Indiana Family and Social Services Administration
Division of Disability, Aging, and Rehabilitative Services

Policy: Protected Health Information and Records Confidentiality
Effective Date: November 8, 2004

I. Purpose

The Protected Health Information (PHI) and Records Confidentiality policy ensures that the Indiana Division of Disability, Aging, and Rehabilitative Services is in compliance with federal and state statutes regarding the privacy of client health information.

II. Application

This policy applies to all employees of the Indiana Division of Disability, Aging, and Rehabilitative Services who use or disclose protected health information originating from a FSSA designated health care component (DHCC) (defined by FSSA AD1-18). Additional policies may apply to employees of the State Developmental Centers and/or those units who manage Medicaid Waiver programs on behalf of the Office of Medicaid Policy & Planning (OMPP). Employees working in Vocational Rehabilitative Services (VRS) and the Disability Determination Bureau (DDB) shall continue to follow the relevant client confidentiality policies in existence prior to the implementation of this policy. As indicated in FSSA AD1-18, VRS and/or DDB staff who utilize and/or receive client records from other designated health care components (e.g. Medicaid, State Operated Facilities, etc.) within FSSA are subject to the relevant policies developed by these business units.

III. Policy Statement

It is the policy of the Indiana Division of Disability, Aging, and Rehabilitative Services that all employees comply with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 regarding PHI and all other Indiana Family and Social Services Administration policy related to HIPAA compliance, (for example, FSSA AD1-17, FSSA AD1–18, and FSSA IT6-1).

This policy will be implemented through the attached standard operating procedures.

A. Definitions

Health care operations:

means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

a) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

b) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

c) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

d) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

e) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

f) Business management and general administrative activities of the entity, including, but not limited to:

    i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

g) Resolution of internal grievances;

h) The sale, transfer, merger, or consolidation of all or part of a covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

i) Creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

B. **Individually Identifiable Health Information** means:

a) A subset of health information, including demographic information, collected from or about the person who has received or is receiving services, and;

i) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

ii) Relates to the past, present or future physical or mental health condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual; and

iii) That identifies the individual; or

iv) Could reasonably be used to identify the individual.

b) Health information includes information whether oral or recorded in any form or medium.

C. **Payment** means:

a) The activities undertaken by:

i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

iii) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

iv) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

v) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

vi) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

vii) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

viii) Utilization review activities, including pre-certification and preauthorization of services, concurrent and retrospective review of services; and

ix) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

(1) Name and address;

(2) Date of birth;

(3) Social security number;

(4) Payment history;

(5) Account number; and

(6) Name and address of the health care provider and/or health plan.

D. **Protected Health Information (PHI)** means:

a) Individually identifiable health information that is:

- Transmitted by electronic media, which includes Internet, Extranet, leased lines, dial-up lines, private networks, magnetic tape, disk, or compact disk (45 CFR §160.103);
- Maintained in any electronic media; or,
- Transmitted or maintained in any other form or medium, which include oral communication, paper, electronic media, hard drives, or any other removable/transportable digital memory medium.

E. **Treatment** means:

a) The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

V. Legal References and Authority

A. Health Insurance Portability and Accountability Act of 1996, Title II, Administrative Simplification, 45 CFR CFR Parts 160 and 164

B. IC 16-39 et.

VI. Attachments

Standard Operating Procedures for Protected Health Information and Records Confidentiality

APPROVED for Implementation

_____ _____

Director, Division of Disability, Aging, and Rehabilitative Services Date

Indiana Family and Social Services Administration
Division of Disability, Aging, and Rehabilitative Services

Standard Operating Procedures
for
Protected Health Information and Records Confidentiality

Approved by:
Effective Date:

Policy: Protected Health Information and Records Confidentiality

Procedures:

General Information

Knowledge of, understanding of and compliance with state policies and FSSA policies is the responsibility of each individual employee. Due to the nature of the work performed, some employees are responsible for compliance with policies and/or procedures that are developed outside the DDARS Central Office. Examples of policies and/or procedures for which specific employees may be accountable include, but are not limited to, Office of Medicaid Policy and Planning (OMPP) policies and procedures for persons working directly with or on behalf of OMPP and/or the State Developmental Center (SDC) policies and procedures. Employees of the State Developmental Centers and employees working on behalf of the OMPP may have more stringent disclosure procedures due to their day to day contact with clients. In all cases, the more stringent procedure will apply.

