are responsible to promptly investigate any known or suspected [privacy/security incidents](#).

Alert: If the incident involves the [improper disclosure](#) of (or possible disclosure of) an individual's Social Security Number, the incident must be reported to the Office of the Indiana Attorney General within two (2) business days of when the Social Security Number was disclosed³. The FSSA Privacy Officer will provide any notifications to the [OAG](#).

Procedures

1. The Privacy/Security Liaison⁴ **will begin a preliminary investigation** of a reported privacy/security incident on the same business day the incident was reported to the PSL by FSSA personnel or the same business day the PSL otherwise learned of a known or suspected privacy/security incident. The investigation should focus on collecting the facts and circumstances regarding the incident:
 - 1.1. Date and time of the privacy/security incident was discovered.
 - 1.2. *Who* (FSSA staff) reported the incident (name, title, contact information)?
 - 1.3. *How* was the incident discovered?
 - 1.4. The nature of the incident:
 - 1.4.1. *What information* was improperly disclosed or compromised (e.g., name, address, RID#, Case#, SSN, date of birth, medical record, etc.)?
 - 1.4.2. *To whom* the information was disclosed?
 - 6.1.1.1. *The volume* of information disclosed (e.g., how many people, how many records, etc.); The names and addresses of the people affected (victims)—may require some investigation or provision of a file if a large number were affected;
 - 6.1.1.2. Which FSSA programs are the victim(s) enrolled in or applying for (e.g., Medicaid, a Waiver program, SNAP, TANF, etc.)?
 - 1.4.3. *How* the incident occurred including the names, titles, and contact information of persons involved in the incident?

³ Reference IC 4-1-10 and IAC 5-1-1.

⁴ If a PSL is not available, the PSL responsibilities outlined here become the responsibility of the supervisor or manager of the person who reported the privacy/security incident.

Section 5: Incident Management & Breach Reporting Policy

FSSA Privacy Compliance Policies & Procedures

1.4.4. *Whether Social Security Numbers* were improperly disclosed or compromised;

Alert: If a Social Security Number(s) was disclosed or suspected to have been disclosed or otherwise compromised, the PSL is to notify the FSSA Privacy Officer on the same business day so that the FSSA Privacy Officer can provide a timely, even if preliminary, notice to the OAG.

1.4.5. *Whether Federal Tax Information* was improperly disclosed or compromised;

Alert: Federal Tax Information (FTI) is provided to the agency by both the Internal Revenue Service and the Social Security Administration. If FTI was disclosed or suspected to have been disclosed or otherwise compromised, the PSL is to **immediately** notify the FSSA Privacy Officer. In these situations, the agency is required to immediately report the incident to the IRS and/or SSA (the report will be made by the FSSA Privacy Officer).

1.4.6. *What actions* have been taken to mitigate the incident (if any)?

1.4.7. And, any other information that seems pertinent.

Advisory: Not all privacy/security incidents may involve the improper disclosure of client personal information, but rather may place the integrity of client personal information at risk. For example, a staff member changed a client's personal information on a computer system without authorization or with malicious intent. Therefore, collect as much information pertinent to the type of incident or suspected incident as possible.

2. If the privacy/security incident is ongoing (e.g., unencrypted e-mails containing client personal information continue to be exchanged), to the extent possible, the PSL should take immediate steps to stop or at least temporarily halt the ongoing incident.
3. **The PSL will notify the FSSA Privacy Officer** of the privacy/security incident and the results of their preliminary investigation within one (1) business day from the point in time in which the PSL became aware of the privacy/security incident and began their preliminary investigation.
 - 3.1. The initial notice to the FSSA Privacy Officer may be in person, by phone, or by e-mail.
 - 3.2. The FSSA Privacy Officer may direct the PSL to undertake certain actions regarding the incident, including, but not limited to, additional data collection, incident mitigation activities, preparation of a draft Incident Report, and other actions deemed reasonable at the time by the FSSA Privacy Officer.

Alert: Any privacy/security incident that appears to place any of the victims of the incident or the agency at **imminent risk of harm**, the PSL should **immediately** notify the FSSA Privacy Officer.

4. If an individual's **Social Security Number** has or is suspected of having been improperly disclosed, the FSSA Privacy Officer will provide preliminary notification to the Office of the Indiana Attorney General.

Section 5: Incident Management & Breach Reporting Policy

FSSA Privacy Compliance Policies & Procedures

- 4.1. The preliminary notification must be provided within two (2) business days of when the improper disclosure occurred or is suspected of having occurred.
 - 4.2. The preliminary notification should be by e-mail to the designated OAG contact and include as many details as are available at the time. A copy of the e-mail should be placed in the Incident File.
 5. If **Federal Tax Information** has or is suspected of having been improperly disclosed or otherwise compromised, the FSSA Privacy Officer will provide notification to the Internal Revenue Service and/or the Social Security Administration in accordance with the Privacy Office's procedures.
 6. The FSSA Privacy Officer, or his/her delegate, will open an [Incident File](#) regarding the privacy/security incident.
 - 6.1. The **Incident File** may include, but is not limited to:
 - 6.1.1. An [Incident Report](#) prepared by the FSSA Privacy Officer;
 - 6.1.2. Supporting materials regarding the incident, including but not limited to:
 - 6.1.2.1. Copies of relevant e-mails regarding the incident
 - 6.1.2.2. Copies of the client's personal information subject to the incident
 - 6.1.2.3. Copies of any disclosure notices prepared due to the incident
 - 6.1.2.4. Copies of relevant documents and files.
 - 6.1.3. Any other information deemed appropriate by the FSSA Privacy Officer.
 - 6.2. **Incident Log:** The FSSA Privacy Officer will maintain a log of all reported privacy/security incidents. The purpose of the log is to provide an easily referenced document of all open and closed privacy/security incidents, including status, notice provision, and reporting to HHS/OCR and/or the OAG as appropriate. This excludes Minor Incidents.
 - 6.3. **Minor Incidents:** Certain privacy/security incidents may be deemed minor by the FSSA Privacy Officer:
 - 6.3.1. Minor incidents may be suspected privacy/security incidents that, upon investigation, are a false-positive and no real incident occurred or a similar circumstance.
 - 6.3.2. Such incidents will be recorded as minor incidents in the secure SharePoint site under Minor Incidents; an incident number is not assigned and a separate log is not maintained.
- Advisory:** Periodically, guidance is sought from the FSSA Privacy Officer by a PSL or other staff member regarding whether a certain action or activity is a privacy/security incident; in those cases where it is clearly not a privacy/security incident no documentation is required.
7. The **FSSA Privacy Officer will promptly investigate the incident** to confirm and document the scope of the privacy/security incident and the associated risk to FSSA and the clients affected.

Section 5: Incident Management & Breach Reporting Policy

FSSA Privacy Compliance Policies & Procedures

- 7.1. The FSSA Privacy Officer will collect, or direct to be collected, any additional and supplemental information deemed necessary to determine the scope of the incident and to identify next step actions. FSSA personnel will fully cooperate with the FSSA Privacy Officer, or his/her staff, in the investigation.
- 7.2. The FSSA Privacy Officer will document the results of the investigation in the Incident Report; any supporting evidence will be captured in the Incident File.
8. The FSSA Privacy Officer will establish additional Privacy Office procedures, to the extent appropriate and necessary, for privacy/security incident investigation and Incident File documentation procedures, including forms and templates.

Section 5.4: Privacy/Security Incident Determination

Purpose

The purpose of this policy and its supporting procedures is to define the steps to be taken to determine the scope of any reported privacy/security incident and to identify the next action steps.

Policy

The FSSA Privacy Officer will, based on the results of the investigation of any reported privacy/security incident, determine the scope of the incident and the risk, if any, to the clients involved and to the agency. The FSSA Privacy Officer will collaborate with appropriate FSSA management, the FSSA Office of General Counsel (including Internal Investigations), the Office of the Indiana Attorney General, and others to the extent prudent and necessary in making this determination.

Based on the FSSA Privacy Officer's determination of scope and risk, the FSSA Privacy Officer will identify the next steps necessary to mitigate the risk, determine whether a [breach](#) of confidentiality has occurred, provide appropriate notice, and recommend corrective actions.

If client personal information has been improperly disclosed⁵ resulting in a breach (i.e., in violation of these Privacy Compliance Policies, business unit policies, state security policies, and/or applicable federal and state laws and regulations), it is FSSA's policy that:

- Written notice will be provided to the victims of the improper disclosure except in cases where (and subject to the FSSA Privacy Officer's discretion):
 - Only the victim's name has been disclosed and there is no identifiable association of the victim with any state benefit programs;
 - Only the victim's name, address, and/or case number have been disclosed, there is no identifiable association of the victim with any state benefit programs, and the FSSA Privacy Officer determines that under the circumstances the risk of substantive financial, reputational, or other harm to the individual is low;
 - Client personal information was unintentionally accessed by a FSSA staff member, who made the access in good faith and is otherwise authorized to access certain client information (e.g., the staff member is authorized to only access client personal information on clients assigned to them, but unintentionally accessed client personal information on a client not assigned to them);
 - Client personal information was inadvertently disclosed by a FSSA staff member (who has authorized access to the information) to another FSSA staff member who has authorized access to client personal information, but not the client personal information inadvertently disclosed to the staff person, provided the client personal

⁵ Note: The unintentional or inadvertent disclosure on client personal information that has been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of encryption technology approved by FSSA is not an improper disclosure or breach unless the password, allowing the information to be decrypted, is known to be compromised or insufficient—reference Section 7.

Section 5: Incident Management & Breach Reporting Policy

FSSA Privacy Compliance Policies & Procedures

information is not used or further disclosed by the recipient (e.g., a supervisor inadvertently e-mails a client's case information to a staff member who is not assigned to that case);

- The FSSA Privacy Officer has good faith belief that the unauthorized recipient of the client personal information would not reasonably be able to retain or use the information—this exception does not apply to privacy/security incidents in which an individual's Social Security Number has been disclosed.

If the FSSA Privacy Officer has determined that a [breach](#) has occurred, the FSSA Privacy Officer will prepare or cause to be prepared appropriate written notice to the victims of the breach as provided in Section 5.5, Breach Notification, and complete the Incident Report accordingly.

If the FSSA Privacy Officer has determined that a breach has not occurred, the FSSA Privacy Officer will determine whether any additional training or other actions are necessary to limit similar privacy/security incidents that did not result in a breach and recommend same to the appropriate agency, division/business unit, and/or Division of Technology management.

Procedures

1. ***Breach determination:*** if a privacy/security incident that has resulted in the improper disclosure of client personal information in violation of these Privacy Compliance Policies, business unit policies, state security policies, and/or applicable state and federal laws and regulations, then a breach of confidentiality has occurred subject to the exclusions identified in the above policy:
 - 1.1. If one of the above exclusions applies, the FSSA Privacy Officer may still classify the incident as a breach based on the facts and circumstances of the incident (e.g., while the improper disclosure was limited, the nature of the cause of the disclosure was egregious or malicious).
 - 1.2. If none of the above exclusions apply, then the FSSA Privacy Officer will provide (or cause to be provided) written notice to the victim(s) of the breach—reference Section 5.5 for breach notification procedures.
2. ***Discovery Date:*** The date by when notice must be provided (reference Section 5.5) for a breach is based on when the breach is first discovered by FSSA. Part of the investigation includes determining when the breach was first known to FSSA.
 - 2.1. Under the HIPAA Breach Rule, *Breaches Treated as Discovered* means that the first day on which a breach is known to FSSA or, by exercising reasonable diligence, would have been known to FSSA, is the date upon which the breach is “discovered.”
 - 2.2. This same approach to determining the Discovery Date will be used for all improper disclosures of client personal information (e.g., improper disclosure of a Social Security Number).
3. Whether or not a breach occurred, if the FSSA Privacy Officer has any reason to believe the cause of the privacy/security incident was intentional or malicious or undertaken for personal gain, the FSSA Privacy Officer may involve, as appropriate:
 - 3.1. FSSA Office of the Secretary (Designee)

