HIPAA OVERVIEW
For

MULTICULTURAL COMMUNITY SERVICES, INC.
1000 WILBRAHAM ROAD
SPRINGFIELD, MA 01109

What is "HIPAA?"
The Health Insurance Portability and Accountability Act of 1996, commonly referred to as HIPAA, was passed to define and limit the circumstances in which an individual's protected health information (PHI) may be used or disclosed by others and to promote standardization and efficiency within the health care industry.

Health Care providers will be able to take advantage of new technologies which will make doing business with health plans less costly and more efficient. With HIPAA there will only be one way to submit a claim, electronically.

HIPAA provides health care consumers with control over their own health care information, sets boundaries on medical record use and release, ensures the security of health information, and establishes a system for accountability for medical record use and release.

HIPAA covers all health information, regardless of the format, and includes electronic records, paper records, and oral communications. It provides safeguards for the physical storage, maintenance, transmission, and access to an individual's health information.

HIPAA requires standardization of electronic patient health, administrative, and financial data; unique health identifiers for individuals, employers, health plans, and health care providers; and security standards protecting the confidentiality and integrity of "individually identifiable health information", past, present, and future.

Who is affected?
All healthcare organizations, including all health care providers (Home Health, VNA, Hospice), physician offices, health plans, employers, public health authorities, life insurers, clearinghouses, billing agencies, information systems vendors, service organizations, and universities are affected by HIPAA.

Every health care provider has the responsibility to guarantee that the software being used by the provider and any related business partners, such as third party billers in processing claims, is complaint with HIPAA.

Are there penalties for non-compliance?
Yes. Violators will face criminal and civil penalties. Violators who unintentionally disclose health information will face civil fines of $100 per violation, up to $25,000 per year for each procedure violated. Violators who intentionally release health information for personal gain will face criminal sanctions punishable by up to $250,000 and 10 years in prison.

Regulatory Overview

Administrative Simplification Provisions

1. Electronic Health Transactions and Code Sets Standards:
    - Requires every provider who does business electronically to use the same health care transactions and code sets.
    - Health organizations must adopt standard code sets to be used in all health transactions example: coding systems that describe diseases, injuries, and other health problems as well as the cause, symptoms, and actions taken must be uniform.
    - Transaction and code sets requirements will give the health care industry a common language to make it easier to transmit information electronically; health claims, health plan eligibility, enrollment/disenrollment, payments for care and health plan premiums, claim status, first injury reports, coordination of benefits, and related transactions will be standardized.
    - The intention is to reduce mistakes, duplication effort and costs.

2. National Identifiers for Providers, Employers, Health Plans, and Patients:
    - Will require health care providers, health plans, and employers to have standardized national numbers that identify them on standard transactions.
    - The Employer Identification Number (EIN), issued by the Internal Revenue Service (IRS), was selected as the identifier for employers and was adopted effective July 30, 2002. The remaining identifiers are expected to be determined in the coming year.
    - Standard identifiers will reduce entities deal with each other, which is seen as confusing.

3. Security of Health Information & Electronic Signature Standards
    - Final Rule published February 20, 2003 and provides a uniform level of protection for all health information that is housed electronically and that pertains to an individual.
    - Outlines the minimum administrative, technical, and physical safeguards required to prevent unauthorized access to protected health care information.
    - Mandates safeguards for physical storage and maintenance, transmission, and access to individual health information.
    - It applies not only to the transactions adopted under HIPAA, but all individual health information that is maintained or transmitted. The Electronic Signature Standard only applies to transactions adopted under HIPAA.

4. Privacy and Confidentiality Requirements:
    - Limits the release of patient protected health information without the patient's knowledge and consent beyond that required for patient care.

Patient's personal information must be more securely guarded and more carefully handled when conducting the business of health care.

- Compliance is required beginning April 14, 2003.
- Privacy standards limit the non-consensual use and release of PHI. Gives patients new rights regarding access to their medical records and to know who has accessed it.
- Restricts most disclosures of health information to the "minimum necessary needed" for the intended purpose and establishes new requirements for access to records by researchers.
- Establishes new criminal and civil sanctions for improper use or disclosure.

5. Add information on WISP
    - Every business that collects personal information about a resident of the Commonwealth of MA must have a written information security program (WISP) similar to the federal HIPAA requirements for protected health information (PHI).
    - Under Massachusetts law, 201 CMR 17.00 residents of the Commonwealth have the right to protection of personal information (PI) which includes: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a person's financial account..
    - Information we collect is contained in the employee's human resource file or the patient's medical records. Specific examples include: social security numbers, driver license; professional license; direct deposit/banking information and Medicare/Medicaid cards.

Notices and Authorizations

Covered entities are required to provide patients with adequate notice of the patient's privacy rights and the privacy practices of the covered entity. Health care providers are required to obtain patient's written acknowledgement of these privacy rights and practices.

The Notice must include:

- Explanation of the way PHI is to be used and disclosed, including the right to receive an accounting of how an individual's PHI has been used or disclosed;
- The right of the individual to refuse treatment;
- Whether the authorization will result in financial gain for the covered entity;
- Basic statements relating to an individual's rights such an individual's right to access PHI, the right of the individual to review and copy their medical records, as well as request amendments and corrections to the records;
- The right of the covered entity to change its policies and procedures; and
- The date the notice is produced.

