Office for Civil Rights
U.S. Department of Health and Human Services

HIPAA Privacy, Security and Breach Notification Rules
July 10, 2014
The Health Insurance Portability & Accountability Act of 1996

- Title I - Health Insurance Portability
- Title II - Subtitle F—Administrative Simplification
HIPAA Privacy Rule

- Final Rule published 12/28/00
- Final modifications published 8/14/02
- Compliance by 4/14/03 for most covered entities
HIPAA in HHS

- OCR (the Privacy and Security Rules):
  - Sets Policy through regulations and interpretations
  - Promotes voluntary compliance
  - Enforces through informal resolution and formal enforcement (CMPs)

- CMS (other Admin. Simp. Rules):
  - Transactions and code sets
  - Provider and plan identifiers
HIPAA Privacy Rule

- The first comprehensive federal privacy protection
- “Federal Floor”: Covered entities can provide greater protection
- More stringent state privacy protections remain in force
Key HIPAA Dates

- **April 14, 2003** – Deadline for Privacy Rule compliance for most covered entities except small health plans
- **April 14, 2004** – Privacy Rule Compliance Deadline for small health plans
- **April 20, 2005** – Security Rule Compliance Deadline for most covered entities except small health plans

45 CFR §§ 164.534 & 164.318
What is information covered?

- Protected health information (PHI) is:
  - Individually identifiable health information
  - Transmitted or maintained in any form or medium
- Held or transmitted by covered entities or their business associates

45 CFR § 160.103
Individually Identifiable Health Information (IIHI)

- Health information, including demographic information collected from an individual
- Information that relates to:
  - physical or mental health or condition of an individual;
  - the provision of health care to an individual;
  - payment for health care to an individual; and

45 CFR § 160.103
Individually Identifiable Health Information (2)

IIHI includes information:

- that identifies the individual; or
- with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

45 CFR § 160.103
Records excluded from the definition of PHI

The definition of PHI excludes PHI in:

- Educational records covered by FERPA
- Student medical records maintained by postsecondary educational institutions
- Employment records held by a covered entity in its role as an employer

45 CFR § 160.103
Standards for De-identified Information

- 18 Identifiers
  - Names
  - Geographic Subdiv.
  - Dates
  - Telephone Numbers
  - Fax Numbers
  - E-mail addresses
  - SSNs
  - Medical Record Numbers
  - Health Plan Numbers

- Account Numbers
- Certificate & License Numbers
- License Plate and Vehicle Identification Numbers
- Device & Serial Numbers
- URLs
- IP Address Numbers
- Biometric Identifiers
- Full Face or comparable photos
- Other Unique Identifiers

45 CFR § 164.514(a) & (b)
Entities Covered by HIPAA

- Health care providers who transmit health information electronically in connection with a transaction for which there is a HIPAA standard
- Health plans
- Health care clearinghouses
- Business Associates

45 CFR §§ 160.102 & 160.103
What is a Health Care Provider?

- Any person or organization who furnishes, bills or is paid for health care in the normal course of business, and

- Who transmits health information electronically in connection with a transaction for which HHS has adopted a HIPAA standard

45 CFR § 160.103
What is a Health Plan?

Any individual or group plan that provides, or pays for the cost of, medical care, including:

- Group Health Plans
- Health insurance issuers
- HMOs
- Medicare, Parts A and B
- Medicaid
- Long term care insurance

45 CFR § 160.103
What is a Health Plan? (2)

Entities that are not considered health plans include:

- Employer plans with fewer than 50 participants and which are self-administered
- Certain government funded plans
- Excepted Benefit Plans

45 CFR § 160.103
What is a Health Plan? (3)

Examples of Excepted Benefit Plans include plans that pay for the cost of:

- Accident or disability income insurance
- Liability insurance (including auto liability)
- Automobile medical payment insurance
- Workers’ compensation insurance
- Other similar insurance under which benefits for medical care are secondary or incident to other insurance benefits.