Section 5: Incident Management & Breach Reporting Policy

FSSA Privacy Compliance Policies & Procedures

- 3.2. FSSA Office of Communications
 - 3.3. FSSA Human Resources
 - 3.4. FSSA Office of General Counsel
 - 3.5. Office of the Indiana Attorney General
 - 3.6. FSSA Internal Investigations
 - 3.7. Law enforcement
 - 3.8. Division/business unit management
 - 3.9. Others as deemed appropriate.
4. Whether or not a breach occurred, if the source of the privacy/security incident was or appears to be technology-based (e.g., malware attack, user authentication control compromise, keylogger presence, etc.), the FSSA Privacy Officer will involve, as appropriate, the Division of Technology Services and the state Chief Information Security Officer in the investigation and determination of mitigating and corrective actions.
 5. Whether or not a breach occurred, if the basis of the privacy/security incident is a lost or stolen portable device (e.g., laptop, USB drive):
 - 5.1. For lost or stolen laptops (including tablets and similar devices):
 - 5.1.1. Ensure that the state Chief Information Security Officer (or his/her designee) is informed of the situation;
 - 5.1.2. For stolen laptops, obtain a copy of the police report from the affected staff member for the Incident File;
 - 5.1.3. For state issued laptops, confirm with the state Chief Information Security Officer (or his/her designee) that the laptop was encrypted;
 - 5.1.4. Confirm with the affected staff member: (a) whether any client personal information was on the laptop; (b) that the laptop was encrypted; and, (c) that the person used a complex password for the laptop encryption software (if applicable) and that the person's password was not lost or stolen with the device and remains secure;
 - 5.1.5. If the laptop contained client personal information and was not encrypted (or the password has been compromised), the affected staff member will need to be able to replicate the client personal information on the laptop—necessary to determine whether a breach has occurred and the number of potential victims.
 - 5.1.6. For state issued laptops, coordinate with the state Chief Information Security Officer (or his/her designee) regarding device remote disposition.
 - 5.2. For lost or stolen USB drives and other portable media including smart phones and tablets:
 - 5.2.1. Confirm with the affected staff member: (a) whether the media was encrypted; (b) whether the media contained client personal information; (c) if the media was encrypted

Section 5: Incident Management & Breach Reporting Policy

FSSA Privacy Compliance Policies & Procedures

that a complex password was in use and the password was not lost or stolen with the device; and, (d) if the media contained client personal information and was not encrypted or the password compromised, how the client personal information contained on the media can be replicated—necessary to determine whether a breach has occurred and the number of potential victims.

5.2.2. For state issued smart phones and tablets, coordinate with the state Chief Information Security Officer (or his/her designee) regarding remote wiping and disabling of the device.

5.2.3. For personally-owned smart phones and tablets, coordinate with the staff member/owner regarding remote wiping and disabling of the device (e.g., through the person's telecommunications carrier, personal remote access accounts like MobileMe, etc.).

6. The FSSA Privacy Officer will update the Incident Report with his/her findings and conclusions.
7. The FSSA Privacy Officer will apprise the associated PSL (and/or the appropriate business unit management staff) of the findings, conclusions, and next steps.

Reference [Section 7](#) regarding Laptop and Portable Device security requirements.

Section 5.5: Breach Notification

Purpose

The purpose of this policy and its supporting procedures is to define the steps to be taken to provide appropriate notice to the clients who are victims of a confirmed [breach](#); and, to provide appropriate notice as required under state and federal rules to the [OAG](#) and [HHS](#).

Policy

The FSSA Privacy Officer is responsible for completing the notification procedures defined here in the event of a confirmed breach of a client's personal information in FSSA's safekeeping.

In the event that the breach is caused by a [Business Associate](#) of FSSA, the FSSA Privacy Officer may direct the Business Associate to prepare and provide the notices in the Business Associate's name and to absorb all costs regarding the provision of notice and any actions necessary to mitigate the deleterious affect of the breach (e.g., to pay for credit monitoring services, implement security enhancements, etc.).

Alert: The HIPAA Breach Rule requires that notice to the victim(s) of a breach must occur without unreasonable delay, but no later than 60 days after the breach was discovered ([Discovery Date](#)). IC 4-1-11 regarding the Breach of the Security of the System, in which client personal information is improperly disclosed, requires notice to be made without unreasonable delay. FSSA has been directed by the OAG to employ a thirty (30) day time limit for any notices to be provided under IC 4-1-11. IC 4-1-10 regarding the release of a Social Security Number requires notice as set forth in IC 4-1-11; however, under IAC 5-1-1 the OAG must be notified of the breach within two (2) business days of the improper release ([Discovery Date](#)) of a SSN or other personal identifying information.

Procedures

1. The FSSA Privacy Officer will review the facts and circumstances of the breach regarding whether notice should be provided to the victim(s) of the breach and/or to others.
2. **OAG/Law Enforcement Coordination:** if the FSSA Privacy Officer has any reason to believe the cause of the breach was intentional or malicious or undertaken for personal gain, the FSSA Privacy Officer will involve the OAG and/or law enforcement personnel (including OGC Internal Investigations), as appropriate:
 - 2.1. The OAG or law enforcement may determine that a delay in providing notice to the victim is necessary to avoid any compromise of the investigation. If a delay is necessary:
 - 2.1.1. The OAG/law enforcement must provide the FSSA Privacy Officer with a written directive requesting the delay (including the reason for the delay) and the time period of the delay.
 - 2.1.2. The FSSA Privacy Officer will document the directive in the Incident Report and delay the provision of notice for the time period specified in the directive.
 - 2.1.3. The FSSA Privacy Officer can delay the provision of notice based on a verbal request from the OAG/law enforcement (documenting same in the Incident Report), but the delay cannot exceed thirty (30) calendar days from the date of the verbal request.

Section 5: Incident Management & Breach Reporting Policy

FSSA Privacy Compliance Policies & Procedures

3. **Improper disclosure of a Social Security Number:** If a client's Social Security Number is disclosed in violation of IC 4-1-10, the FSSA Privacy Officer will provide notice of the incident to the OAG within two (2) business days from the Discovery Date in accordance with 10 IAC 5-1-1.
 - 3.1. This notice to the OAG may be preliminary pending confirmation that an actual disclosure of a SSN occurred (i.e., an improper disclosure of a SSN is suspected, but unconfirmed; providing preliminary notice within the two (2) business day timeframe satisfies 10 IAC 5-1-1, even if the OAG notice is retracted later should it be determined that a SSN was not improperly disclosed).
 - 3.2. This notice may be by e-mail and should indicate that an investigation is underway and steps have been taken, as appropriate, to stop any continuation of the improper disclosure.
 - 3.3. If it is confirmed that a SSN was improperly disclosed, once the investigation is complete and notice provided to the victim, a copy of the notice and the Incident Report is to be sent to the OAG for their files.

Note: it has been past practice for the OAG to subsequently send a letter to the FSSA Privacy Officer indicating whether or not FSSA fulfilled the requirements of the law regarding SSN improper disclosures; the letter should be filed in the Incident File.

4. **Notice to Individuals:**

- 4.1. Timing of Notice: Written notice to the victim(s) of a breach will be provided without unreasonable delay and in no case not later than thirty (30) calendar days after the Discovery Date if a social security number was disclosed (unless otherwise delayed by the OAG/law enforcement). If a social security number was not disclosed, written notice will be sent without unreasonable delay, but in no case not later than sixty (60) days from the Discovery Date.

- 4.2. Content of Notice and Distribution:

- 4.2.1. The written notice to the victims will be written in plain language and include the elements required under the HIPAA Breach Rule (including notices for breaches that do not involve PHI or are otherwise not a violation of the HIPAA Privacy Rule):

- 4.2.1.1. A Disclosure Notice template—prepared and maintained by the Privacy FSSA Officer—provides the appropriate format and content requirements, with options based on the type of information disclosed (e.g., credit bureau contact information in the event of a financial or SSN disclosure).

- 4.2.2. The written notice will be sent to the victim(s) by first class mail, USPS, at their last known address; in certain cases, as determined by the FSSA Privacy Officer based on the facts and circumstances of the situation, written notice will be provided to the victim's authorized representative/personal representative/parent/legal guardian in addition to or in lieu of the victim.

- 4.2.3. At this juncture, delivery of written notice by e-mail is not approved.

- 4.2.4. IC 4-1-11-9 Alternate Form of Notification: If the breach is clearly not the result of a violation of the HIPAA Privacy Rule and the conditions of IC 4-1-11-9 are met, the FSSA

Section 5: Incident Management & Breach Reporting Policy

FSSA Privacy Compliance Policies & Procedures

Privacy Officer, in collaboration with the FSSA Office of General Counsel and the FSSA Director of Communications, may use the alternative form of notification as provided for in IC 4-1-11-9.

- 4.3. **Urgent Situations:** In situations that the FSSA Privacy Officer deems urgent due to the nature of the breach (e.g., possible imminent misuse of client personal information resulting in identity theft), FSSA may provide information to the victims by phone or other means as determined by the FSSA Privacy Officer. Provision of written notice is still required.
- 4.4. **Notice to Media:** If the breach is a violation of the HIPAA Privacy Rule (as determined by the FSSA Privacy Officer) and involves more than 500 victims (individuals), notice to the media is required in accordance with the HIPAA Breach Rule:
 - 4.4.1. Providing notice to the media will be done in accordance with the HIPAA Breach Rule with respect to timing (same time period as providing notice to the individual victims), content, and distribution (e.g., to prominent media).
 - 4.4.2. The FSSA Privacy Officer will collaborate with the FSSA Communications Director in drafting the media notice and its distribution.
 - 4.4.3. **Website Posting:**
 - 4.4.3.1. In addition to media notice, notice will be conspicuously posted on FSSA's website home page regarding the breach and include appropriate contact information.
 - 4.4.3.2. A toll free number and e-mail address will be provided for individuals to contact FSSA about the breach.
 - 4.4.3.3. The posting will remain on the website for no less than ninety (90) calendar days.
 - 4.4.3.4. To the extent deemed appropriate by the FSSA Communications Director, a summary notice also may be posted on the state's website home page with a link to the FSSA webpage.

Inquiry Response: The FSSA Privacy Officer will collaborate with the FSSA Communications Director regarding FSSA's response content and procedures for responding to individual and media inquiries.

Alert: FSSA has the burden of proof under federal regulations to demonstrate that either a breach, in fact, did not occur; or, that all appropriate actions and notices were undertaken in a timely manner. All of the actions taken, including copies of notices, should be documented in the Incident Report and Incident File as a means to provide this proof.

Section 5.6: Mitigation & Corrective Actions

Purpose

This policy has three purposes:

1. To establish the requirement that FSSA undertake all reasonable actions to mitigate the deleterious (harmful) effects of any [breach](#) experienced by the agency.
2. To identify appropriate and reasonable corrective actions to be undertaken to minimize the risk of subsequent, similar breaches.
3. For privacy/security incidents that did not result in a breach, to identify appropriate and reasonable corrective actions to reduce associated risk that a similar privacy/security incident does not subsequently result in a breach or other improper use of client personal information.

Policy

1. The FSSA Privacy Officer will direct reasonable actions to be undertaken by the affected business units and/or [Business Associates](#) to mitigate the deleterious effects of any breach, including any actions necessary to stop an ongoing breach. FSSA division management will be responsible to undertake these actions in a timely manner.
2. If a Business Associate is involved with the breach—whether the source of the breach, a contributor, or in a position to effectively assist with mitigation activities—the responsible business unit will work with and, to the extent appropriate, oversee the mitigation activities of the Business Associate.
3. FSSA division management is responsible to assess and implement corrective actions reasonably identified by the FSSA Privacy Officer and/or division personnel to minimize the risk of subsequent, similar breaches.
 - 3.1. Division management’s assessment may include the identification of alternative, but equally effective corrective actions (in lieu of the corrective actions identified by the FSSA Privacy Officer).
 - 3.2. The assessment is to be completed within a reasonable period of time, based on the scope and complexity of the identified corrective action; division management will provide the FSSA Privacy Officer a timeline in which the assessment and their determination will be completed.
 - 3.3. If, based on their assessment, division management determines that the cost or complexity of the corrective action is greater than the associated risk—that is, division management is willing to assume the risk of a subsequent, similar breach and not invest in the corrective action—they must document that determination and risk acceptance in a formal memo to the FSSA Privacy Officer for inclusion in the Incident File.
4. For privacy/security incidents that did not result in a breach, the FSSA Privacy Officer may identify corrective actions to prevent similar privacy/security incidents from occurring (that may result in a breach or other improper use of client personal information).