Procedures must be in place for the covered entity to limit the scope of the requests to the minimum amount of information needed to achieve the purpose for which the information is requested.

Covered Entities may only use or disclose protected health information without an individual's authorization:

- ❖ To carry out treatment, payment, or health care operations (including incidental disclosures such as sign in sheets at MD office)
- ❖ National activities such as research, judicial and administrative proceedings, law enforcement, emergency situations (information may be provided to next of kin, for identification of body of deceased), government health data systems, and in connection with an enforcement action or compliance review brought about by the Secretary of DHHS.

An individual's prior written authorization is required when:

- The individual's protected health information is to be used for marketing purposes by the covered entity, with the exception of a face-to-face encounter or communication involving promotional gifts of nominal value.

- For example, health plans are allowed to inform patients of additional coverage benefits and services, such as discounts for prescription eyewear.
- In response to a request by an individual to inspect and obtain a copy of his/her own protected health information
- An individual's protected health information will be used or disclosed during the course of research.
- Psychotherapy notes are requested by an individual or other covered entity.

Requirement for Authorizations Requested by Individuals
Valid authorizations must be in plain language and contain at least the following elements:

- A specific and meaningful description of the information to be used or disclosed that identifies the information;
- The name or other specific identification of the covered entity authorized to make the requested use or disclosure;
- The name or other specific identification of the party to whom the covered entity may make the requested use or disclosure;
- A description of the purpose of the requested use or disclosure;
- An expiration date for the authorization;
- A statement of the individual's right to revoke the authorization in writing at any time and a description of how the authorization may be revoked by the individual;
- A statement that the covered entity may not condition treatment, payment, enrollment, or eligibility for benefits; and
- Be signed and dated by the individual. If the authorization is signed by a personal representative of the individual, a description of the representative's (legal) authority is included.

Authorizations must be retained for 6 years. "Defective" authorizations will not be considered valid if the expiration date has passed, the form was not filled out correctly, has been revoked, or is missing any of the key elements.

Covered Entity Requirements
All covered entities are required to:

- ✓ Designate a Privacy Official
- ✓ Develop a Privacy Training Program for employees.
- ✓ Implement safeguards to protect PHI from intentional or accidental misuse.
- ✓ Provide a means for individuals to lodge complaints about the covered entity's information practices.
- ✓ Develop a system of sanctions for employees and business partners who violate the covered entity's policies or procedures.
- ✓ Maintain documentation of policies and procedures for complying with the requirements of the HIPAA standards.

Health care providers and plans must restrict the amount of information to the *minimum necessary* to achieve the purpose of the use or disclosure of PHI.

Business practices will need to be “privacy aware.” Providers and insurance companies will need to re-write contracts with business partners such as auditors, attorneys, and consultants to ensure that they adhere to privacy rules.

Compliance Deadlines:

- ✓ Compliance for the Privacy Rule is April 14th 2003. Small Health Plans have until April 14, 2004 to comply with Privacy Rule.
- ✓ For those who submitted a compliance extension plan and received a one year extension for complying with the electronic transactions and code sets standards, testing of software is required by April 16, 2003.
- ✓ The deadline for complying with the Electronics transaction and code sets for those who requested extension is October 16, 2003.

In conclusion, there are five basic principles inherent in HIPAA

1. Consumer Control now provides consumers with critical new rights to control the use and release of their personal and medical information.
2. Boundaries are now defined as to how an individual ‘s health information should be used for certain purposes only.
3. Accountability for all covered entities which defines how there will be specific federal penalties if a person’s right to privacy is violated.
4. Security safeguards will be implemented. It is the responsibility of organizations that are entrusted with health information to protect it against deliberate or inadvertent misuse or disclosure.
5. Need to balance privacy protection with public responsibility to support such national priorities as protecting public health, conducting medical research, improving the quality of care, and fighting health care fraud and abuse.

Definition of Terms:

Covered Entity	Any Health Plan, Health Care Clearinghouse, or Health Care Provider who transmits any protected health information.
Health Care Provider	A provider of services of medical or health services and any other person or organization that furnishes, bills, or is paid for health care in the normal course of business.
Health Information	Any information, oral or recorded in any form that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse, which relates to (past, present, or future) physical or mental health or condition of an individual, that is used in the provision of health care to an individual, or for past, present, or future payment for the health care provided to an individual.
Business	

Partner	Any person to whom the covered entity discloses personal health information to so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity. Business partners include: lawyers, auditors, consultants, third party administrators, data processing firms, and billing firms.
Designated Record Set	A group of records, under the control of a covered entity, from which information is retrieved using the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual, which is used to make decisions about the individual.
Disclosure	The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.
Individually Identifiable Health Information	Information that is a subset of personal health information including demographic information collected from an individual, and that, is created by or received from a health care provider, health plan, employer, or health care clearinghouse. This information relates to the past, present, or future physical or mental health or 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 identifies the individual, or there is a reasonable basis to believe that the information can be used to identify the individual.
Protected Health Information (PHI)	Individually identifiable health information that is or has been electronically transmitted or electronically maintained by a covered entity and includes such information in any other form. Electronic means computer, dial up lines, private networks, telephone voice response, fax back systems.
Use	The employment, application, utilization, examination, or analysis of information within the covered entity that holds the information.