45 CFR § 160.103
Business Associates

- Agents, contractors, others who perform a function on behalf of a covered entity that requires use or disclosure of protected health information

- The Privacy Rule requires satisfactory assurance – usually a contract or other written arrangement – that a business associate will safeguard protected health information, limit use and disclosure

45 CFR §§ 160.103, 164.502(e), 164.504(e)
Business Associates after HITECH

- Direct Liability for Business Associates (§ 160.402)
- Permissible Uses and Disclosures by BAs are still largely specified in the BA Contract (§ 164.502(a)(4))
- Permits uses and disclosures for the proper management and administration or to carry out the legal responsibilities of the BA (§ 164.504 (e)(4))
Uses & Disclosures: Key Points

- NO use or disclosure of PHI unless required or permitted by the Rule

- Required disclosures are limited to:
  - Disclosures to the individual who is the subject of information as required by sections 164.524 & 164.528
  - Disclosures to Secretary of HHS to determine Privacy Rule compliance

- All other uses & disclosures in Rule are permissive
Uses & Disclosures: Key Points (2)

- The Privacy Rule prohibits both impermissible uses and impermissible disclosures.
- Disclosure = Divulging information to a person or entity outside the entity holding the information.
- Use = Sharing, utilization, examination or analysis of information within the entity that maintains the information.

45 CFR § 160.103
Permitted Uses and Disclosures

- To the Individual
- Treatment, Payment and Health Care Operations
- Incidental
- Authorized
- Where an opportunity to agree or object is required
- Public policy purposes

45 CFR § 164.502(a)(1)
A Covered Entity may use or disclose PHI to carry out essential health care functions:

- Treatment
- Payment
- Health Care Operations

45 CFR § 164.502(a)(1)(ii) & § 164.506
What is Treatment?

Treatment means the provision, coordination, or management of health care by one or more health care providers, including:

- Consultation between health care providers;
  or
- Patient referrals

45 CFR § 164.501
What constitutes Payment?

Payment means the activities of:

- Health care providers to obtain payment or be reimbursed for the provision of health care
- Health plans to obtain premiums, fulfill coverage responsibilities, or provide reimbursement for the provision of health care

45 CFR § 164.501
What are Health Care Operations?

- Health Care Operations are administrative, financial, legal and quality improvement activities.
- Necessary to run business and to support core functions of treatment and payment.

45 CFR § 164.501
Health Care Operations (2)

- Quality assessment and improvement activities
- Training, accreditation, certification, credentialing, licensing, reviewing competence, evaluating performance
- Fraud and abuse detection

45 CFR § 164.501
Opportunity for an Individual to Agree or Object – Facility Directories

- Unless the individual restricts or prohibits, a CE may include in its facility directory PHI including the individual’s:
  - Name
  - Location in the facility
  - General condition
  - Religious affiliation
- Emergency exception due to individual’s incapacity

45 CFR § 164.510(a)
Disclosures to a Patient’s Friends & Family

- Unless individual objects:
  - CE may disclose PHI to friends or family relevant to their involvement with individual’s care or payment related to individual’s health care
  - CE may notify individual’s family or personal rep of individual’s location, condition or death

- When individual is not present or incapacitated, above disclosures are permissible if, based on CE’s professional judgment, it is in the individual’s best interest

45 CFR § 164.510(b)
Public Policy Purposes

A CE may use or disclose PHI (without patient authorization or opportunity to object):

a. As required by law
b. For public health activities
c. About victims of abuse, neglect or domestic violence
d. For health oversight activities

45 CFR § 164.512
Public Policy Purposes (2)

e. For judicial and administrative proceedings

f. For law enforcement purposes

g. About decedents (to coroners & medical examiners)

h. For cadaveric organ, eye or tissue donation

45 CFR § 164.512
Public Policy Purposes (3)

i. For research purposes
j. To avert a serious threat to health & safety
k. For specialized government functions
l. For workers’ compensation purposes

45 CFR § 164.512
Incidental Uses and Disclosures

- A CE may use or disclose PHI that is “incident to” an otherwise permitted use or disclosure provided minimum necessary and safeguard standards are met.

- Privacy Rule does not require private rooms, sound proofing or encryption of telephone systems.