Section 5: Incident Management & Breach Reporting Policy

FSSA Privacy Compliance Policies & Procedures

- 4.1. This may include other issues and risks identified during the course of a privacy/security incident investigation that need to be addressed to avoid a subsequent privacy/security incident.
- 4.2. FSSA division management is responsible to assess and implement these corrective actions.
- 4.3. The assessment is to be completed within a reasonable period of time, based on the scope and complexity of the identified corrective action; division management will provide the FSSA Privacy Officer a timeline in which the assessment and their determination will be completed.
- 4.4. If, based on their assessment, division management determines that the cost or complexity of the corrective action is greater than the associated risk—that is, division management is willing to assume the risk of a subsequent, similar privacy/security incident and not invest in the corrective action—they must document that determination and risk acceptance in a formal memo to the FSSA Privacy Officer for inclusion in the Incident File.

Advisory: Corrective actions are dependent on the situation and the facts and circumstances of the incident and may range from staff member counseling to developing system modifications to significantly changing business processes. For large-scale and/or complex corrective actions, the FSSA Privacy Officer will collaborate with division management with identifying reasonable corrective actions.

Simple corrective actions (e.g., counseling or retraining a staff member) may be completed and documented for inclusion in the Incident Report by business unit management without a formal assessment as described above.

Procedures

Appropriate mitigation and corrective action procedures are dependent on the situation and the facts and circumstances of the breach or privacy/security incident, and will need to be determined on a case-by-case basis. The following are intended to provide guidance, unless otherwise stated. The FSSA Privacy Officer will document the mitigation and recommended corrective action procedures in the Incident Report.

1. **Stop On-going Breach:** If a breach of client personal information is ongoing—for example, provider manual containing client personal information in example screen shots is posted on a public website—the first action item is to take all reasonable actions to stop the breach; in this example, remove the manual from the website or shut down the website.
2. **Return Request:** Client personal information improperly disclosed by tangible means should be retrieved from the recipient as soon as possible:
 - 2.1. Tangible means is a physical document (e.g., notice, letter, appeal hearing packet), an electronic file (e.g., spreadsheet, e-mail), a device (e.g., USB drive), or similar.
 - 2.2. Upon learning that client personal information was improperly disclosed by tangible means, staff personnel should immediately contact the recipient and ask for its return—record the date contact was made and the name and contact information of the recipient.

Section 5: Incident Management & Breach Reporting Policy

FSSA Privacy Compliance Policies & Procedures

- 2.2.1.If necessary, a self-addressed stamped envelope may be sent to the recipient to return physical documents or devices. The FSSA Privacy Officer can assist; see 2.3 below.
- 2.2.2.If the tangible means was an electronic file sent by e-mail or other electronic means, ask the recipient to completely delete the file (from their inbox, deleted items, folders, and recycle bin), and to send you a confirmation e-mail that they did so.
- 2.2.3.If the tangible means was client personal information contained in an e-mail, ask the recipient to completely delete the e-mail (inbox, deleted items, any other mail folder or folder), and to send you a confirmation e-mail that they did so.

Advisory: Do not ask the recipient to “destroy” physical documents or devices. FSSA wants it returned so that we can be assured of its proper destruction. For some, “destroy” may simply mean “toss it in the trash.”

- 2.3. Disclosure Return Request/Attest Letter: in most cases in which client personal information was improperly disclosed to an individual, the FSSA Privacy Officer will send or cause to be sent a letter to the recipient that:
 - 2.3.1.Asks for the return of the client personal information, if it has not already been returned.
 - 2.3.2.Asks the recipient to attest in writing (by signing and returning the letter) that they did not retain, use, or further disclose the client personal information improperly sent to them.
 - 2.3.3.A stamped, self-addressed (to the FSSA Privacy Officer) envelope will be included.

Alert: If OCR investigates a breach, it will ask what efforts were made to retrieve client personal information that was improperly disclosed, if it was in tangible form (as described above).

3. **Corrective Actions**: Within sixty (60) calendar days of a reported privacy/security incident, whether or not the incident resulted in a breach, the FSSA Privacy Officer, in collaboration with the business unit originating the privacy/security incident and others as deemed appropriate by the FSSA Privacy Officer, identify recommended corrective actions to minimize the risk of a reoccurrence of a similar or associated privacy/security incident. The corrective actions may include, but are not limited to:
 - 3.1. Counseling/Retraining: In cases where a lack of privacy discipline on the part of a FSSA staff member is the source of a privacy/security incident/breach, the FSSA Privacy Officer may recommend that the staff member be counseled by their supervisor on the matter and, perhaps, be retrained on FSSA’s Privacy Compliance Policies and the business unit’s privacy policies and procedures.
 - 3.1.1.Such counseling and/or retraining should be documented in the staff person’s file with a confirming e-mail to the FSSA Privacy Officer (for the Incident File) as evidence that the counseling and/or retraining occurred (including date).

Section 5: Incident Management & Breach Reporting Policy

FSSA Privacy Compliance Policies & Procedures

- 3.1.2. In certain cases, the FSSA Privacy Officer may recommend that all staff personnel involved in similar services subject to the privacy/security incident be formally “reminded” of the appropriate confidentiality policies and procedures. The formal reminder may be in whatever form best suits the business unit; a confirming e-mail should be sent to the FSSA Privacy Officer for inclusion in the Incident File as evidence that the formal reminder occurred (including date).
- 3.2. System/Process Modifications: In cases where the FSSA Privacy Officer has recommended changes to application systems and/or business processes to minimize the risk of similar or associated privacy/security incidents (whether or not a breach has occurred):
- 3.2.1. The affected division and business unit should assess the cost, complexity, and likelihood the modification will achieve the risk reduction objective, and made a determination as whether to accept the risk, implement an alternative but equally effective modification, or to proceed with the recommended modification.
- 3.2.2. The affected division and business unit should apprise the FSSA Privacy Officer of their determination.
- 3.2.2.1. If the determination is to accept the risk (and make no changes), the division must communicate this decision in a formal memo to the FSSA Privacy Officer for the Incident File.
- 3.2.2.2. If the determination is to make the modification, the division and business unit should report their progress on a periodic and timely basis to the FSSA Privacy Officer until completion (so that progress and completion may be documented in the Incident File).
- 3.3. Policy & Procedure Changes: The basis for the privacy/security incident may be a result of missing or insufficient policies and/or procedures at the agency and/or business unit level. The FSSA Privacy Officer may recommend appropriate changes on such policies and procedures for enactment by the agency and/or the business unit.
- 3.4. Personnel Actions: Any resulting personnel actions are the responsibility of the business unit. The FSSA Privacy Officer may recommend the business unit consider disciplinary action for staff who repeatedly violate these Privacy Compliance Policies and/or the business unit’s policies and procedures.

Section 5.7: Notice to HHS

Purpose

Under federal regulations, FSSA is required to report to [HHS/OCR breaches](#) that involved the disclosure of [PHI](#). The purpose of this policy is to ensure the timely reporting of such breaches.

Note: improper disclosures of Social Security Numbers are also to be reported to the Office of the Indiana Attorney General; Section 5.5 addresses this requirement.

Policy

The FSSA Privacy Officer is responsible for notifying HHS/OCR of breaches involving PHI in accordance with the HIPAA Breach Rule, and for maintaining a log of all such breaches.

For breaches that are caused by a Business Associate, either the FSSA Privacy Officer or the Business Associate will provide notice to HHS/OCR depending on the circumstances and as directed by the FSSA Privacy Officer.

Procedures

1. Incident Tracking Log: The FSSA Privacy Officer will maintain a master log of all privacy/security incidents, which also identifies those incidents resulting in a breach that is reportable to HHS/OCR. The form and format of the log is at the discretion of the FSSA Privacy Officer.
 - 1.1. The objective is to maintain a comprehensive list of all suspected and confirmed privacy/security incidents, excluding minor incidents.
 - 1.2. Incidents resulting in a breach of PHI will be so identified, and the date each such incident is reported to HHS/OCR will be documented on the log.
 - 1.3. The FSSA Privacy Officer will update the incident tracking log contemporaneously with any actions taken with respect to each privacy/security incident.
2. Notice to HHS/OCR:
 - 2.1. If the breach results in notice to the victims of the breach and PHI was improperly disclosed, the FSSA Privacy Officer will provide notice to HHS/OCR (except as described in 2.2):
 - 2.1.1. If 500 or more individuals (victims) are subject to the breach, the FSSA Privacy Officer will provide notice to HHS/OCR contemporaneously with providing notice to the victims.
 - 2.1.2. If fewer than 500 individuals (victims) are subject to the breach, the FSSA Privacy Officer will provide notice to HHS/OCR:
 - 2.1.2.1. Either contemporaneously with providing notice to the victims; or,
 - 2.1.2.2. Not later than sixty (60) calendar days after the end of the calendar year in which the breach occurred.
 - 2.1.3. Notice to HHS/OCR is made via its website (subject to change by HHS/OCR):

Section 5: Incident Management & Breach Reporting Policy

FSSA Privacy Compliance Policies & Procedures

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>

2.2. If the breach results in notice to the victims of the breach and PHI was improperly disclosed, and the source of the breach is a [Business Associate](#):

2.2.1. If the Business Associate is also a [Covered Entity](#) under the HIPAA rules, the Business Associate typically would provide notice to HHS/OCR:

2.2.1.1. The FSSA Privacy Officer will determine, based on the circumstances, whether collaboration with the Business Associate is necessary regarding the content and timing of the notice to HHS/OCR.

2.2.1.2. The FSSA Privacy Officer will determine, based on the circumstances, whether a copy of the notice to HHS/OCR is needed for the Incident File.

2.2.1.3. These determinations will be documented in the Incident Report and noted on the incident tracking log by the FSSA Privacy Officer.

Section 6: E-mail Policy

Purpose

The purpose of this policy is to establish the rules and procedures to be followed by FSSA and its personnel ([workforce members](#)) with respect to use of electronic mail (e-mail).

Background

E-mail is a primary business communication tool employed by FSSA (and most organizations). It provides a convenient and traceable means to exchange information among staff members, clients, service providers, and the public. However, e-mail can be a significant source of [privacy/security incidents](#), if not used judiciously.

In the normal conduct of business, e-mail is used to send and receive [client personal information](#), as well as other agency sensitive information. This is both a necessary and appropriate use of e-mail technology, and, generally stated, is more secure and cost effective than other information exchange technologies like faxing, provided appropriate controls are used to protect the information from improper disclosure or compromise.

It is important to note that the improper use of e-mail, whether intentional or unintentional, is a major source of privacy/security incidents, including those that result in a [breach](#) of confidentiality. Two common causes of such incidents are misdirected e-mail—i.e., sent to the wrong person; and, e-mailing client personal information insecurely [Outside the State Network](#)—i.e., unencrypted e-mail sent to a **non-in.gov** address.

Therefore, specific e-mail policies and procedures are necessary to direct and guide FSSA personnel in the appropriate use and protection of e-mail; not to hinder communications, but rather to minimize the risk of client personal information being improperly used or disclosed.

Policy

All FSSA personnel are required to comply with this e-mail policy, as further defined in the following subsections.

Section 6.1: E-mail Rules

Purpose

The purpose of this policy is to establish the rules regarding e-mail use by FSSA personnel.

Policy

All [FSSA personnel](#) will follow these rules regarding their use of e-mail in the conduct of state business on behalf of FSSA.

1. E-mail content and attachments are subject to the Use and Disclosure Policy defined in these Privacy Compliance Policies ([Section 1](#)). Only personnel so authorized by their business unit may send client personal information by e-mail.

Advisory: Before sending client personal information by [State E-mail](#), ask yourself:

(1) Is it necessary to include the information?

(2) Is there a better means to communicate the information other than by e-mail (e.g., phone call or hand delivery, *but not fax*); and,

(3) Do I need to encrypt the information (see [Section 6.2 E-mail Security](#))?

Always minimize the amount of client personal information in any e-mail to the least possible amount needed—**Minimum Necessary Applies to State E-mail, as well.**

2. [State E-mail](#) that **contains client personal information**, including any attachments, **cannot be sent Outside the State Network** unless the message and any attachments are secured as specified in [Section 6.2 E-mail Security](#).

Alert: Sending a State E-mail that contains client personal information, including any attachments, Outside the State Network that has not been secured in accordance with Section 6.2 E-mail Security is a violation of these Privacy Compliance Policies, constitutes a privacy/security incident, and may result in personnel sanctions in accordance with state and FSSA policy.

