



Foster Family-based Treatment Association

294 Union Street
Hackensack, NJ 07601

Phone: (800) 414-3382, ext. 113 ~ Fax: (201) 489-4593 ~ E-mail: ffta@ffta.org ~ Website: www.ffta.org

To: Members – Foster Family-based Treatment Association

From: Ken Olson, Chairperson, FFTA Public Policy Committee

Date: April 18, 2003

Re: HIPAA Compliance

The deadlines for compliance with the HIPAA rules are fast approaching. HIPAA could have a dramatic impact on your agency. If you haven't started to work towards HIPAA compliance, please read this memorandum carefully, and consult with your attorney.

This update will provide information to FFTA members on HIPAA and the **actions** required to ensure HIPAA compliance with the privacy standards. Also included is a list of resources that will provide you with additional information about HIPAA. FFTA will send you a subsequent update focusing on code sets and electronic transactions.

1. Background.

1.1 What is HIPAA?

HIPAA requires the Secretary of Health and Human Services ("HHS") to enact rules to establish national standards for electronic transactions between health plans and health care providers. The national standards are intended to enable the healthcare industry to move from inconsistent formats required by different payers to a single system. The law also requires the Secretary to establish standards for protection of the privacy of individually identifiable health information and security of health information systems.

1.2 Who is required to comply with HIPAA?

The "covered entities" to which HIPAA applies includes health care clearinghouses and health care providers. The "rule of thumb" is that a provider of health or mental health services that has a Medicare/Medicaid ID number and uses computers to support clinical and business operations is probably a HIPAA covered entity. **Most treatment foster care agencies are required to comply with the HIPAA standards.**

1.3 What are the HIPAA requirements?

The table that follows identifies the rules enacted by the Department of Health and Human Services and the deadlines for compliance.

RULE	STATUS	COMPLIANCE DATE
Privacy	Final	April 14, 2003
Code Sets and Electronic Transactions	Final	October 16, 2003
Security of Health Information Systems	Proposed. Final rule expected any time.	Spring 2005
Unique Identifiers		
Employers	Final	July 30, 2004
Health Care Providers	Proposed 5/98	Unknown
Health Plans	No action	Unknown
Individuals	No action	Unknown

1.4 Code Sets and Electronic Transactions.

The transactions governed by HIPAA include billing transactions used by most TFC agencies and the exchange of referral information between public and private agencies.

DHHS rules establish national standards for diagnostic and procedure codes to be used in the HIPAA transactions, and for the content, format and data exchange protocols for electronic transactions.

Please note:

- As of October 16, 2003, only HIPAA standard code sets and transaction protocols may be used. “Local codes” are prohibited.
- Health plans, including state administered plans such as Medicaid, are required to participate in HIPAA standard transactions.
- Health care providers are not legally required to engage in electronic transactions. But if they do participate in any of the HIPAA transactions, they must conduct the transaction using the code sets and transaction standards adopted by DHHS. This allows providers to submit paper documents for some or all of the HIPAA transactions to health plans that will accept them, using forms such as the HCFA-1500.

(Please note that reversion to paper transactions is not a viable long-term option for health care providers. Both public and private payers are likely to make electronic billing a condition of participation in their programs. Beginning on October 16, 2003, all Medicare claims are to be submitted electronically, using the HIPAA standards. Private insurance companies that have invested millions to become HIPAA compliant will only see a return on that investment if contracted providers engage in electronic transactions.)

The standard diagnostic and procedure codes applicable to treatment foster care agencies are the ICD-9-CM diagnostic codes and the CPT-4R and HCPCS procedure codes.

1.5 The Privacy Rule.

The most pressing deadline for agencies concerns the privacy provisions of HIPAA. The deadline for compliance with the Privacy Rule is **APRIL 14, 2003**.

The HIPAA Privacy Rule was first enacted in December of 2000 and was revised last year. The Privacy Rule establishes minimum national standards and implementation requirements that HIPAA "covered entities" (**including TFC agencies**) must follow to protect the privacy of "protected health information."

"Protected health information" refers to any "individually identifiable health information" in any form that is created or received by a HIPAA covered entity. Individually identifiable health information means any health information, including demographic information, that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care, or ... payment for the provision of health care to an individual."

The Privacy Rule addresses four main subjects:

- Administrative obligations of covered entities;
- Obligations of covered entities in structuring certain business relationships;
- Use and Disclosure of Protected Health Information;
- Rights of Individuals

As a rule, HIPAA supersedes contrary provisions of law. But HIPAA does not supersede state or federal privacy laws that are "more stringent" than the standards and requirements created by the Privacy Rule. This means that it will be necessary to compare each provision of the Privacy Rule with federal or state law, determine which provision most protects individual privacy or creates individual rights relative to health records, and follow the "more stringent" requirement.

