



October 16, 2009

GENERAL LETTER NO. 1-C-19

ISSUED BY: Information Security and Privacy Office, Division of Data Management

SUBJECT: Employees’ Manual, Title 1, Chapter C, **CONFIDENTIALITY AND RECORDS**, Contents (page 1), revised; and pages 38, 39, 40, and 105, revised.

Summary

The Chapter 1-C section, “CONFIDENTIALITY: Sanctions for Violation of Client Confidentiality: Protected Health Information,” is revised to:

- ◆ Remove details on penalties for violation of the Health Insurance Portability and Accountability Act, based on a request from the Department’s Bureau of Human Resources. Violations had been classified as Level 1: Carelessness; Level 2: Unauthorized Access; and Level 3: Malicious, willfulness, or noncompliance for personal gain.
- ◆ Change language to clarify that:
 - A person who violates the Department’s privacy or security policies related to protected health information will be subject to discipline, up to and including discharge.
 - Information collected in the investigation of the violation will be turned over to law enforcement and to any applicable licensing agency.

Effective Date

Immediately.

Material Superseded

Remove the following pages from Employees’ Manual, Title 1, Chapter C, and destroy them:

<u>Page</u>	<u>Date</u>
Contents (page 1)	May 13, 2005
38	October 5, 2007
39, 40, 40a, 40b	May 13, 2005
105	October 5, 2007

Additional Information

Refer questions about this general letter to your service area manager, facility superintendent, or regional collections administrator.

	<u>Page</u>
OVERVIEW	1
Legal Basis.....	1
Purpose.....	3
Purpose of the HIPAA Privacy Rule	4
Applicability of HIPAA Policies	5
Definitions	6
GATHERING INFORMATION	19
Notice to Suppliers of Information	20
Review of Forms.....	21
Personally Identifiable Information	22
Data Processing Matching	28
CONFIDENTIALITY.....	31
Responsibilities of Department Administrators.....	31
Maintaining Security of IRS Data.....	32
Maintaining Confidentiality Within the Department.....	33
When Staff or Relative Is Client.....	35
Releasing Information Over the Telephone.....	35
Volunteer Third-Party Informant.....	36
Reporting a Breach of Confidentiality.....	36
Sanctions for Violation of Client Confidentiality.....	36
Federal Tax Information	37
Protected Health Information.....	38
Assurances of Confidentiality.....	39
Protection of Source.....	39
Request to Withhold Record From Examination.....	40
Request.....	41
Decision	42
Request Granted or Deferred	42
Request Denied	43

No liability shall arise with respect to any disclosure that results from a good faith, but erroneous, interpretation of Section 6103. Return information not directly associated with an individual taxpayer is not considered confidential.

Federal tax return information loses its special status as protected material once a third party has subsequently verified it. Otherwise, the information retains the federal tax information status.

Do not share federal tax information with any subcontractor, volunteer, state legislator, representative of congress, or other state agency. **Exception:** The Welfare Reform Act of 1997 authorizes disclosure of limited information to an agency or contractors to the extent necessary for establishing and collecting child support obligations and locating people owing such obligations.

Federal tax information cannot be provided to the DIA unless it is subsequently verified by a third party through release form 470-3741, *Employer's Verification of Earnings*, or 470-3742, *Financial Institution Verification*. If the client refuses to sign form 470-3741 or 470-3742, a referral for fraud cannot be initiated using the federal tax information.

If you discover a possible improper inspection or disclosure, contact your immediate supervisor and the Treasury Inspector, General Tax Administration, Ben Franklin Station, PO Box 589, Washington, DC 20044-0589 or the TIGTA hotline at or 1-800-366-4484.

Protected Health Information

Legal reference: Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, Sections 1173, 1176 and 1177

If you knowingly and willfully violate HIPAA confidentiality and security policies regarding protected health information, you are subject to civil penalties and criminal investigation and prosecution.

If you violate the Department's privacy or security policies regarding protected health information, you may be subject to disciplinary actions up to and including termination. In addition, all information gathered while investigating the offense shall be turned over to the appropriate law enforcement agency for use in criminal proceedings and to any applicable licensing agency or bureau.

Assurances of Confidentiality

Legal reference: 441 IAC 9.5(17A,22)

Give assurance of confidentiality to people supplying information only as specified under [Protection of Source](#) and [Request to Withhold Record From Examination](#). These policies concern information that would otherwise be available, either to the subject of the record or to the public.