3. State E-mail that contains **client personal information**, including any attachments, may be sent [Inside the State Network](#) without the additional security precautions as specified in [Section 6.2 E-mail Security](#). The sender, however, should consider the volume and types of client personal information being sent and the number of recipients, and encrypt the e-mail message and/or attachments (as described in Section 6.2) if additional protection is appropriate under the circumstances.
4. **Federal Tax Information**, as obtained by the agency from the Internal Revenue Service and the Social Security Administration cannot be sent by e-mail Inside or Outside the State Network.

Section 6: E-mail Policy

FSSA Privacy Compliance Policies & Procedures

5. Subject Line: **Never put client identifying information** in the Subject Line of an e-mail.
 - 5.1. Refer to [Section 6.2 E-mail Security](#).
6. Personnel are strictly prohibited from posting any client personal information regarding FSSA clients on any [social media](#) sites.
7. Personnel may not store state information such as e-mail attachments on non-State-owned equipment or devices except as provided for in [Section 7 Portable Device Policy](#).
8. Personnel will comply with Practice 7.8.1 of the [IOT Security Framework](#) regarding prohibited e-mail practices.
9. Personnel may access their State E-mail remotely using, for example, mobile/smart phones and home computers, subject to the restrictions and guidance in [Section 7 Portable Device Policy](#).
10. Personnel may not allow another person, whether or not they are a workforce member, to use their State E-mail Account. This would be a violation of state security policy ([IOT Security Framework](#)) and the [Information Resource Use Agreement](#) (IRUA) signed by the staff member, and a violation of these Privacy Compliance Policies.

Alert: Allowing someone else to use your State E-mail Account, including giving them your password to state systems, besides being a violation of policy, means anything they do under your name can and will be traced back to you. With your password and/or your State E-mail Account, everything this person does will be assumed to be you.

11. State E-mails should be sent only to **known** businesses, clients, or other State E-mails accounts:
 - 11.1. **Personnel are individually responsible** to ensure State E-mails are sent only to the **intended and authorized recipient**; misdirected e-mail may result in a [privacy/security incident](#).

Caution: Outlook automatically populates e-mail addresses based on the first few letters of the recipient's name or e-mail address you type in. It is very easy to accidentally send an e-mail to John.Doe@doc.in.gov instead of the intended recipient Jan.Doe@fssa.in.gov .

12. Signature Block and Confidentiality Notice: All State E-mails that contain client personal information (in the message and/or as attachments) are to include the following signature block:

Your name

Your contact information (title, phone number, e-mail address)

[And, the following confidentiality notice approved by the Office of General Counsel:]

Confidentiality Notice: This communication, including any attachments, may contain confidential or privileged information. If you have received this communication in error, please notify the sender by reply e-mail and destroy all copies of the message and any attachments; do not copy or further transmit the message or any attachments.

Section 6: E-mail Policy

FSSA Privacy Compliance Policies & Procedures

- 12.1. In Outlook, under Tools/Options/Mail Format/Signatures/E-mail Signature the above signature block can be added; the signature block should be selected for **New Messages** and **Replies/Forwards**.
13. Personnel who become aware of a violation or possible violation of this policy are to report the violation to their supervisor; if the supervisor is not available, then it should be reported to the assigned Privacy/Security Liaison. Violations of this policy can lead to a privacy/security incident, as well as staff member sanctions in accordance with FSSA and state policy.
 - 13.1. The supervisor (or [PSL](#)) will review the situation and take appropriate corrective action.
 - 13.2. If it appears that the violation has resulted in a privacy/security incident, the supervisor (or PSL) will act in accordance with [Section 5 Incident Management and Breach Reporting](#) of these Privacy Compliance Policies.

Procedures

None under this policy. Business Units may develop more detailed e-mail procedures, as needed, and such procedures may be more restrictive depending on the business need.

Section 6.2: E-mail Security

Purpose

The purpose of this policy and its supporting procedures is to establish the rules regarding securing e-mail content to protect the confidentiality and integrity of any client personal information that may be legitimately communicated by [State E-mail](#).

Policy

It is FSSA's policy that:

1. Any State E-mail that contains, including attachments, client personal information that is to be sent [Outside the State Network](#) must be properly secured through the use of [encryption](#) technologies, as described in this section.
2. It is the individual staff member's responsibility to properly secure any State E-mail the individual sends (including Replies and Forwards) Outside the State Network that contains client personal information and ensure that it is sent to only the intended recipient.
3. It is the individual staff member's responsibility to ensure any State E-mail the individual sends (including Replies and Forwards) Inside the State Network that contains client personal information is sent to only the intended recipient.
4. All State E-mail sent Outside the State Network may be automatically scanned by IOT to detect client personal information. This will help detect and prevent the unauthorized disclosure of client personal information by e-mail.

Procedures

1. Any State E-mail that contains client personal information *and* is to be sent **Outside the State Network** must be secured through the use of **CertifiedMail**. ***This is the required method. Other tools used in lieu of CertifiedMail require the written approval of the FSSA Privacy Office.***

CertifiedMail is the State of Indiana's internally hosted solution to sending [encrypted](#) e-mails [Outside the State Network](#). Your e-mail is encrypted when you send it using CertifiedMail. Your e-mail is actually posted to a secure CertifiedMail server in IOT. The recipient will receive an e-mail telling them they have a secure e-mail message and instructions on how to access the CertifiedMail message through a web portal.

For instructions on how to obtain and use CertifiedMail [double-click](#) on the icon below:



CertifiedMail Guide
V2.pdf

Alert: Do not include client personal information in the subject line. The subject line is not encrypted and appears in the recipients Inbox as part of the e-mail telling them they have a secure e-mail.

Advisory: A CertifiedMail message can also be sent from your smart phone or similar device by typing \$secure as the first word in the subject line. Note this is a dollar sign (\$) followed by the letters e c u r e; there is no S: \$secure

2. Any State E-mail that contains client personal information sent [Inside the State Network](#) can be further protected through Office 2007 encryption techniques. This is not required, but would add protection against inadvertently e-mailing client personal information to the wrong address and/or to further protect highly sensitive information or attachments with large volumes of client personal information.
 - 2.1. Any attachments (e.g., Word file, Excel file, PowerPoint file) can be encrypted, password protected and attached to your e-mail (Attach Files).
 - 2.2. If the text of your e-mail message will contain client personal information, you can write your message in Word and not Outlook; encrypt the Word file and attach it to your e-mail. In the Outlook e-mail text tell the recipient to see the attached file(s).
 - 2.3. The password(s) for the attachments are to be [complex](#) and communicated separately to the recipient(s); e.g., by phone.

Advisory: You can send the password to the recipient by separate e-mail, but you must be sure the recipient's address is correct and use **Delivery Receipt** and **Read Receipt Requested** to verify the correct recipient received your password, or ask them to reply that they received the password before sending the document.

If you routinely exchange encrypted documents with a recipient, you can establish a pre-arranged password with the recipient to be used for all such documents. However, the prearranged password should be changed at least every 90 calendar days.

For instructions on how to encrypt documents/files using Office 2007 [double-click](#) on the icon below:



Safeguard your
Office 2007 files with

Alert: CertifiedMail does not protect you from sending your e-mail to the wrong person.

The first time a recipient receives a CertifiedMail, the recipient goes to the CertifiedMail web portal and creates their own user ID and password, and then has access to the e-mail message.

Section 6: E-mail Policy

FSSA Privacy Compliance Policies & Procedures

Thus, if you send the CertifiedMail to the wrong person, they will be able to access the e-mail message. CertifiedMail's purpose is to protect the content of your e-mail while it is in transit over the Internet.

Advisory: For highly sensitive documents or files with large amounts of client personal information that you need to send Outside the State Network, it is strongly recommended that you encrypt those documents using Office 2007 *and* use CertifiedMail. Then, if the e-mail goes to the wrong recipient, they will not be able to open the documents without the complex password you assigned.

Global Address List Issue:

Outlook has a handy feature that automatically populates the To, CC, and BCC address boxes in an e-mail message based on the first few characters you type in.

Be careful! You can easily send your e-mail to the wrong person—always review the e-mail addresses before you press Send or Send Certified.

All FSSA personnel have access to the Global Address List, which contains the e-mail addresses of everyone with a State E-mail Account, plus a large number of non-in.gov addresses. This is to make it convenient for you to find someone's e-mail address.

Be careful! It is easy to select the wrong person from the Global Address Book. You might mean to select John.Doe@fssa.in.gov, but inadvertently selected Jon.Doe@isdh.in.gov whose address appears right next to John's in the Global Address List.

While the e-mail message and any attachments are secure during transit Inside the State Network, if the wrong recipient receives your e-mail a privacy/security incident may have occurred.

To minimize the risks of sending a misdirected e-mail message containing client personal information Inside the State Network, it is recommended that you encrypt the message and/or attachments following the procedure described above (i.e. Office 2007).

Section 6.3: Using a Scanner to Scan/Send Client Personal Information

Many business units have printer/copier/scanners that can be used to scan and e-mail documents. Most of these scanners have the ability to encrypt the scanned document.

The same security rules apply to documents scanned and e-mailed from a scanner as apply to e-mail, reference [Section 6.2](#) above.

If the scanned document contains [client personal information](#) and it is to be e-mailed [Outside the State Network](#), the document must be [encrypted](#).

If the scanned document contains client personal information and it is to be e-mailed [Inside the State Network](#), it is preferred that the document be encrypted to minimize any risk should the document be inadvertently e-mailed to the wrong address.

Double click on the icon below for simple instructions on how to scan, encrypt, and e-mail documents using the Aficio MP C5000 printer/scanner/copier—refer to the user manual if you have a different model printer/scanner/copier.



Encrypt and E-mail
Scanned Document .p

Section 7: Laptop & Portable Device Policy

Purpose

The purpose of this policy and its supporting procedures is to establish the rules regarding portable devices employed by FSSA personnel, including laptops and smart phones, as well as the use of personally-owned computers to access [State E-mail](#).

Background

Many FSSA staff are assigned a laptop computer for daily use instead of a desktop computer. Other FSSA staff may periodically use a laptop from their business unit's loaner pool when portable computing is needed. Laptops present a particular security risk given that they are subject to theft and loss.

Many FSSA staff members have use of a mobile phone (smart phone) capable of receiving and sending e-mail; some are provided state-issued smart phones for just this purpose. The use of smart phones to send and receive State E-mail is generally permitted, but certain rules are necessary to ensure the continuing protection of client personal information when accessed by way of a smart phone or other device capable of sending and receiving e-mails.

Likewise, many FSSA staff members access their State E-mail Accounts from their personally-owned computers and smart phones over the Internet using Outlook Web App (OWA); also referred to as Outlook Web Access. Doing so is generally permitted provided the staff member applies some simple security rules over OWA use.

Portable media devices, including USB drives, external hard drives, CD/DVD's, and tape present some unique security issues given the ease by which such devices can be lost or stolen. This policy significantly limits what types of portable media may be used to hold client personal information and requires that all such devices be encrypted.

Policy

It is FSSA's policy that:

1. FSSA personnel may use either state-owned or approved personally-owned smart phones or similar devices (e.g., tablets, notepads) to access [State E-mail](#) containing client personal information provided appropriate security controls are in place as described in the Procedures section of this policy.
2. FSSA personnel may use personally-owned personal computers (desktops, laptops, etc.), smart phones, and similar devices (e.g., tablets, notepads) to access State E-mail containing client personal information via OWA provided appropriate security controls are in place as described in the Procedures section of this policy.
3. With respect to [portable media](#): FSSA personnel may not transfer [client personal information](#) to any portable media except FSSA approved and [encrypted](#) USB drives and external hard drives.
 - 3.1. The **use of any other portable media** such as CD's, DVD's, tape, unapproved USB drives, and unapproved external hard drives **is strictly prohibited**.

Section 7: Portable Device Policy

FSSA Privacy Compliance Policies & Procedures

3.2. Client personal information should not be transferred to any portable media unless absolutely necessary for business purposes.

3.2.1. FSSA staff are responsible for the security of client personal information copied to portable media including the ability to completely replicate all of the client personal information should the portable media be lost or stolen.

4. With respect to laptops⁶: FSSA personnel may not transfer client personal information to any laptop that is not encrypted in accordance with FSSA's [encryption standard](#).