45 CFR § 164.502(a)(1)(iii)
Minimum Necessary

- A CE must make reasonable efforts to limit the use or disclosure of PHI to the minimum amount necessary to accomplish the intended purpose.

- Minimum necessary does not apply to certain uses and disclosures listed at 164.502(b)(2)

45 CFR § 164.502(b) and § 164.514(d)
Minimum Necessary (2)

- CE required to identify persons or classes of persons in its workforce who need access to PHI to carry out duties
- For each class of persons, CE must specify the categories of PHI to which access is needed
- CE must make “reasonable efforts” to limit workforce members’ access to specified categories of PHI

45 CFR § 164.514(d)
Uses and Disclosures
Requiring Authorization

- Authorizations are required for uses and disclosures not otherwise permitted or required by the Rule
- With some exception, a CE cannot condition treatment, payment, eligibility or enrollment on provision of an authorization

45 CFR § 164.508
Individual’s Rights

Individually have the right to:

- A written notice of privacy practices from covered entities
- Inspect and obtain a copy of their PHI
- Obtain an accounting of disclosures
- Amend their records
- Request restrictions on uses and disclosures
- Accommodation of reasonable communication requests
- Complain to the covered entity and to HHS

45 CFR § 164.520, 164.522, 164.524, 164.526, 164.528, 164.530
Notice of Privacy Practices

An individual has a right to adequate written notice of the:

- Uses and disclosures of PHI that may be made by the Covered Entity,

- Individual’s rights and the CE’s legal duties with respect to the PHI

- 45 CFR § 520(b) specifies the required elements of an NPP

45 CFR § 520
Access of Individuals to PHI

- Individual has a right to inspect and obtain a copy of PHI about the individual in a Designated Record Set for as long as it is maintained by the CE.

- Designated Record Set includes:
  - Medical & billing records of health care providers
  - Health plan enrollment, payment, claims & case/medical management systems
  - Records used to make decisions about individuals

45 CFR § 164.524 and § 164.501
Access of Individuals to PHI (2)

HIPAA Access right does not apply to:

- Psychotherapy Notes
- Information compiled for use in civil, criminal, or administrative action
- PHI subject to CLIA

45 CFR § 164.524(a)(1)
Access of Individuals to PHI (3)

- CE must respond in a timely fashion.
  - Within 30 days in most cases
  - Can take an additional 30 days if CE informs individual of the reason for delay in writing within the original 30 day time limit (e.g. Records not maintained on-site)
- CE can provide a summary of PHI in lieu of providing access so long as individual agrees.

45 CFR § 164.524(b) & (c)
Access of Individuals to PHI (4)

- CE may impose a reasonable cost-based fee for providing access
- Can only include the cost of:
  - Copying (including labor and supplies)
  - Postage
  - Preparing explanation or summary
- Cannot charge for the cost of retrieval
Amendment of PHI

An individual has the right to request that a CE amend the PHI or a record about the individual in a DRS for as long as it is maintained by the CE.

45 CFR § 164.526
Amendment of PHI (2)

A CE may deny the request if it determines that the PHI to be amended:

- Was not created by the CE (unless the patient shows that the originator of the PHI is no longer available)
- Is not part of the DRS
- Would not be available for inspection under 164.524 or
- Is accurate and complete

45 CFR § 164.526
Handling Amendment Requests

- Timely action by Covered Entity:
  - Accepting the amendment or
  - Written denial of the amendment

- Must respond to amendment request within 60 days of receiving request

45 CFR § 164.526(b)
Denials of Amendment Requests

- Individuals may submit written disagreement
- Covered Entity may rebut in writing
- CE must include request, denial, disagreement and rebuttal in Designated Record Set

45 CFR § 164.526(d)
Accounting of disclosures of PHI

- An individual has a right to receive an accounting of disclosures of PHI made by a CE in the 6 years (or less) prior to date requested.
- Many exceptions to accounting requirement as listed at 164.528 (a)(1).
- Must act on accounting request within 60 days of receiving request.
- Accounting requirement applies only to disclosures.