Employee Responsibilities

Every employee of the Indiana Division of Disability, Aging, and Rehabilitative Services is responsible for ensuring that confidentiality is maintained for those individuals for which information is available.

Procedures

1. Each employee shall be responsible for maintaining the confidentiality of all PHI in their possession.
2. Employees are required to complete the approved Family and Social Services Administration HIPAA training. New employees are responsible for completing this training within 10 business days of their hire date. If reasonable, employees shall complete the training prior to any exposure to PHI.
3. Any employee who receives documents with PHI and does not need the information to complete his/her assigned duties will place the documents in the locked waste bin provided for paper that needs to be shredded.
4. Any employee who has computer access to PHI and does not need this access to complete his/her assigned duties will inform the Division of Technology Services that access is not required and should be removed from his/her computer.
5. Employees who receive verbal communications that contain PHI, either by telephone or face-to-face, may have temporary notes of the communication that will be destroyed once the work activity is completed. When not in direct use, all temporary notes will be kept in a locking drawer prior to destruction.
6. Employees whose work duties require regular and/or on-going use of PHI shall ensure that his/her access to PHI is limited to the minimal amount of information necessary to perform the work duties.
7. As required by the role based access provisions of HIPAA, Bureau Directors, or their designees, are responsible for determining access needed for assigned staff and for granting the appropriate access for assigned staff.
8. All employees will have access to file cabinets that are routinely locked for filing of PHI when such information is not being used.
9. All employees, except employees of the individual State Developmental Centers shall be required to acknowledge receipt of this procedure and to affirm compliance with the procedure. (Form A)

10. Employees working at the State Developmental Centers are responsible for compliance with the individual centers policies and procedures regarding the Health Insurance Portability and Accountability Act.
11. Employees working within bureaus who manage Medicaid Waiver programs are required to adhere to the relevant OMPP HIPAA Privacy and Security policies and procedures. These employees are also required to complete the relevant OMPP HIPAA training modules.

Requests for Information

During the course of performing work activities, employees may receive requests for information, including data, which is specific to an individual client or would enable the user of the information to identify specific individual(s). The release of this information is governed by the HIPAA Privacy Rule (and other relevant state and/or federal laws).

a. Examples of when disclosure of PHI is <u>permitted</u>:
    - To the individual identified in the information, unless the release would endanger the life or physical safety of the individual or another person.
    - For treatment, payment, or certain healthcare operations (see definition section)
    - As permitted by 45 CFR 164.512 (a-j). Disclosures under this section shall be reviewed by the Privacy Coordinator (or FSSA Privacy Official) assigned to the unit that generated and/or maintains the PHI that has been requested for disclosure.
    - Pursuant to a HIPAA compliant authorization signed by the individual (or their personal representative).
b. Disclosure of client-identifying information is <u>required</u>:
    - To the individual identified in the information, or the individual's personal representative, when requested by the individual or his/her personal representative, unless release to the individual would endanger the life or physical safety of the individual or another person, or
    - When required by the Secretary of Health and Human Services to investigate or determine compliance with the Privacy Rule.

Procedures

1. All releases of information (limited exception would include a treatment related purpose) with PHI shall contain the minimum necessary amount of information required to accomplish the intended purpose of the request.
2. All safeguards (identified below) shall be used to protect the information being released.
3. A Release of Information form signed by the individual identified in the information or that individual's guardian or legal representative, as appropriate, is required for the following types of release:
    - To any person seeking information about the individual for purposes other than treatment, payment, or healthcare operations
    - Psychotherapy notes
    - For any other purpose not permitted or required without an authorization under the Privacy Rule or State law, whichever is more restrictive
4. The Release of Information form should be initiated by the person requesting the information and the original hard copy sent to DDARS. Information being released should be limited to the minimal amount of information necessary to comply with the stated purpose and intent of the release.
5. Some requests may not require a Release of Information form. Employees who think that the release is not required shall request supervisory assistance to obtain verification from the Privacy Coordinator assigned to the relevant designated health care component or the FSSA Privacy Official.