4.1. Client personal information may be transferred only to state-owned laptops unless prior permission is granted by the appropriate business unit management for a staff member to use a non-state-owned laptop:

4.1.1. Contractors (that meet the definition of [workforce member](#)) are often required to provide their own laptops; that is, they are not issued a state-owned laptop. Such contractors may transfer client personal information to their laptops provided that:

4.1.1.1. Doing so is a necessary course of business for the contractor in order for them to fulfill their contractual obligations to FSSA;

4.1.1.2. The contractor's host business unit management (who has engaged the contractor) has authorized placing client personal information on the laptop;

4.1.1.3. The laptop is encrypted in accordance with FSSA's [encryption standards](#) and protected with a [complex password](#);

4.1.1.4. The laptop has up-to-date anti-virus and firewall technology in place; the anti-virus and firewall technology must meet or exceed the functionality of the state's anti-virus and firewall technology employed on state-owned laptops; and, the anti-virus and firewall technology must be kept up-to-date at all times (e.g., through a subscription service with the vendor of the technology).

4.1.1.5. The contractor fully agrees to be responsible for the security and confidentiality of any client personal information on the laptop, including providing appropriate and secure backup or the ability to otherwise completely replicate the client personal information; and,

4.1.1.6. The contractor will fully and completely remove all client personal information from the laptop: (1) when it is no longer necessary for the contractor's work for FSSA or (2) upon completion of the contractor's engagement to FSSA, including if the contractor is reassigned to a different FSSA business unit and the client personal information is not applicable to the contractor's new assignment.

4.1.2. FSSA staff should avoid copying client personal information to a laptop unless absolutely necessary for business purposes:

⁶ The term laptop applies to any portable computing platform including, but not limited to, tablets such as iPads, Nexus tablets, Kindles, and Surface tablets, notebooks, and net-books.

- 4.1.2.1. **FSSA staff are responsible for the security of client personal information copied to a laptop including the ability to completely replicate all of the client personal information should the laptop be lost or stolen.**
- 4.1.2.2. Once the client personal information is no longer needed on the laptop, the staff person who copied the information to the laptop is responsible to completely remove all of the client personal information from the laptop (including recycle bin).
- 4.1.3. State-owned laptops may not be taken offsite (out of the state government offices) unless authorized by the staff person's business unit management—reference IOT [Security Framework](#) Chapter 6.2. This authorization may be included in the individual's job description; it may be conferred by e-mail; or, it could be defined in the business unit's policies and procedures (e.g., staff at a certain level are permitted to take their assigned laptop offsite).
5. **With respect to desktops: copying or transferring client personal information to the hard drive of the staff person's desktop computer is strictly prohibited.**
6. **Password Protection:** These Privacy Compliance Policies and the [IOT Security Framework](#) require the use of [complex passwords](#) for all user accounts; this includes passwords for laptops, portable media, encrypted documents, and CertifiedMail accounts.
 - 6.1. **Sharing of your password** with someone else is a **direct violation of this policy.**
 - 6.2. Placing a copy of your password on a laptop or portable media device or smart phone is the same as [sharing your password](#). If the device is lost or stolen, the contents will not be protected, whether or not it is encrypted, if your password is compromised.
7. It is preferred that any client personal information that must be transferred for use by FSSA staff, including contractors (workforce members)—for example, creating or using an Excel spreadsheet or Word document—be retained on the staff person's **home drive** assigned to them by IOT, and not on a laptop or similar device. Home drives are on the state's network, secured, and backed up by IOT. Some business units also have secure share drives for the sharing of documents containing client personal information among authorized users; these drives are also on the state's network, secured, and backed up by IOT.
8. Each FSSA staff person is responsible to comply with this policy and is responsible to help maintain adequate security over their use of portable devices and laptops.

Procedures

- A. With respect to using **smart phones and similar devices**⁷:

⁷ In this respect, similar devices means other portable computing platforms including, but not limited to, tablets such as iPads, Nexus tablets, Kindles, and Surface tablets. FSSA recognizes that tablet-type devices have common features with both smart phones and laptops; thus, the Privacy Compliance Policies and Procedures regarding laptops and smart phones equally apply to tablet-type devices.

Section 7: Portable Device Policy

FSSA Privacy Compliance Policies & Procedures

1. This procedure applies to state issued devices and approved personally-owned (or contractor owned) devices used on a *routine* basis for state business purposes in which client personal information is accessed, including State E-mail accessed via [Exchange ActiveSync](#).
2. The device is to be protected through the use of a complex password which must be entered to access the device and its e-mail function.
 - 2.1. The number of password entry attempts should be set to 10 or fewer.
 - 2.2. After the number of failed password entry attempts has been exceeded the device is to be set to fully erase all data on the device.
 - 2.3. The **password is to be changed** at least every ninety (90) days.
3. The device is to be encrypted in accordance with FSSA's [encryption standards](#). This is to include any removable memory cards used by the device.
4. The device is to be set to auto lock (requiring entry of the password to use the device) after no more than 15 minutes of inactivity.
5. If possible, the number of e-mail messages that may be retained on the device should be limited. This would help minimize any exposure should an unauthorized person somehow gain access to the device.
6. Downloading of State E-mail attachments to the device is generally prohibited, subject to procedure C below.
7. If the device is to be returned, sold, given away, or otherwise disposed of, all of the data on the device is to be permanently erased first. For state issued devices, IOT shall wipe all content prior to re-issuing the device. For non-state owned devices, it is the user's responsibility to permanently erase all of the data on the device (following the manufacturer's instructions for doing so) and to attest that they have done so.
8. If the device is not capable of meeting the standards in this section, the user is prohibited from using it to access any client personal information.
9. Non-state issued devices used to access client personal information under this section require written approval from the FSSA Privacy Officer, excepting only personally-owned devices used as described in Procedure B below.

10. **Alert:** If the device is lost or stolen:

- 10.1. **Immediately change your state network password**—the password you use to access your State E-mail Account and FSSA systems. You can call the IOT Help Desk or use the automated password reset feature provided by IOT.
- 10.2. Notify your supervisor and your assigned Privacy/Security Liaison so that precautions can be taken to monitor any unauthorized attempts to access your State E-mail Account.

Section 7: Portable Device Policy

FSSA Privacy Compliance Policies & Procedures

- 10.3. Call the IOT Help Desk to report the incident. For state-owned devices and for many personal devices, IOT can remotely wipe the device.
- 10.4. If it is your personal device, contact your carrier to report the incident; your carrier can disable the device so it cannot be used as a phone or to access the Internet.

11. **BlackBerry Devices:** Double-click on the icon below for guidance on securing your BlackBerry device in accordance with these policies and procedures:



Blackberry Device
Security User Guide V

- B. With respect to using personally-owned **personal computers/tablets/notepads, smart phones** and similar devices⁸ for accessing State E-mail containing client personal information through OWA:

1. This procedure applies to the use of personally-owned devices used to periodically access State E-mail through OWA (Outlook Web App) (e.g., periodically accessing your State E-mail from your home computer or personal smart phone); as opposed to personally-owned devices approved for use on a routine basis for state business in lieu of using a state issued device (these devices connect to State E-mail directly through [Exchange ActiveSync](#)).
2. Use of personal devices to periodically access State E-mail, either through OWA is permitted.
3. The device should be protected with a complex password, and have up-to-date anti-virus and firewall technology employed as described above. The password should not be stored on the device.
4. Downloading of State E-mail attachments to the device is generally prohibited, subject to procedure C below.
5. If your personally-owned device connects to the Internet by way of a home wireless network (WiFi), your wireless network should be encrypted (WPA2) and password protected to prevent eavesdropping and unauthorized use of your wireless network.
6. If the device is lost or stolen, follow the directions under A.10 above.

- C. With respect to **downloading State E-mail attachments** containing client personal information to personally-owned devices (smart phones, personal computers, tablets, notepads, etc.):

1. Client personal information cannot be stored on non-state-owned devices, subject to Policy #4 of this Section 7.
2. FSSA recognizes that periodically, when accessing State E-mail on a personal device it is necessary to download an e-mail attachment to read it or work with it. In these situations:

⁸ This procedure applies to personally-owned computing platforms including, but not limited to, desktops, laptops, notebooks, net-books, and tablets such as iPads, Nexus tablets, Kindles, and Surface tablets, as well as personally-owned smart phones.

Section 7: Portable Device Policy

FSSA Privacy Compliance Policies & Procedures

- 2.1. The attachment may be downloaded temporarily for immediate use.
 - 2.2. Upon completion, the downloaded attachment is to be immediately deleted (including from any recycle bin).
 - 2.3. Care should be taken to ensure that any downloads are not accessible by others who may otherwise have access to the device (e.g., family members). If necessary, this may require you to encrypt and password protect the document while it is on your device.
 - 2.4. The staff person is responsible to ensure the security and confidentiality of any attachments downloaded, including the introduction of a virus or other malware if any attachments are uploaded (e.g., you revise and e-mail back a Word document; your anti-virus software should scan the document before uploaded to minimize the risk that a virus attached itself to your document).
 - 2.5. Care should be taken to avoid allowing files with client personal information from being automatically backed up to an unauthorized remote location (i.e., auto backup utilities such as Carbonite should be turned off for files containing client personal information).
- D. With respect to **portable media devices** (e.g., USB drives, external hard drives, CD/DVD's, tape):
1. Client personal information cannot be copied or transferred to any portable media except FSSA approved encrypted USB Drives and hard drives.
 2. Copying or transferring client personal information should be limited to only when absolutely necessary for legitimate business purposes and then to the absolute minimum amount of information necessary for the business purpose.
 3. Once the purpose for the copy or transfer is complete, the client personal information on the portable media should be completely erased.
 4. The staff person copying/transferring the client personal information to the portable media is responsible for the security of the device, including the ability to completely replicate all of the client personal information should the device be lost or stolen.
 5. Double-click on the following icon for a list of FSSA approved portable media:


FSSA Approved
Portable Media.pdf
 6. Because the portable media is encrypted, each device must be set up with the appropriate security policies, including the use of a complex password.
 - 6.1. Some of the approved devices require an Administrator to setup the device (and are identified as "Requires Administrator setup" in the approved portable media list). Double-click on the following icon for the device Administrator Instructions:



MXI USB
Administrator Instruc

6.2. Once the device is setup by the Administrator, it is ready for use. Double-click on the following icon for user instructions.



MXI USB User
Instructions.pdf

6.3. Other approved devices do not require an Administrator to setup the device (and are identified as “Does not require Administrator setup” in the approved portable media list). These devices are less complex to use and the user can setup the device themselves. Double-click on the following icon for device setup and use instructions:

[Insert Kingston DT4000 User Instructions]

6.4. Each business unit is responsible for designating a staff member to serve as Administrator for the portable devices to order, inventory, setup (if necessary), and deploy the devices to the users.

6.5. Only users with a legitimate business need for portable media should be provided with the device.

7. When portable media devices are no longer needed by a user, they are to be turned in to the designated business unit Administrator to be recycled, which will permanently erase all data on the device and make it available for reuse.

8. **All other portable media** (non-encrypted) in place at each business unit is to be promptly turned in to the FSSA Privacy Office for proper destruction.

E. Laptop/Portable Media Backup:

1. As noted, staff members are responsible for the security of client personal information copied or transferred to laptops and portable media devices, including the ability to completely replicate all of the data on the laptop/device should the laptop/device be lost or stolen.

2. If the client personal information cannot be easily replicated from FSSA systems, the staff member should backup the client personal information on the device to their network “home” drive. This can be easily accomplished using Windows Explorer (copy or drag).

2.1. If it is not possible or practical to backup the information to one’s “home” drive: for laptops, a backup may be made to approved portable media provided the portable media is secured (e.g., locked in a drawer) and kept separate from the laptop. For portable media, a backup may be made to a second approved portable media device, which is to be secured and kept separate from the first device.

Section 7: Portable Device Policy

FSSA Privacy Compliance Policies & Procedures

- 2.2. Once the purpose for which the client personal information was copied to the device is complete, the client personal information should be appropriately filed for retention purposes and the copies on the device and, as appropriate, the user's home drive or other devices, deleted.
- F. Under Policy #4 of this Section 7, client personal information cannot be copied or transferred to a laptop that is not encrypted. To confirm the laptop you are using is encrypted, double click on the icon below for instructions:



G. With respect to laptops:

1. Laptops should be physically secured to your desk with the use of a cable lock to help prevent theft.
2. Laptops should be physically secured during transport:
 - 2.1. Lock the laptop in the trunk of your car—don't leave it on the seat where it can be easily seen.
 - 2.2. Be sure the laptop is either powered down or in sleep mode requiring entry of your password to gain access.
 - 2.3. Do not leave the laptop unattended during transport.
 - 2.4. Do not leave the laptop in your car (trunk or otherwise) overnight.
3. Family members, friends, and others are strictly prohibited from using a state-owned laptop.
4. FSSA staff are responsible for the security of any state-owned laptops they take offsite (out of the state government buildings).
5. If the laptop is lost or stolen, follow the instructions under A.10 above.
6. If you are using a loaner laptop, prior to turning the laptop back in:
 - 6.1. Delete all client personal information from the laptop, including from the recycle bin.
 - 6.2. Have the administrator of the laptop remove you as a user (this removes your ID and your password from the laptop).