45 CFR § 164.528
Administrative Requirements

- Flexible & scalable
- Covered entities required to:
  a. Designate a privacy official
  b. Train its workforce on HIPAA policies & procedures
  c. Implement administrative, technical, and physical safeguards to protect the privacy of PHI

45 CFR § 164.530
d. Develop a HIPAA complaint process

e. Have and apply appropriate sanctions against workforce members who violate the entity’s policies or Privacy Rule

f. Mitigate any harmful effect of a use or disclosure of PHI that is known to the CE

g. Refrain from intimidating or retaliatory acts

45 CFR §§ 160.316 & 164.530(g)
Administrative Requirements (3)

h. Not require individuals to waive their HIPAA rights as a condition of treatment, payment, enrollment in a health plan or eligibility for benefits

i. Develop policies and procedures designed to comply with Privacy Rule standards

j. Document HIPAA policies & procedures as well as any actions or communications required by the Privacy Rule

k. Group Health Plans not subject to (a)-(f) & (i)

45 CFR § 164.530
Personal Representatives

- A person legally authorized to
  - Make health care decisions on an individual’s behalf
  - Act for a deceased individual or the individual’s estate
- Must be treated by the CE as the individual for HIPAA purposes

45 CFR § 164.502(g)
Personal Representatives (2)

Privacy Rule permits exception when a CE reasonably believes that

- Personal Representative may be abusing or neglecting the individual
- Treating the person as the personal representative could otherwise endanger the individual

45 CFR § 1264.502(g)(5)
Parents and Minor Children

- In most cases parents are personal representatives for and can exercise individual rights on behalf of their minor children.

- Privacy Rule creates exception where, under State law, parents are not the child’s personal representative.

- In such instances Privacy Rule defers to State and other law to determine rights of parents to access and control child’s PHI.
HIPAA Compliance and Enforcement

- Technical assistance for voluntary compliance
- Any person or organization can file complaints with OCR (generally within 180 days)
- OCR may investigate complaints and may conduct compliance reviews
- OCR shall attempt to resolve noncompliance by informal means

45 CFR §§ 160.304, 160.306 & 160.308
Civil Money Penalty Amounts

<table>
<thead>
<tr>
<th>Penalty Amount</th>
<th>For violations occurring prior to 2/18/2009</th>
<th>For violations occurring on or after 2/18/2009</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Up to $100 per violation</td>
<td>$100 to $50,000 or more per violation</td>
</tr>
<tr>
<td>Calendar Year Cap</td>
<td>$25,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

• OCR may reduce a penalty if the failure to comply was due to reasonable cause and not willful neglect, and the penalty would be excessive relative to the noncompliance.
Criminal Penalties for Willful Disclosures

- For knowingly obtaining or disclosing identifiable health information relating to an individual in violation of the Rule:
  - Up to $50,000 & 1 year imprisonment
  - Up to $100,000 & 5 years if done under false pretenses
  - Up to $250,000 & 10 years if intent to sell, transfer, or use for commercial advantage, personal gain or malicious harm

- Enforced by DOJ

42 USC § 1320d-6
HIPAA Security Rule

- 45 CFR Part 160 & Part 164, Subpart “c”
  - Administrative Simplification Subpart
  - Definitions in 45 CFR 160.103 apply to Security Rule
    - Examples--covered entity, protected health information, business associate

- Regulatory history

- Compliance date:
  - No later than April 20, 2005 for all covered entities except small health plans
  - No later than April 20, 2006 for small health plans
Security Standards: General Rules

- Applies to **Electronic Protected Health Information (e-PHI)**
- That a Covered Entity
  - Creates
  - Receives
  - Maintains
  - Transmits

45 CFR 164.306(a)
The Guiding Principles of Security

- Ensure e-PHI is used, stored, transmitted or received with:
  - **Confidentiality**
    - only the right people see it
  - **Integrity**
    - the information is what it is supposed to be – no unauthorized alteration or destruction
  - **Availability**
    - the right people can see the e-PHI when needed

