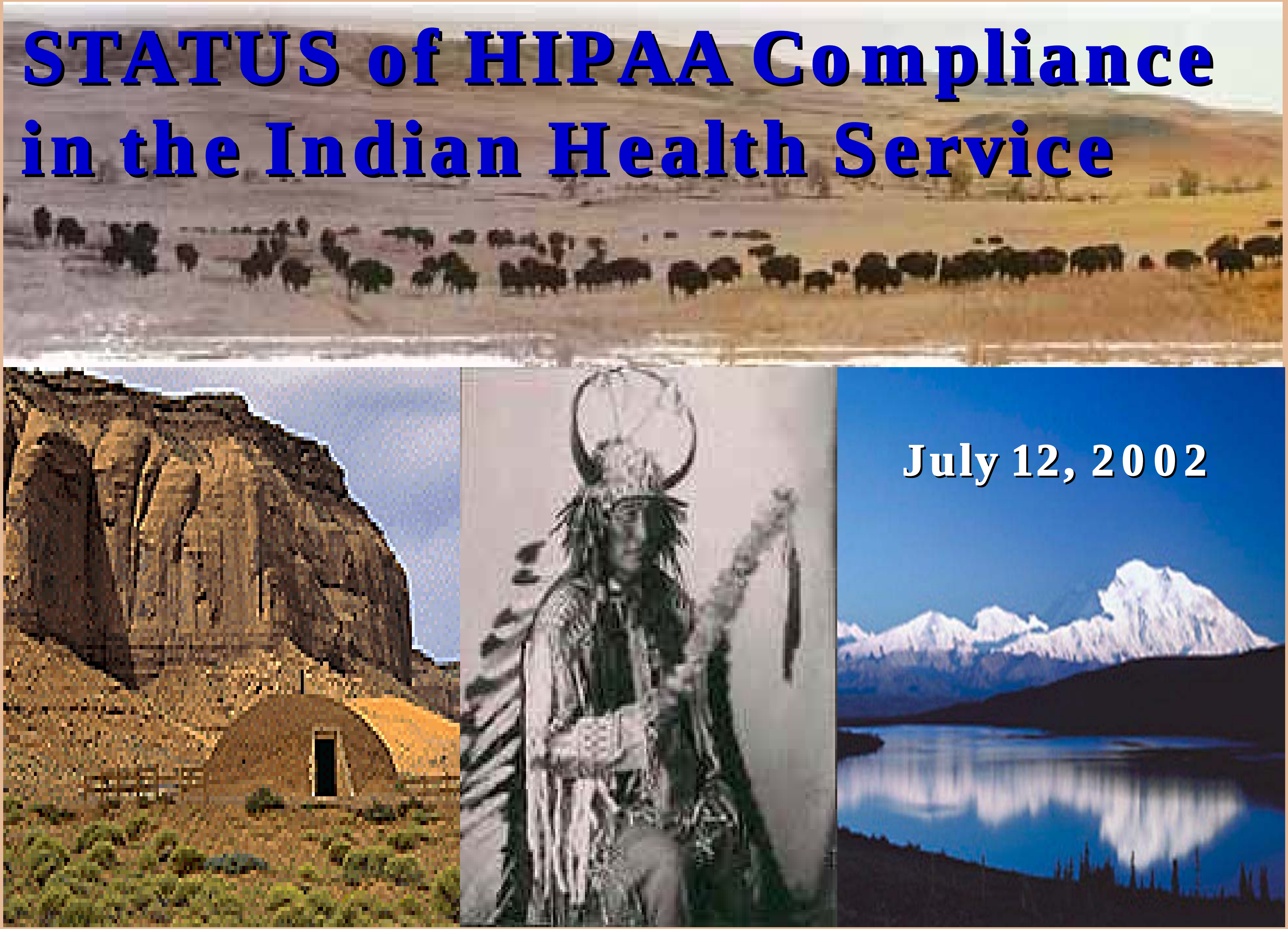
STATUS of HIPAA Compliance in the Indian Health Service



July 12, 2002

Briefing Objectives

- Provide an overview of HIPAA
- Outline current status of HIPAA compliance activities
- Discuss key upcoming tasks to becoming HIPAA compliant

Questions Asked

- What is HIPAA?
- Do we have to comply with it?
- What happens if we do not?
- What systems does it effect?
- What resources will be needed?
- Why do it?
- Funding available?