Section 8: Fax Policy

Purpose

Periodically, client personal information must still be faxed. The purpose of this policy is to ensure that faxing client personal information is kept to the minimum necessary and that any such faxing is appropriately secured.

Policy

With respect to faxing client personal information, whether faxed within the agency or outside of the agency, it is FSSA's policy that:

1. Faxing of [client personal information](#) should be avoided if possible; it is more secure⁹ to e-mail the information following the rules established in [Section 6 E-mail Policy](#).
2. If faxing of client personal information is necessary, the procedures established in this policy are to be followed.
3. Under no circumstances is Federal Tax Information received by the agency from the Internal Revenue Service or the Social Security Administration to be faxed. Such information must be otherwise securely communicated (contact the FSSA Privacy Officer for guidance).

This policy only applies to faxing client personal information, including Federal Tax Information; the faxing of other information is subject to the business units' applicable policies and procedures.

Procedures

If client personal information must be faxed:

1. The client personal information is to be limited to the amount minimally necessary for the purpose of the fax (minimum necessary rule applies).
2. The FSSA staff member faxing the client personal information must be authorized to see and use such information in accordance with the business unit's privacy policies and procedures.
3. A fax coversheet is to be used that contains:
 - a. The name, address, and phone number of the business unit sending the fax.
 - b. The name, telephone number, and fax number of the person sending the fax.
 - c. The total number of pages being faxed, including the cover sheet.
 - d. The date and time the fax is sent.

⁹ Faxing over telephone lines is generally insecure as the fax is sent in clear text over open lines and there is no automated authentication of the recipient, and proper receipt cannot be confirmed until after the fax is sent.

Section 8: Fax Policy

FSSA Privacy Compliance Policies & Procedures

- e. Any special instructions regarding the fax, such as special delivery instructions, the need for immediate attention, etc.
 - f. Instructions for the recipient to call the sender immediately upon receipt of the fax to confirm its receipt, including the number of pages received.
 - g. Instructions for the recipient to clear any memory buffers in their fax machine (or delete from their fax server), if the machine is so equipped, so that the fax cannot be reprinted.
 - h. A warning banner across the top: *This fax contains confidential and privileged information.*
 - i. A Confidentiality Notice at the bottom: *This facsimile contains confidential and privileged information. If you have received this facsimile in error, please immediately call the sender and destroy all copies of the facsimile by shredding; clear any memory buffers on your fax machine or delete it from your fax server; and, do not copy or further transmit the facsimile.*
4. The person sending the fax is to call the recipient prior to faxing the client personal information so that the recipient is aware that the fax is being sent; and, to ask the recipient to call back the person sending the fax to confirm its receipt, including the number of pages sent.
 5. Confirm with the recipient that the fax, including all pages sent, was received.
 6. If a fax containing client personal information was inadvertently sent to the wrong recipient:
 - a. The sender should immediately call the recipient:
 - i. Explain the fax was sent in error;
 - ii. Request that the recipient shred the fax (all pages) and clear any memory buffers on their fax machine or delete from their fax server so that the fax cannot be reprinted; and,
 - iii. Obtain verbal confirmation (get the recipient's name, address, and phone number) that the fax was shredded and the memory cleared from their fax machine (or deleted from their fax server).
 - b. The sender should report the incident in accordance with [Section 5.2](#) of these Privacy Compliance Policies.

Alert: The person sending the fax is responsible to ensure the fax is sent in accordance with these procedures, including confirmation that the fax was completely received by the intended recipient.

Section 8: Fax Policy

FSSA Privacy Compliance Policies & Procedures

With respect to client personal information received by fax (sent from within or outside of the agency):

1. The FSSA staff member receiving the fax must be authorized to see and use the client personal information (anticipated to be sent) in accordance with the business unit's privacy policies and procedures.
2. Request that the sender of the fax call you just prior to sending the fax.
3. Stand by the fax machine to ensure you are the only one to physically receive the fax.
4. Confirm the number of pages received matches the count provided by the sender.
5. Call the sender to confirm the receipt of the fax and the number of pages.
6. Clear the memory buffer of the fax machine, if it has one (refer to the machine's operation manual), or delete it from your fax server (if used) to ensure the fax cannot be reprinted.
7. Note on the fax cover sheet the date and time you called the sender and the date and time you cleared the fax machine memory buffer (if it has one; if it does not, make a note to that effect on the fax cover sheet).

Regarding fax machines with stored fax numbers (e.g., speed dial) or the use of fax servers with stored fax numbers:

1. The name of the recipient or organization associated with the fax number should be clearly identified.
2. The fax numbers are to be verified for correctness at least every three months; the business unit owning/using the fax machine is to create a log of each verification and retain it for one year.
 - a. Fax numbers can be verified by calling the recipient or organization associated with the fax number to confirm the number is still valid.
 - b. Changed or discontinued fax numbers should be corrected immediately on the fax machine or fax server.

Section 9: Computer & Paper & Media Disposal

Purpose

Proper disposal of computers, paper records, and other media that contains [client personal information](#) is essential to ensuring such information is completely eradicated as part of the disposal process; thus, avoiding any opportunities for a [privacy/security incident](#) to occur.

Policy

It is FSSA's policy that:

1. Each business unit will develop Computer & Paper & Media Disposal policies and procedures, and submit those to the FSSA Privacy Officer for review and approval.
2. With respect to computers (desktops, laptops, tablets, and similar computing devices including state-owned smart phones), the business unit's policies and procedures should address:
 - a. Maintaining an inventory of such devices to be disposed of or put into surplus (e.g., asset tag number, description, date disposed of);
 - b. Sanitizing the memory and hard drives of the devices; this may include reliance on IOT for sanitizing¹⁰ devices;
 - c. Disposing of all such devices by returning the device to the Indiana Office of Technology (IOT) for proper sanitization and physical disposal (or reimaging and redistribution); and,
 - d. Specifically addressing such devices that are not going to be returned to IOT and how the devices will be sanitized and physically disposed of or sanitized and put into surplus.
3. With respect to paper disposal, the business unit's policies and procedures should address:
 - a. A requirement to shred all paper documents that contain client personal information;
 - i. A definition as to the type and degree of shredding (e.g., cross-cut shredding; shredding in conformance with the NSA/CSS 02-01 specification);
 - b. Provision of secure shred bins or baskets (e.g., locked), including distribution; and,
 - c. A determination as to whether the business unit will perform the shredding or use a qualified third-party service (Business Associate Agreement required for third-parties).
4. With respect to electronic media (e.g., USB drives, CD/DVD's, tapes, external hard drives, etc.), the business unit's policies and procedures should address:
 - a. Sanitizing memory (e.g., USB drives) and hard drives prior to disposal or putting into surplus;
 - i. Keeping a log of all such devices sanitized and disposed of or put into surplus

¹⁰ Sanitizing of hard drives and memory (where data is retained in memory) and media cards typically is to be done in conformance with the National Institute of Standards & Technology (NIST) Special Publication 800-88 Rev 1.

Section 9: Computer & Paper & Media Disposal

FSSA Privacy Compliance Policies & Procedures

- ii. Sanitizing in conformance with NIST 800-88 Rev 1
 - b. Method of physical disposal or putting into surplus; and,
 - c. Means to thoroughly destroy media such as CD/DVD's and tapes, as part of the disposal process, such that any data that may be contained on the media is irretrievable.
5. With respect to microforms (e.g., microfilm, microfiche, etc.), the business unit's policies and procedures should address:
- a. The method and means to securely collect microform media (e.g., use of locked burn bins); and,
 - b. The method and means to thoroughly destroy microform media (e.g., burn to white ash), including whether the business unit will engage a third party to perform the destruction (requires a Business Associate Agreement).

Procedures

As discussed above, each business unit is to develop Computer & Paper & Media Disposal policies and procedures and submit them to the FSSA Privacy Officer for review and approval.

Advisory: All FSSA business units are strongly encouraged to turn into the FSSA Privacy Office all CD/DVD's, tapes, unapproved USB drives, unused phone memory cards, and similar media as soon as possible for proper disposal. In accordance with [Section 7](#), only FSSA-approved portable media may be used; all other media will need to be sanitized and disposed of. The FSSA Privacy Office will undertake the disposal effort for this media so the business units need not worry about the proper disposal of these legacy items.

If any of the unapproved media contains information the business unit needs to retain, the information first may be copied to an approved portable media device or to the network home drive of an authorized user prior to turn in.

Section 10: Training Requirements

Purpose

All FSSA personnel must be trained on these Privacy Compliance Policies in order to assure continuing compliance with these policies and procedures.

Policy

All [FSSA personnel](#) are to be trained on these Privacy Compliance Policies. All new hires and transferees will be trained on these Privacy Compliance Policies within thirty (30) calendar days of their hire or transfer date. All FSSA personnel will receive refresher training on these Privacy Compliance Policies on a schedule determined by the FSSA Privacy Officer.

The FSSA Privacy Officer will provide updates to the training as substantive changes to these Privacy Compliance Policies are released.

All business unit personnel will be trained on the business unit's subsidiary policies and procedures within a reasonable timeframe established by the business unit.

Procedures

In collaboration with FSSA Human Resources and agency management, the FSSA Privacy Officer will determine the most appropriate procedures for providing the required training.

The objective will be to provide a training curriculum and delivery method most suitable to effectively reach all FSSA personnel within the required timeframes. The FSSA Privacy Officer will develop, to the extent needed, more detailed procedures on training content development, deployment, and competency exams.

Section 11: Staff Protection from Retaliatory Acts

Purpose

One objective of this policy is to help ensure that any known or suspected privacy/security incidents are promptly reported. Staff personnel must be assured that if they report a known or suspected privacy/security incident they will not be subjected to any form of retaliatory act or disciplinary action by FSSA or the state.

Policy

It is FSSA's policy that the agency, including its management and staff, will not intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against any member of FSSA's [workforce](#) who has reported a known or suspected privacy/security incident or has exercised any rights under the applicable federal and state laws and regulations (under which these Privacy Compliance Policies were developed). Such retaliatory acts are a direct violation of this policy.

This policy does not prevent FSSA from undertaking appropriate disciplinary action for policy violation(s) by a staff person reporting a suspected or known privacy/security incident.

Procedures

1. If any member of FSSA's workforce believes they have been retaliated against, regardless of form, for reporting a known or suspected privacy/security incident, the staff person should immediately notify their supervisor, unless the supervisor is the alleged source of the retaliation in which case the staff person should report the situation to the FSSA Human Resources Director.
 - 1.1. If, after reporting an alleged retaliation to their supervisor the staff person believes the supervisor has not acted on the report in good faith or in a timely manner, the staff person should contact the FSSA Human Resources Director.
2. The staff person's supervisor, in collaboration with the FSSA Human Resources Director, will promptly investigate the alleged retaliation and report the results to the FSSA Human Resources Director.
 - 2.1. If appropriate, the Human Resources Director will undertake the investigation.
3. The FSSA Human Resources Director will respond to the results of the investigation in accordance with FSSA's policies for dealing with policy violations, including the imposition of sanctions on those responsible for the retaliatory acts.

Section 12: Sanctions for Policy Violation¹¹

Purpose

It is the purpose of this policy to establish the sanctions FSSA personal are subject to for violation of these Privacy Compliance Policies and Procedures.

Policy

Failure by [FSSA staff](#) to comply with these Privacy Compliance Policies and Procedures, including any supplemental polices established by FSSA regarding the privacy and security of client personal information in FSSA's safekeeping and any subsidiary policies and procedures established by a FSSA business unit will be addressed using the State Personnel Department Progressive Discipline Policy and/or agency specific policy.