When the information is ordinarily confidential, as described under [AVAILABILITY OF RECORDS](#), you can give assurances of this confidentiality.

Protection of Source

Legal reference: Iowa Code sections 22.7(18), 232.71B, 235A.19, and 235B.6;
441 IAC 175.41(235A), 175.52(235A), and 176.10(3)

You may assure an informant that the informant's identity will not be disclosed, except pursuant to court order, when all of the following conditions apply:

- ◆ The informant is outside of government,
- ◆ The informant is not required by law, rule, or procedure to provide it,
- ◆ The informant does not agree to the release, and
- ◆ You reasonably believe that the informant would be discouraged from providing the information without this protection.

Assure a reporter of child abuse information that the reporter's identity shall be held confidential unless disclosure of the reporter's name is ordered by a court after a finding that the reporter's name is needed to resolve an issue in any phase of a case involving child abuse.

Policies for protecting the identity of a reporter of child abuse are described in 17-B, [ASSESSMENT POLICY](#).

Procedures for protecting the identity of a reporter of dependent adult abuse are described in 16-G, [DEPENDENT ADULT PROTECTIVE SERVICES](#).

When releasing dependent adult abuse information to someone who has access under Iowa Code section 235.6, you may withhold the name of the person who reported the abuse if you believe the disclosure of that person's identity would be detrimental to the person who made the report.

Clearly state any assurances of confidentiality in the record to avoid unauthorized dissemination.

Request to Withhold Record From Examination

Legal reference: 441 IAC 9.5(1) and 9.5(3)

Any person may ask the Department to treat a record as a confidential record and to withhold it from public inspection when the following conditions apply:

- ◆ The person would be aggrieved or adversely affected by disclosure of the record,
- ◆ The person asserts that Iowa Code section 22.7, another applicable provision of law, or a court order authorizes the custodian to treat the record as a confidential record.

Failure of a person to request confidential record treatment for a record does not preclude you, as the custodian, from treating it as a confidential record. However, if a person who has submitted business information to the Department does not request that it be withheld from public inspection under Iowa Code sections 22.7(3) and 22.7(6), you may proceed as if that person has no objection to its disclosure to members of the public.

This provision is most applicable to businesses that are required to submit information that they believe to be trade secrets or to give unfair advantage to competitors. It is intended to put the responsibility for the claim of confidentiality on the business instead of on the Department. It is not likely to be used in relation to Department records.

The Department is required to follow local protocol for joint assessments when both the assessment worker and law enforcement are involved in a case of child or dependent adult abuse. See 16-E(1), [Persons Involved in an Investigation or Assessment](#), and 16-G, [Authorized Access](#), for details of law enforcement access in these cases.

Only FIP and the Food Assistance program provide for release of confidential information to law enforcement in cases not involving a Department fraud investigation, imminent harm, or a deceased subject. Do not release information acquired in the administration of any other program on this basis. The following sections explain these exceptions.

Threat to Health or Safety for All Programs

Legal reference: 441 IAC 9.10(18)“a,” 45 CFR 160.203(b) - (c), 164.512(c), (f), and (j)

Protective service staff request assistance from law enforcement when the subject of a report appears to be in imminent danger. (See 17-B(1), [Access to Child Abuse Information](#), 16-G, [Observation and Ensuring Safety](#), and 16-G(1), [Rejected Intakes/Information and Referral](#).)

When a client threatens or commits harm to Department staff or property, report the client’s name and details of the threat or act to law enforcement officials. Do not release other information regarding the client’s relationship to the Department.

When you believe a client intends to harm someone, you may warn the intended victim or the police or both. Disclose only the name, identification, and location of the client and the details of the client’s plan of harm.

Threat to Health or Safety for Health Information

Legal reference: 441 IAC 9.10(18)“b,” 45 CFR 164.512(j)

You may use or disclose protected health information when you believe, in good faith, that the use or disclosure is necessary:

- ◆ For law enforcement purposes as described in this chapter; or
- ◆ To prevent or lessen a serious and imminent threat to the health or safety of a person or the public and you are making the disclosure to a person reasonably able to prevent or lessen the threat, including the target of the threat.

In these circumstances, observe all applicable laws and standards of ethical conduct.