Why Was HIPAA Enacted?

- Assure portability of health insurance
- Decrease healthcare fraud and abuse
- Improve efficiency and effectiveness of health care
- Enforce standards
- Guarantee security and privacy of Protected Health Information
- Offers more rights to patients on the use of their health information

HIPAA – More Than Meets the Eye

What We're Learning

- Laws / Regulations overlap with HIPAA
- Legal Reviews needed on all aspects
- Development of "Forms & Policy" is complex (need for legal language and need for grade school readability)
- Nothing available "Off-the-Shelf"

What We're Learning—cont'd

- Penalties for non-compliance
- Touches on almost every aspect of providing health care
- HIPAA Law applies to EVERYONE! Federal and Private Health Care Industry

What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996
  - Portability
  - Accountability
  - Administrative Simplification

What are the important elements of HIPAA that require compliance?

- Standard electronic transaction formats
- Standard code sets
- Security
- Privacy

There's Something for Everyone

HIPAA Regulations

- Healthcare Providers
- Healthcare Payers
- Healthcare Clearinghouses

Employees

Vendors

Business Associates

Physicians

3rd Party Consultants

Attorneys

Headquarters

Areas

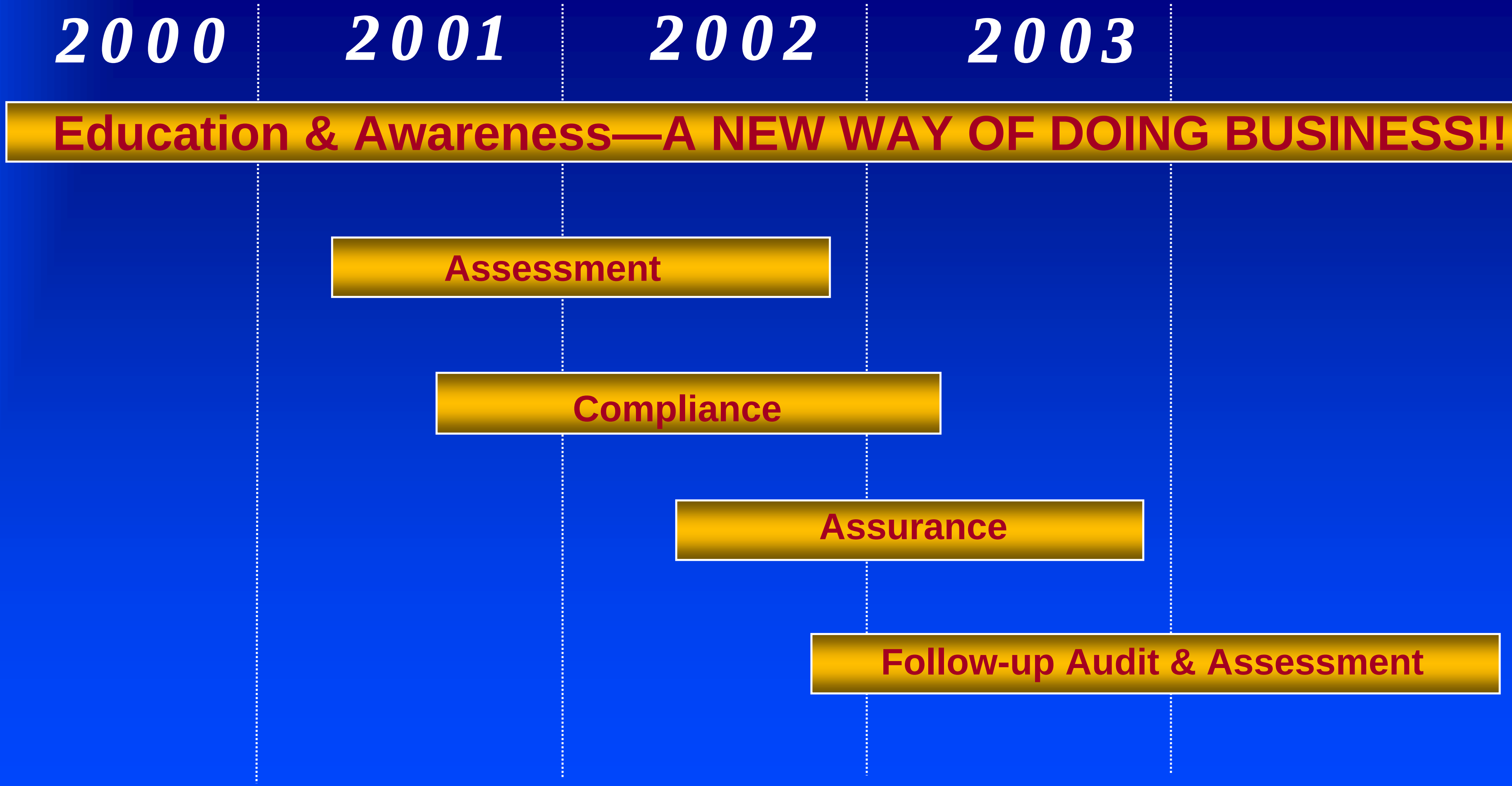
I/T/U Sites

Principles for Achieving HIPAA Compliance

- Senior management involvement! Senior manager assigned with HIPAA responsibility
- Interdisciplinary team approach
- Nationwide HIPAA awareness
- Build upon existing organization strengths! Use common sense strategies
- National compliance plan

INDIAN HEALTH SERVICE • DHHS • PHS

What are the key steps to be taken to achieve compliance with HIPAA?



2000 2001 2002 2003

Education & Awareness—A NEW WAY OF DOING BUSINESS!!

Assessment

Compliance

Assurance

Follow-up Audit & Assessment

Focus Groups for Achieving HIPAA Compliance in the IHS

- Transactions & Code Sets
- Security
- Privacy

More questions about HIPAA

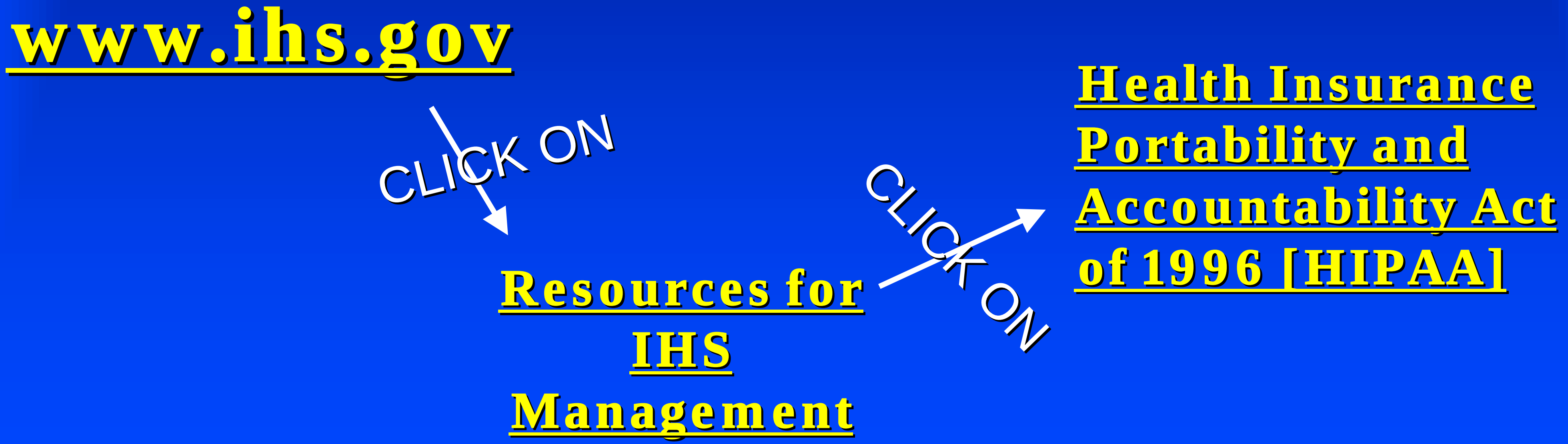
- How will the HIPAA regulations be enforced?