45 CFR 164.306(a)
Rule Requires CE’s to Safeguard e-PHI

- Protect e-PHI against reasonably anticipated threats or hazards to the security or integrity of information
- Protect against reasonably anticipated uses and disclosures not permitted by the Privacy Rule or Security Rule
- Create and put into place policies and procedures to ensure compliance by workforce

45 CFR 164.306(a)
A Flexibility of Approach

- Rule permits scalability and flexibility
- A CE’s choice of security measures to implement standards and specifications can take into account:
  - Size
  - Complexity
  - Capabilities
  - Technical Infrastructure
  - Cost of security measures
  - Potential security risks

45 CFR 164.306(b)
What are the Standards?

- 164.306: Security Standards: General Rules
- 164.308: Administrative Safeguards
- 164.310: Physical Safeguards
- 164.312: Technical Safeguards
Administrative Safeguards

- Administrative Safeguards
  - “...are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information.”

45 CFR §§ 164.304 & 164.308
Administrative Safeguards

- **164.308(a)(1)(i) Security Management Process:** Implement policies and procedures to prevent, detect, contain, and correct security violations.
Administrative Safeguards

- **164.308(a)(2) Assigned Security Responsibility (R):** Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
Administrative Safeguards

164.308(a)(4)(i) Information Access Management: Implement policies and procedures for authorizing access to electronic PHI that are consistent with the applicable requirements of the Privacy Rule.
Administrative Safeguards

- 164.308(a)(5)(i) Security Awareness and Training: Implement a security awareness and training program for all workforce members (including management)
Physical Safeguards

Physical Safeguards are “physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.”

45 CFR §164.304
Physical Safeguards

- **164.310(a)(1) Facility Access Controls:**
  Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
Physical Safeguards

- **164.310(b) Workstation Use (R):** Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access e-PHI.
Physical Safeguards

- 164.310(c) Workstation Security (R): Implement physical safeguards for all workstations that access e-PHI, to restrict access to authorized users
Technical Safeguards

- **164.312(a)(1) Access Control**: Implement technical policies and procedures for electronic information systems that maintain e-PHI to allow access only to those persons or software programs that have been granted access rights in... [Information Access Management]
Technical Safeguards

- **164.312(b) Audit Controls (R):** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use e-PHI
164.312(c)(1) Integrity: Implement policies and procedures to protect e-PHI from improper alteration or destruction
Technical Safeguards

164.312(e)(1) Transmission Security: Implement technical security measures to guard against unauthorized access to e-PHI that is being transmitted over an electronic communications network
HIPAA Security Rule Enforcement

- Delegation of Authority – July 27, 2009
- OCR, rather than CMS, now enforces the Security Rule
Issues in Security Enforcement Actions
(April 20, 2005 to December 31, 2009)

The compliance issues investigated most frequently, in order, are:

- Information access management
- Access controls
- Security awareness and training
Case Example – Security Rule

- Electronic storage media containing e-PHI for 2 million individuals were stolen from a vehicle used by a hospital’s off-site storage vendor.
- HHS compliance review evaluated CE’s overall Security Rule risk management process.
- HHS required the hospital to put into place corrective action plan to appropriately protect e-PHI
  - Encryption of e-PHI placed on storage media
  - Contractor requirements to transport and store backup tapes
  - Security Awareness training policies
  - Periodic review and updates of policies and procedures
Breach Notification Rule -- Subpart D

- 164.400 – Applicability
- 164.402 – Definitions
- 164.404 – Notification to individuals
- 164.406 – Notification to media
- 164.408 – Notification to Secretary/OCR
- 164.410 – Notification by business associates
- 164.412 – Law enforcement delay
- 164.414 – Administrative requirements and burden of proof
Brief Summary

- Covered entities must:
  - notify each affected individual of breach of “unsecured protected health information.”
  - Notice to media if more than 500 people in single area affected.
  - Notice to Secretary of breach through OCR website.
  - Most notifications must be provided without unreasonable delay (but no later than 60 days) of discovery of breach.

- Business associate must notify covered entity of breach and identify individuals affected.

What is a “breach”

- An impermissible acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI.

- To compromise the security or privacy means to pose a *significant risk* of financial, reputational, or other harm to the individual.

