



Department of Mental Health and Mental Retardation Office of Deaf Services

Basic HIPAA Facts

This summary presents some basic HIPAA information and is intended to assist staff in understanding their obligations under the law. It is not intended to supersede any DMH or facility policy, nor is it in any way to be construed as legal advice. Please consult relevant DMH and facility policies for further information

What HIPAA Is:

HIPAA is the Health Insurance Portability and Accountability Act of 1996. Simplified, HIPAA was established to:

- Allow portability of pre-existing condition exemption between employer health insurance group plans
- Standardize electronic transactions in health care to reduce costs through adjustments in (record formats, code sets, identifiers, eligibility, referral, claims, remittance, etc.
- Protects records of consumers from unauthorized disclosure

The General Requirements Encompass Five Specific Areas:

- **Electronic Data Interchange (EDI)** - electronic transfer of information among organizations (New date of compliance 10/16/2003)
- **Code Sets** - uniform codes for illnesses and treatments (No definite date of compliance)
- **Identifiers** - standardized numbers identifying health providers, plans, and employers (No definite date of compliance)
- **Security** - standards for protecting confidentiality, integrity, and availability of data (No definite date of compliance)
- **Privacy** - standards defining appropriate and inappropriate disclosures of individually identifiable health information and how patient rights are to be protected (**Final date of compliance 4/14/2003**)

Acronyms

HIPAA...	Health Insurance Portability and Accountability Act of 1996	BA	Business Associate
NIH.....	National Institutes of Health	EDI	Electronic Data Interchange
HHS.....	Health and Human Services	CMC	Correctional Managed Care
OCR.....	Office of Civil Rights	HIM	Health Information Management
GLB.....	Gramm-Leach-Bliley Act	HIC	Health Information Committee
OIG.....	Office of the Inspector General	SMR	Subsidiary Medical Record
SB11....	Senate Bill 11	UMR.....	Unit Medical Record
FERPA..	Family Educational Rights and Privacy Act	CMR.....	Case Management Record
CMS	Centers for Medicare and Medicaid Services	CPO.....	Chief Privacy Officer
PHI	Protected Health Information	ISO	Information Security Officer
IIHI	Individually Identifiable Health Information	PDA	Personal Digital Assistant (This includes Sidekicks and Blackberries)
TPO	Treatment, Payment, or Healthcare Operations	ROI	Release of Information

What Can and Can't Be Done With Your Personally Owned PDA

Can't Do:

- Send **ANY** information about a patient on your PDA
- Use name, initials, place of residence or other information if it would be possible to identify who you were talking about (IIHI)
- Send information about the progress of the patient, **whether an ROI is signed or not** (PHI)
-

Can Do:

- Call a code or respond to a code
- Send a request to VP or meet about an unidentified patient
- Let your supervisor know you are going to be out sick, arrive late, etc
- Arrange a meeting or call for a progress report **IF** ROI is signed.

What Can and Can't Be Done Using E-Mail

Can't Do:

- Send **any information** about a patient on your personal e-mail account (This includes **ANY** public domain service like Yahoo or Hotmail)
- **Short rule – DO NOT use private e-mail accounts for ANY information about patients**
- Sending PHI or IIHI through a non-secure network without encryption
- Send PHI or IIHI to another domain from your name@alabama.gov without encryption

Can Do:

- Send information using your name@alabama.gov to another name@alabama.gov address **IF**
 1. the other person is involved in the care of the patient and has either an ROI or a BA agreement
 2. Sending **ONLY** information needed to facilitate treatment
- Talk about the program in general without any reference to consumers.
- If the recipient has a signed ROI or BA agreement you can send **encrypted** messages

Basic Guidelines:

1. Don't send any PHI or IIHI using your personally owned PDA
2. Don't use your personal e-mail account for any work related communication
3. If you send PHI or IIHI to someone inside the Alabama.gov system, they must have permission to see the information
4. If you send PHI or IIHI to someone **outside** the Alabama.gov system, they must have permission to see the information **AND** it must be encrypted. (Greil policy says fax or snail mail only)