Those authorities prescribe the procedures for investigation, standards for decision making, and process for third party review of outcomes. Determinations of the severity of misconduct (categorization as minor, serious, or severe) will include consideration of factors identified in the state and federal laws identified within this policies (e.g., severity, intent, and patterns). Sanctions for contracted staff will be based on the provisions indicated in the applicable contracts and/or agreements.

Any use or disclosure of client personal information that is inconsistent with these Privacy Compliance Policies and Procedures, any supplemental polices established by FSSA regarding the privacy and security of client personal information in FSSA's safekeeping and any subsidiary policies and procedures established by a FSSA business unit will be reported to the applicable Privacy/Security Liaison and/or the FSSA Privacy Officer as defined in Section 5 of these Privacy Compliance Policies and will be investigated as described therein.

FSSA personnel should also understand that in addition to any sanctions that may be imposed under this policy, the individual may also be subject to criminal and civil penalties as prescribed under applicable state and federal law.

Procedures

None under this policy.

¹¹ This replaces FSSA-AD1-17.

Section 13: Retention Policy

Purpose

FSSA is obligated under both state and federal laws and regulations to maintain certain documentation regarding client personal information for specified periods of time (e.g., Indiana Public Records Retention, HIPAA Privacy Rules, etc.).

Policy

All actions and activities under these Privacy Compliance Policies will be documented and retained in accordance with applicable retention laws and regulations, but in all cases for no less than six (6) years from their date of creation. Each version of these Privacy Compliance Policies will likewise be retained for a period of no less than six (6) years from its creation date.

The individual business units are responsible to retain copies of their subsidiary policies and procedures in accordance with applicable retention laws and regulations, but in all cases each version must be retained for no less than six (6) years from its creation date.

The FSSA Privacy Officer is responsible for maintaining all documented actions and activities (e.g., Incident File) under these Privacy Compliance Policies for the required timeframe and in a manner that allows for reasonable, timely retrieval.

Procedures

The FSSA Privacy Officer will develop procedures for the Privacy Office to document and maintain these Privacy Compliance Policies and all actions and activities under these Privacy Compliance Policies in a manner consistent with this policy.

Section 14: Definitions

These definitions apply to these Privacy Compliance Policies and Procedures.

Term	Definition
Breach	<p>This term breach has a particular meaning under the HIPAA Breach Rule: the acquisition, access, use, or disclosure of protected health information in a manner not permitted under the HIPAA Privacy Rules which compromises the security or privacy of the protected health information.</p> <p>Under these Privacy Compliance Policies, this definition is expanded to include all client personal information in FSSA’s safekeeping in which an improper disclosure of client personal information has occurred in violation of these policies, business unit policies, state security policies, and/or applicable federal and state laws and regulations.</p> <p>Under the HIPAA Breach Rule, <u>a breach requires written notification to the victim</u> of the breach (the person whose PHI was improperly disclosed). Under these Privacy Compliance Policies, the requirement is expanded include breaches of any client personal information in FSSA’s safekeeping.</p> <p>In addition, certain state laws and administrative codes require written notice to the victim of a breach of confidentiality (e.g., IC 4-1-11 requires notice to the victims of a security breach; IAC 5-1-1 requires notice to victims for which their social security number is disclosed in violation of IC 4-1-10). Thus, the expansion of the definition of a breach under these Privacy Compliance Policies helps to assure FSSA’s compliance with state laws and regulations.</p> <p>The HIPAA Breach Rule allows for certain exclusions in which an improper disclosure is not considered a breach; for example, unintentional access otherwise made in good faith or a disclosure in which there is reasonable belief that the recipient could not have retained the client personal information.</p> <p>The FSSA Privacy Officer will consider these exclusions as guidance, in addition to guidance provided by other sources such as the Office of the Indiana Attorney General, with respect to making a determination as to whether a privacy/security incident has resulted in a breach.</p>
Business Associate	<p>A Business Associate (BA) is a person or entity that performs a service for FSSA and within the scope of that service obtains, creates, maintains, or uses client personal information—specifically, protected health information. BA’s are under contract with FSSA and the contract has specific provisions</p>

Section 14: Definitions
FSSA Privacy Compliance Policies & Procedures

		<p>regarding the BA’s obligations with respect to the client personal information, including PHI.</p> <p>Individual contractors acting as a member of FSSA’s workforce may not necessarily be BA’s, but are still obligated to comply with these Privacy Compliance Policies and all applicable laws and regulations protecting client personal information.</p>
Business Unit(s)		<p>Business unit means, collectively and individually, FSSA divisions, bureaus, sections, facilities (including State Operated Facilities, or SOF’s), and program areas. This is a term of convenience.</p> <p>For example, the Division of Family Resources is a business unit; the Bureau of Child Care is a business unit within the Division of Family Resources business unit.</p>
Client		<p>Means constituents, beneficiaries, applicants, patients, customers, members, and other terms used by FSSA’s various programs to describe individuals who have <u>applied for and/or are the recipients of FSSA services</u>. This includes information on former clients (applicants, beneficiaries, etc.) whose information remains in FSSA’s safekeeping.</p> <p>Use of the term client is intended to simplify policy and procedure statements by having a single reference term.</p>
Client Personal Information		Means Personal Information about a client.
Complex Password		<p>In accordance with IOT Security Framework Practice 8.2.1 (state security policy), a complex password is:</p> <ol style="list-style-type: none"> 1. A password that contains at least eight (8) characters; and, 2. A password that contains characters from three of the four following categories: <ol style="list-style-type: none"> 2.1. English uppercase letters (A-Z) 2.2. English lowercase letters (a-z) 2.3. Base ten digits (0-9) 2.4. Special characters (\$, #, %, *, _, etc.) <p>For example: Jk23&\$BA is a complex password. The word BLUE is not a complex password.</p> <p>The use of two-factor authentication—for example, use of biometrics and a PIN—instead of a complex password requires written permission of the FSSA Privacy Officer.</p>
Covered Entity		<p>A Covered Entity is an entity that must comply with the HIPAA rules.</p> <p>HIPAA defines a Covered Entity as a health plan, a health care clearinghouse, or a health care provider who transmits in electronic form any of the transactions covered under HIPAA</p>

Section 14: Definitions
FSSA Privacy Compliance Policies & Procedures

	<p>(e.g., claims).</p> <p>Under the HIPAA rules, state Medicaid plans are specifically identified as Covered Entities. Much of FSSA falls within the definition of a Covered Entity.</p>
Disclosure	<p>As used in these Privacy Compliance Policies, Disclosure means to provide client personal information to someone or some entity.</p> <p>Proper disclosures occur all of the time in the course of the agency’s business. We disclose to providers that a client is eligible for medical services covered under their Medicaid plan; we disclose client case information to the client regarding their benefits status; we disclose client personal information to one another as part of our day-to-day jobs.</p> <p>Improper disclosures occur when we disclose client personal information to someone or some entity who is not authorized to have the information; a disclosure that is not permitted by these Privacy Compliance Policies and the laws and regulations under which they were developed (e.g., HIPAA Privacy).</p>
Encryption	<p>Encryption makes words, documents, files, and e-mail indecipherable to anyone who might see the information, unless they have the decryption key. The purpose is to prevent an unauthorized person from seeing the content.</p> <p>For example, say you want to send the message, “How are you, today?” Anyone who can see your message can see exactly what you wrote.</p> <p>However, if you encrypt the message, the reader would only see “ch& 99! Oh% 7h\$9O,” unless they have the key to decode the message.</p> <p>Encryption technology works behind the scenes. For example, when you send an e-mail by CertifiedMail, CertifiedMail encrypts the message. When the recipient logs into the CertifiedMail portal to retrieve your message, CertifiedMail will decrypt the message for them, but only for them.</p> <p>Similarly, if you encrypt an Excel file, Excel will ask you for a password. The only way for someone to decrypt the file is to enter that password; otherwise they cannot see the content.</p> <p>It works the same way for the hard disk on your laptop. If it is encrypted, they only way anyone can access the hard drive and use your laptop is if they enter your password. Even if they extract the hard drive from your laptop they cannot read the information on the hard drive.</p> <p>The use of encryption helps protect the agency and you. For example, if you mistakenly send an Excel file by e-mail to the</p>

Section 14: Definitions
FSSA Privacy Compliance Policies & Procedures

	<p>wrong recipient, and the Excel file is encrypted, then the information is not compromised because the recipient cannot open the file or see its contents without the password.</p>
<p>Encryption Standards</p>	<p>The encryption standards for portable devices approved by FSSA are those consistent with NIST Special Publication 800-111 <i>Guide to Storage Encryption Technologies for End User Devices</i>.</p> <p>The encryption standards for data in motion (transit) are those that comply with FIPS (Federal Information Processing Standards) 140-2, which includes, as appropriate, NIST Special Publication 800-52, <i>Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations</i>; 800-77, <i>Guide to IPsec VPNs</i>; or 800-113 <i>Guide to SSL VPNs</i>; and, may include others that are FIPS 140-2 validated.</p> <p>At a minimum, encryption technology employed by FSSA, including contractors to FSSA, will meet or exceed the encryption functionality for both data at rest and data in motion employed by IOT.</p>
<p>Exchange ActiveSync</p>	<p>Exchange ActiveSync is the technology employed by IOT to automatically synchronize Outlook e-mail and calendars with a person’s smart phone.</p> <p>The smart phone has to be setup to use Exchange ActiveSync. State-issued smart phones (e.g., Blackberries) are setup for Exchange ActiveSync. Personally-owned smart phones can also be set up for Exchange ActiveSync, provided the smart phone is approved by the FSSA Privacy Officer and its use is approved by the staff person’s business unit.</p> <p>Exchange ActiveSync requires that the staff person’s network ID and password be captured in the smart phone in order for the automatic synchronization to work (e.g., you enter a calendar event in your smart phone, your Outlook calendar is automatically updated; you receive an e-mail in your Outlook inbox, the same e-mail automatically appears in your smart phone’s Exchange e-mail in box).</p> <p>This is why appropriate security controls over the smart phone are needed. If your smart phone is lost or stolen, whoever obtains it can access your State E-mail unless the device is secured with a complex password.</p>
<p>HHS</p>	<p>U.S. Department of Health and Human Services (HHS), which is the parent agency of the Centers for Medicare and Medicaid Services (CMS) and the Office of Civil Rights. HHS has ultimate responsibility for the development, promulgation, and enforcement of the HIPAA rules, as well as the regulations</p>

Section 14: Definitions
FSSA Privacy Compliance Policies & Procedures

		regarding Medicaid programs.
HIPAA		<p>Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191). As a federal law, HIPAA has several components. For the purposes of these policies, we mean Title II, Subtitle F of the Act, which addresses Administrative Simplification.</p> <p>This section, among other things, provides the legal basis for the HIPAA Privacy Standard (or Rule) and the HIPAA Security Standard (or Rule), as well as the standards regarding HIPAA Compliance and Enforcement, and Civil Penalties (for failure to comply). Reference 45 CFR Parts 160, 162, and 164).</p> <p>HITECH supplemented HIPAA with, among other things, the HIPAA Breach Standard (or Rule).</p> <p>The HIPAA Act, as supplemented by HITECH, updated the Social Security Act, including Sections 1176 and 1177, which establish both civil and criminal penalties for HIPAA violations (the former for failure to comply with HIPAA, the latter for misuse of client personal information).</p>
HITECH		<p>In February, 2008 Congress enacted the Health Information Technology for Economic and Clinical Health Act (HITECH) as part of the American Recovery and Reinvestment Act (ARRA).</p> <p>Subtitle D of HITECH strengthened some of the provisions of the HIPAA Privacy Rule, ensured Business Associates are covered by HIPAA Privacy/Security, expanded enforcement capabilities, and increased the monetary penalties for failure to comply and the criminal penalties for abuses of protected health information.</p>
ICES		<p>The Indiana Client Eligibility System (ICES) is the system of record for all FSSA clients (past and present) and applicants. ICES contains, among many elements, client/applicant demographics, benefit programs applied for/receiving, identification of Authorized Representatives, legal guardians, family members, and case supporting information.</p>
Improper Disclosure		<p>This is a disclosure of client personal information to people or organizations not authorized by policy or law to receive such information, including the disclosure of client personal information in violation of applicable laws and regulations, these Privacy Compliance Policies, business unit policies, and/or state policies.</p> <p>For example, under HIPAA PHI cannot be disclosed to a state legislator unless the client has expressly authorized the disclosure.</p>
Incident File		<p>An electronic file, organized by privacy/security incident,</p>