HHS Office of Civil Rights has been charged with enforcement.

Accrediting organizations are planning to include HIPAA requirements in their accreditation process.

IHS HIPAA WEB SITE

- **Where can I get information about HIPAA and what IHS is doing to become compliant?**



www.ihs.gov

CLICK ON

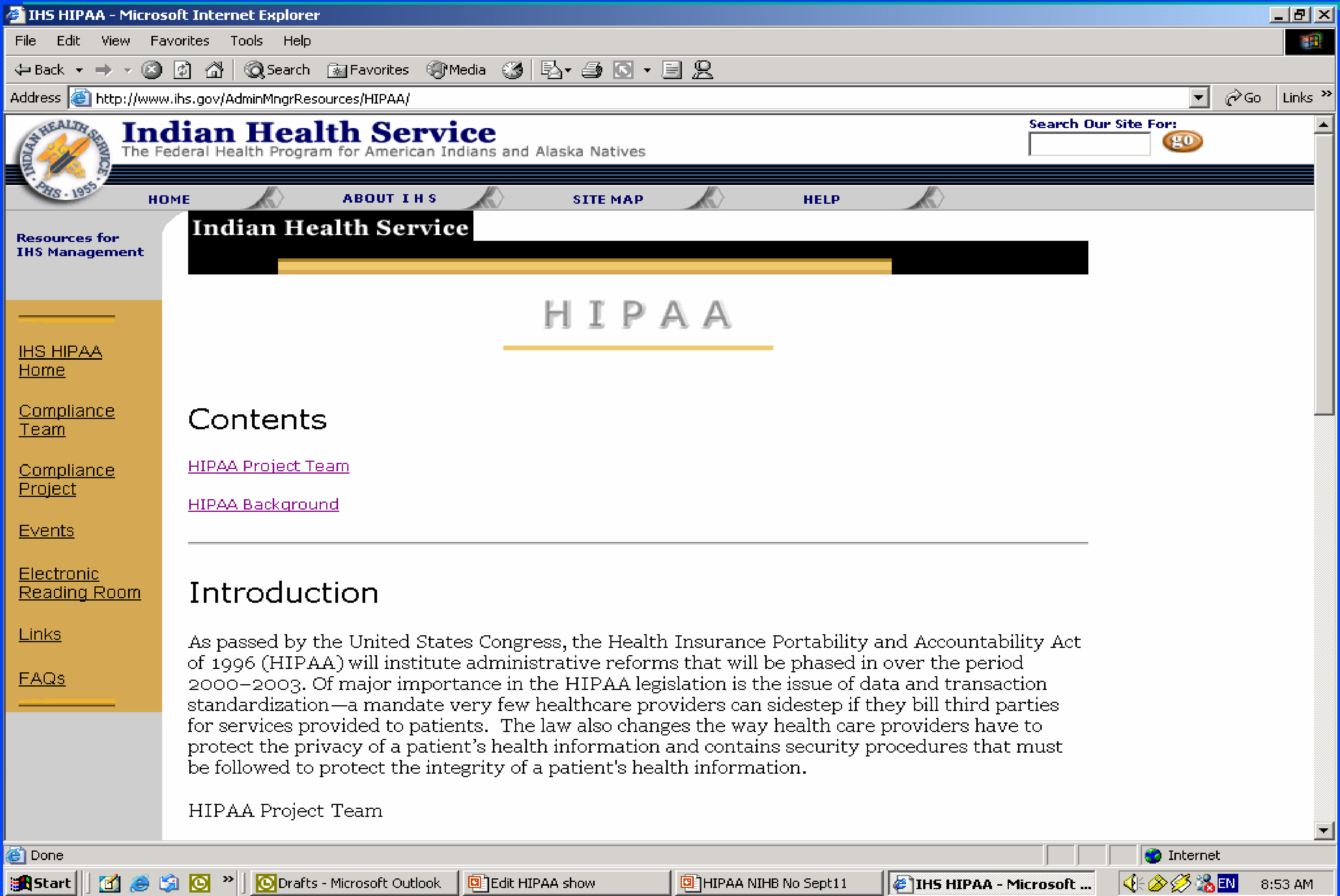
Resources for IHS Management

CLICK ON

Health Insurance Portability and Accountability Act of 1996 [HIPAA]

Where can I learn more?

WWW.IHS.GOV



IHS HIPAA - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.ihs.gov/AdminMngrResources/HIPAA/
Go Links
Search Our Site For:
go
HOME
ABOUT IHS
SITE MAP
HELP
Done
Internet
Start
Drafts - Microsoft Outlook
Edit HIPAA show
HIPAA NIHB No Sept11
IHS HIPAA - Microsoft ...
EN
8:53 AM

Indian Health Service
The Federal Health Program for American Indians and Alaska Natives

Resources for IHS Management

- IHS HIPAA Home
- Compliance Team
- Compliance Project
- Events
- Electronic Reading Room
- Links
- FAQs

Indian Health Service

HIPAA

Contents

HIPAA Project Team

HIPAA Background

Introduction