1.6 Security of Information Systems.

HHS published a proposed rule to establish standards for security of health information systems on August 12, 1998. A final rule is expected at any time. The proposed rule addresses four main subjects:

- Administrative procedures to guard data integrity, confidentiality and availability;
- Physical safeguards to guard data integrity, confidentiality and availability;
- Technical security to guard access to protected data; and
- Technical security to protect the integrity and prevent unauthorized access to data transmitted over a communications network.

The deadline for compliance with the final rule will be two years and two months after the final rule is published in the Federal Register. But please note that compliance with some of the provisions of the Privacy Rule is only possible if information systems include appropriate technical mechanisms to control access to protected health information.

2. Actions Required to Meet the HIPAA Privacy Standards

There is very little time available before the April 14, 2003 deadline for compliance with the HIPAA Privacy Rule. By that date, you need to do the following:

- Prepare written Privacy Policies and Procedures.
- Appoint someone to act as your corporate Privacy Officer.
- Appoint someone to act as the Contact Person for individuals who wish to exercise their rights under HIPAA.
- Train staff about your privacy policies and procedures. Ideally, this training should also explain password procedures and other basic methods of protection of the security of information systems.
- Prepare a Notice of Privacy Practices to be given to new service recipients beginning on April 14, 2003. Post a copy of the Notice in your waiting room, or on your web site if you have one.
- Update forms used to secure permission to obtain protected health information about children or disclose that information to third parties. The forms should conform to the minimum HIPAA standards, the Family Educational Rights and Privacy Act (FERPA) and the applicable provisions of state laws.
- Review staff access to protected health information to ensure that access is limited to that which is the “minimum necessary” to enable people to do their jobs.
- Review procedures for responding to requests for disclosure of protected health information to ensure that proper authorization is obtained and records are kept from disclosures.
- Ensure that personnel policies include a statement that employees are expected to follow your organization's policies and procedures for the protection, privacy and security of health information, and that disciplinary action will be taken against employees for violating privacy policies. Keep a record of such disciplinary actions.
- Establish policies and procedures for responding to the following requests by individuals to exercise their rights under HIPAA:
 - Restrict use and disclosure of protected health information;
 - Confidential communications;
 - Review and receive a copy of records;
 - Add information to a record;
 - Receive an accounting of certain disclosures of their protected health information.
- Enter Business Associate Agreements with people or organizations that perform services for your agency and, as a result, have access to protected health information. The agreement must include provisions required by the HIPAA Privacy Rule. Examples of business associates are billing companies, software vendors, attorneys, financial auditors, and **Foster Parents**.

3. Resources Available

A number of books have been published about HIPAA compliance. Many organizations offer consulting services to help HIPAA covered entities evaluate their readiness to comply with the HIPAA standards and to prepare for HIPAA compliance. Information is also available from the Department of Health and Human Services. Here is a list of resources that may help you to understand and address the HIPAA requirements.

3.1 Public Resources.

Department of Health and Human Services	http://www.aspe.hhs.gov/admsimp/
DHHS Office of Civil Rights	http://www.hhs.gov/ocr/hipaa/
Health Resources and Services Administration U.S. Department of Health and Human Services	http://www.hrsa.gov/website.htm#toolkits
Workgroup for Electronic Data Interchange	http://www.wedi.org/

3.2 Publications.

A Path to HIPAA Compliance, is a continuously updated, searchable online guide to HIPAA, including model policies and procedures and forms that may be downloaded and used by subscribing agencies. The guide was written specifically for behavioral health organizations by attorney Paul Litwak. For more information, visit: www.hipaacomplianceguide.com.

3.3 Consultants and Attorneys.

Guidance about HIPAA readiness is available from a number of sources. Three groups that focus specifically on the needs of behavioral health organizations are:

National Council Consulting Services, (301) 984-6200, <http://www.nccbh.org/hipaa.htm>. The National Council for Community Behavioral Health operates a consulting service. The NCCBH consultants have worked with a number of community mental health organizations to help them prepare for HIPAA compliance.

Paul Litwak, Esq. provides legal advice to health care organizations concerned about HIPAA. He can be reached at 757-431-2020, or e-mail: plitwak@att.net. Website: www.paul-litwak.com.

Renee Popovits, Esq. of Popovits & Robinson, PC also specializes in HIPAA compliance for behavioral health organizations. She can be reached at 708-532-7114, e-mail: rpopovits@popovitslaw.com. Website: <http://www.popovitslaw.com>