Business Associate Contract Requirements:

All contracts or MOU's that involve the use and/or disclosure of PHI shall verify with the FSSA HIPAA Privacy Official that the appropriate HIPAA contract language has been included.

De-Identification of Client Information

Request for data / information that is not specific to an identified client may be released as long as an individual consumer cannot be identified. According to 45 CFR 164.514 (b), a covered entity may determine that health information is not individually identifiable health information only if:

1. A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
    i. Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
    ii. Documents the methods and results of the analysis that justify such determination; or
2. The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:
    A. Names;
    B. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
        1. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
        2. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
    C. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
    D. Telephone numbers;
    E. Fax numbers;
    F. Electronic mail addresses;
    G. Social security numbers;
    H. Medical record numbers;

I. Health plan beneficiary numbers;
J. Account numbers;
K. Certificate/license numbers;
L. Vehicle identifiers and serial numbers, including license plate numbers;
M. Device identifiers and serial numbers;
N. Web Universal Resource Locators (URLs);
O. Internet Protocol (IP) address numbers;
P. Biometric identifiers, including finger and voice prints;
Q. Full face photographic images and any comparable images; and
R. Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

ii. The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

Due to the extensive requirements for de-identification. the appropriate Privacy Coordinator assigned to the relevant designated health care component or the Bureau Director shall be included in the review process to verify that de-identification has occurred.

Accounting for Released Information

Any use or disclosure of PHI that falls outside of the treatment, payment, or health care operations exception may be subject to the accounting requirements of HIPAA. An example would include a disclosure for audit purposes of a Medicaid Waiver program by the Centers for Medicare and Medicaid Services. The accounting requirement within DDARS applies to the use and/or disclosure of PHI originating from a State Developmental Center and/or a Medicaid Waiver program operated on behalf of the OMPP.

DDARS staff who utilize PHI from a State Developmental Center and/or a Medicaid Waiver program shall be responsible for coordinating with the appropriate Privacy Coordinator from the State Developmental Center and/or OMPP to ensure that the

proper documentation is maintained in accordance with the HIPAA accounting requirements.

Procedures

1. Any employee receiving a request for PHI from a Medicaid Waiver program or a State Developmental Center that does not meet the definition of a treatment, payment, or health care operation shall confer with the Privacy Coordinator from the appropriate State Developmental Center or OMPP to comply with the accounting requirements.

Safeguards for Client-Identifying Information

Procedures

1. Division managers should reasonably limit the number of staff who are authorized to transmit PHI via e-mail. Employees will use due diligence when transmitting client-identifying information via an e-mail system. Extreme caution shall be used when addressing e-mail messages from the global address list in Outlook to avoid an inappropriate disclosure. If at all possible, information shall be de-identified in the transmission.
2. Fax communications shall follow the requirements identified in FSSA Policy AD1-18.
3. Employees, while in public places where there is a possibility of any unauthorized person overhearing the conversation, shall refrain from using (if reasonable) client-identifying information in oral communications, either face-to-face or telephone.
4. Printed or written materials that contain client-identifying information shall be protected from viewing by unauthorized persons. When not directly working with printed or written materials, employees shall ensure that they are in a secured space.
5. Confidential information may not be removed from the office except with specific authorization by the employee's supervisor.

6. All employees working on computers with access to confidential information shall ensure that the workstation is locked if the employee is not at the workstation.
7. Administrators of databases maintained by DDARS shall conduct routine risk assessments to validate that appropriate physical, technical, and administrative safeguards are in place for the management of electronic client-identifying information in these databases. The Division of Technology Services can be contacted for technical assistance in this process.

Form A

Division of Disability, Aging, and Rehabilitative Services
Employee Acknowledgement of
Policy and Procedures for
Protected Health Information and Records Confidentiality

I have received a copy and reviewed the Policy and Procedures for Protected Health Information and Records Confidentiality. I have had the opportunity to discuss the information in the policy and procedures with my supervisor and to ask questions about my responsibilities.

_____ _____

Employee Signature Date

_____ _____

Supervisor's Signature Date