- Uses or disclosures of limited data sets in which all dates of birth and zip codes have also been removed are not considered to compromise the security or privacy of PHI.

45 C.F.R. §164.402
What is a “Significant Risk” of Harm

- Determined by the covered entity through a risk assessment once it learns of a possible breach.

- In determining the level of risk, the covered entity should make a fact-based evaluation of factors such as the recipient of the PHI, the nature of PHI itself, any mitigation that can be taken to lessen potential harm, and the likelihood the PHI can readily identify an individual.

45 C.F.R. § 164.402
Significant Risk of Harm-Examples

- Covered entity mistakenly discloses PHI to the wrong pharmacy. Since the pharmacy is also a covered entity and obligated to comply with the Security and Privacy Rules, this may not pose a significant risk of harm to the individual.

- Covered entity loses an unencrypted laptop containing PHI. However, it is recovered the next day and a forensic analysis reveals that the information contained was not opened, altered, transferred, or otherwise compromised. This may not pose a significant risk of harm to the individual.

45 C.F.R. § 164.402
Notification obligation only applies to “Unsecured PHI”

- Unsecured PHI is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals per guidance issued by the Secretary and available on the OCR website (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html).

- Acceptable methods of securing PHI are encryption and destruction.

- Loss or compromise of PHI that has been encrypted or destroyed pursuant to the guidance does not trigger the duty to provide breach notification.
Notification to Individuals-164.404

Following the discovery of a breach of unsecured PHI, a covered entity must notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of the breach.

45 C.F.R. §164.404(a)(1)
Timeliness of Individual Notification

- Breach notification must be provided to the individual without unreasonable delay and in no case later than **60 calendar days** after discovery of the breach.

- 60 days is an outer limit, if the covered entity has completed its risk assessment and confirmed the breach within 20 days, it should send the notifications immediately instead of waiting until day 60.

45 C.F.R. §164.404(b)
Content of Notification

The notification must contain, to the extent possible, the following:

- A description of what happened and dates, if known
- A description of the types of unsecured PHI involved in the breach
- Any steps individuals should take to protect themselves
- A description of what the covered entity is doing to investigate and mitigate harm
- Contact information for individuals to learn more which must include a toll-free telephone number, e-mail address, website, or postal address

The notification must be written in plain language.

45 C.F.R. §164.404(c)
Notification to the Media

- For a breach involving more than 500 residents of a State or jurisdiction, the covered entity must notify prominent media outlets serving that State or jurisdiction in addition to written notice to individuals.
- Must be done without unreasonable delay, no later than 60 days after discovery of breach.
- Content of the notification to media is the same as that which must be provided to individuals.

45 C.F.R. §164.406
Examples of Notification to Media

- If a laptop that contains unsecured PHI of more than 500 residents of a particular city is stolen, the covered entity must notify a major television station or daily newspaper serving that city or entire State.

- If the stolen laptop contained the unsecured PHI of 200 residents from State A, 200 residents of State B, and 200 residents of State C, no reporting to the media would be required since there were not 500 or more residents affected from any one State.

45 C.F.R. §164.406
Notification to the Secretary

- For breaches affecting 500 or more individuals, the covered entity must report the breach to the Secretary without unreasonable delay and not later than 60 days after discovery of the breach.

- For breaches affecting fewer than 500 individuals, the covered entity may report the breach to the Secretary annually.

- Reporting by covered entities will be done via OCR’s website.

- This data is collected for reporting to Congress and notification to the Regions.

45 C.F.R. §164.408
Business Associates

- Business associates must notify covered entities of breaches without unreasonable delay and in no case later than 60 days.

The content of the notification from the BA to the CE must include, to the extent possible, the identification of the affected individuals and any other information that is known to the BA that the CE is required to include in its notice to the individual.

45 C.F.R. §164.410
OCR Website

For more information see:
www.hhs.gov/ocr/hipaa
Contact Information

Valerie Montoya
Equal Opportunity Specialist
1301 Young Street, Suite 1169
Dallas, TX 75202
Direct 214-767-1717
Fax 214-767-0432
Email Valerie.Montoya@hhs.gov