Section 14: Definitions
FSSA Privacy Compliance Policies & Procedures

	<p>maintained by the FSSA Privacy Officer that contains all of the pertinent information regarding any given privacy/security incident. A secured paper file may also be maintained.</p> <p>Incident Files are maintained on a highly secured SharePoint site under the direct and sole control of the FSSA Privacy Officer.</p>
Incident Report	<p>This refers to the official Incident Report prepared by the FSSA Privacy Officer (or their delegate) regarding known and suspected privacy/security incidents.</p> <p>The objective of the report is to capture all of the pertinent details regarding a reported privacy/security incident and the conclusion drawn from the evidence (e.g., whether a reportable breach of confidentiality has occurred).</p> <p>Attached by reference to the report is all of the supporting information regarding the incident such as copies of e-mails about the incident, copies of the client personal information improperly disclosed or compromised, copies of notices (to the victims), and a list of all personnel involved in the incident.</p> <p>Multiple Incident Report forms are used, depending on the type of incident. The Privacy Officer is responsible to maintain the Incident Report forms and preparation guidance.</p>
OAG	Office of the Indiana Attorney General.
OCR	Office of Civil Rights (OCR). OCR is a division of HHS and is directly responsible for the development, promulgation, and enforcement of the HIPAA Privacy, Security, and Breach rules.
Personal information	<p>With respect to these policies, is the same as Client Personal Information.</p> <p>This is information about an individual, including health information.</p> <p>This is information that identifies the individual (e.g., name) and something about the individual (e.g., address, date of birth, gender, etc.).</p> <p>Certain types of client personal information are protected under state or federal law: PHI, PII.</p> <p>Client personal information includes information regarding an individual’s legal guardian, authorized representative, family members, assistance group members, health care representative, provider, and other people directly associated with the individual.</p> <p>Client personal information may be in any form: electronic, paper (including microfiche and similar media), or within</p>

Section 14: Definitions
FSSA Privacy Compliance Policies & Procedures

		verbal communications.
Personally Identifiable Information—PII		<p>This is information associated to an individual; also referred to as PI or client personal information or Protected Information.</p> <p>Under IC 4-1-6 PI means any information that describes, locates, or indexes anything about an individual or that affords a basis for inferring personal characteristics about an individual (e.g., education, financial transaction, medical history, employment records, photographs, etc.).</p> <p>Under IC 4-1-11, PI means an individual’s first name and last name or first initial and last name; and, at least one of the following: (a) social security number; (b) driver’s license number or identification card number; or (c) account number, credit card number, debit card number, security code, access code or password of an individual’s financial account.</p>
Portable Media		<p>This term refers the electronic media that can be used to store information including, but not necessarily limited to: USB drives, external hard drives, CD’s, DVD’s, tape, and smart phones that can also be used as USB drives.</p>
Privacy/Security Incident		<p>A privacy/security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of client personal information (CPI) or interference with system operations in an information system.</p> <p>Examples include (but are not limited to):</p> <ul style="list-style-type: none"> • An e-mail containing CPI is sent outside of the state network and is not encrypted (e.g., not sent by CertifiedMail)—this could lead to attempted or successful unauthorized access to the information. • An appeal hearing packet is mailed to the wrong person—this could result in the disclosure of CPI to an unauthorized person. • A laptop containing or potentially containing client personal information is stolen—the thief may gain access to this information. • The verbal disclosure of client personal information of an adult client to a family member of the client who is not the client’s authorized representative or legal guardian—this is successful unauthorized access and an improper disclosure. • An e-mail containing CPI sent inside the state network but to wrong person in another agency—unauthorized access has occurred. • A virus or other malware is detected on a state computer (or a personal computer legitimately being used for state business)—at a minimum this is

Section 14: Definitions
FSSA Privacy Compliance Policies & Procedures

	<p>interference with system operations and, depending on the type of malware, may lead to unauthorized access to CPI.</p> <ul style="list-style-type: none"> • A case worker shows a client personal information about the client on a computer screen, but discovers the information does not belong to that client (it was incorrectly attached to the wrong client file)—this is an improper disclosure resulting in unauthorized access to client personal information. • Unauthorized access to an application (e.g., AIM, ICES, INsite, etc.)—this may lead to unauthorized access to CPI and is an intrusion; unauthorized access can occur from a variety of sources ranging from someone obtaining an authorized user’s ID and password to an external intrusion (hack) into the system.
Privacy/Security Liaison	Reference Section 4 of these Privacy Compliance Policies for an explanation. Also referred to as PSL.
Protected Health Information—PHI	<p>Information that relates to an individual’s past, present, or future physical or mental health or condition, including the provision of healthcare to the individual, <i>and</i> the past, present, or future payment for healthcare, and which identifies the individual (or which can be used to identify the individual).</p> <p>For example, a Medicaid claim is PHI; an individual’s application for a disability waiver program is PHI.</p> <p>PHI is specifically protected by HIPAA.</p>
Safekeeping	<p><u>Client personal information</u> that is created, obtained, maintained, and used by FSSA in its normal course of business, regardless of form, for which there is a reasonable expectation or regulatory requirement that the information is to be kept secure, confidential, and not improperly changed.</p> <p>This includes client personal information created, obtained, maintained, and/or used by a third party on FSSA’s behalf (and under contract with FSSA for services that require use of client personal information).</p> <p>In particular, PHI and PII are to be safely kept.</p>
Section 1176 of the Social Security Act	<p>This section establishes the penalties for failure to comply with the provisions of the HIPAA Privacy Rule. The penalties are tiered based on the nature and circumstances of the offense and range from \$100 per violation (with an annual limit of \$25,000 for repeatedly violating the same provision) to \$50,000 per violation (with an annual limit of \$1.5 million for repeatedly violating the same provision).</p> <p>Sections 13401 and 13404 of <u>HITECH</u> provides that these</p>

Section 14: Definitions
FSSA Privacy Compliance Policies & Procedures

	penalties apply to Business Associates, as well as covered entities.
Section 1177 of the Social Security Act	<p>This section establishes the penalties for person or covered entity who knowingly violates the HIPAA Privacy Rule:</p> <ol style="list-style-type: none"> 1. Be fined not more than \$50,000, imprisoned not more than 1 year, or both; 2. If the violation is committed under false pretenses, be fined not more than \$100,000, imprisoned for not more than 5 years, or both; and 3. If the violation is committed with the intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm, be fined not more than \$250,000, imprisoned not more than 10 years, or both. <p>Sections 13401 and 13404 of HITECH provides that these penalties apply to Business Associates, as well as covered entities. Section 13409 of HITECH clarified that these penalties also apply to individuals (including employees).</p>
State E-mail	<p>Means e-mail used by FSSA personnel to conduct the state’s business on behalf of FSSA and the State of Indiana—the content of the e-mail, including attachments, is for state or FSSA business.</p> <p>Typically, this is e-mail generated from or sent to your State E-mail Account.</p> <p>Contrasted with personal e-mail used by staff to conduct their personal business; typically, this is e-mail generated from or sent to your personal e-mail account (like Gmail, Yahoo, Hotmail, Comcast, ATT, etc.).</p>
State E-mail Account	<p>Your State E-mail Account (or Address) is the fssa.in.gov e-mail address assigned to you by FSSA Account Control/IOT.</p> <p>For example: John.Doe@fssa.in.gov</p> <p><u>All state e-mail accounts end in in.gov.</u> For example, Jane Doe at the Indiana State Department of Health would have an e-mail address of Jane.Doe@isdh.in.gov.</p>
State Network	<p>This is the technical infrastructure provided and managed by the Indiana Office of Technology (IOT) used for access to state systems (e.g., ICES) and e-mail communications.</p> <p>With respect to e-mail: “Inside the State Network” means that e-mail from one in.gov e-mail address is sent to or received from another in.gov e-mail address.</p> <p>For example: Jane.Doe@isdh.in.gov sends an e-mail to John.Doe@fssa.in.gov. This e-mail would be transmitted</p>

Section 14: Definitions
FSSA Privacy Compliance Policies & Procedures

	<p>inside the state network.</p> <p>Whereas, “Outside the State Network” means the e-mail is either sent to or received by a non-in.gov email address over the Internet.</p> <p>For example: John.Doe@fssa.in.gov to Jan.Doe@anthem.com. This e-mail would be transmitted outside the state network as it is going to a company (non-state) e-mail account over the Internet.</p> <p>This would include e-mail from or to a staff member’s personal e-mail account, whether or not the e-mail is sent or received while you are at work.</p> <p>For example: John.Doe@att.net to Jan.Doe@gmail.com or John.Doe@att.net to Jan.Doe@fssa.in.gov are sent to received from outside the state network.</p> <p>Alert: personal e-mail is processed by the e-mail host service (e.g., Google for gmail, Microsoft for hotmail, AT&T for att.net, etc.). This means your personal e-mail goes through their computer systems and network and may or may not be secure.</p> <p>In addition, because these are Internet-based e-mail services, your personal e-mail could literally travel the world before it reaches its destination; this includes in.gov e-mail sent outside the state network (i.e., to a non-in.gov e-mail address).</p>
Workforce Member	<p>Means FSSA state employees, volunteers, interns, trainees, contractors, and other persons whose conduct, in the performance of work for FSSA, is under the direct control of FSSA, whether or not they are paid by FSSA. This includes contractors engaged by the IDOA Managed Service Provider.</p> <p>The terms <i>personnel</i> and <i>staff member</i> as used in FSSA policies and procedures both mean Workforce Member.</p>

Section 15: Citations & Authorities

These FSSA Privacy Compliance Policies and supporting procedures have been developed under certain federal and state laws and regulations, including but not limited to:

- 45 CFR Parts 160, 162 & 164, Health Insurance Reform: Security Standards; Final Rule (effective April 21, 2003)—HIPAA Security Rule
- 45 CFR Parts 160 & 164, Subpart E, Standards for Privacy of Individually Identifiable Health Information; Final Rule (as amended; effective April 14, 2003)—HIPAA Privacy Rule
- 45 CFR Parts 160 & 164, Subpart D, Breach Notification for Unsecured Protected Health Information; Interim Final Rule (effective September 23, 2009)—HIPAA Breach Notification Rule
- 45 CFR Parts 160 & 164, Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable (effective April 17, 2009)—HIPAA Encryption Guidance
- 42 CFR Subpart F Safeguarding Information on Applicants and Recipients (Medicaid)
- 42 CFR Part 2 safeguards for mental health records
- 7 CFR 272.1(c) Use and disclosure restrictions for Food Stamps applicants/recipients
- 45 CFR 205.50 Safeguarding information for financial assistance programs (TANF)
- 34 CFR 361.38 Protection, use, and release of Personal Information (Vocational Rehabilitation)
- 34 CFR Part 99 (FERPA) privacy of educational records
- IDEA Parts B & C (First Steps); 42 CFR Parts 300 & 303 (confidentiality of student records)
- IC 4-1-11, Notice of Security Breach (effective July 1, 2006)
- IC 4-1-10, Release of Social Security Number (effective July 1, 2006)
- IC 4-1-6, Fair Information Practices; Privacy of Personal Information (reference for dates)
- IC 12-14-1-7 Confidentiality of TANF records
- IC 5-14-3 Access to Public Records
- IC 16-36-1 Health Care Consent
- IC 16-39-2 Release of Mental Health Records
- IC 4-13.1 Office of Technology (authority to establish state security standards and policies)

In addition, the state's technology security standards and polices as defined in the IOT Security Framework: <http://www.in.gov/iot/2339.htm>.

Section 16: Policy Administration

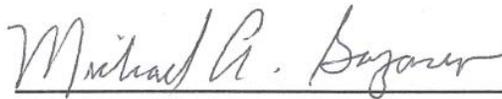
Updates and Version Control

Version	Revision Date	Revision Purpose	Completed By
1.0--Draft	July 27, 2012	Initial Release for Comment Period of 7/30/2012-8/30/2012	Cliff McCullough
1.0	November 27, 2012	Final version incorporating comments from the Comment Period	Cliff McCullough

Signature Page

Related Policies: Replaces FSSA AD1-17 and FSSA AD1-18
Legal Reference: [Section 15: Citations & Authorities](#)
Originating Office: FSSA Privacy Office/HIPAA Compliance Office
Effective Date: December 31, 2012

Approval:



Michael A. Gargano, Secretary
Indiana Family & Social Services Administration