As passed by the United States Congress, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) will institute administrative reforms that will be phased in over the period 2000–2003. Of major importance in the HIPAA legislation is the issue of data and transaction standardization—a mandate very few healthcare providers can sidestep if they bill third parties for services provided to patients. The law also changes the way health care providers have to protect the privacy of a patient's health information and contains security procedures that must be followed to protect the integrity of a patient's health information.

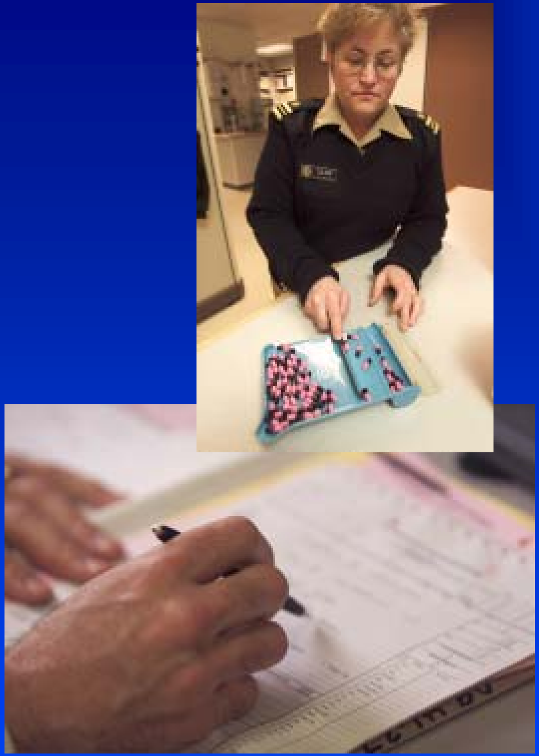
HIPAA Project Team

Current Status and Next Steps

- What does the HIPAA rule require?
- What is our current status?
  - Do existing practices comply?
  - Are current policies adequate?
- What do we need to do?
  - What new practices or procedures are required?
  - What new or updated policies are required?
- What is the impact of each?

Transaction Standards

- Designed to improve the efficiency and effectiveness of health care systems
- Improves overall data quality
- Standards became effective on October 16, 2000
- Can request a 1 year extension of compliance date to October 16, 2003



Current Status for Transaction Standards

- Converting current transactions for professional and institutional claims
- Adopted ANSI ASC X12N (version 4010) for professional and institutional claims

Current Status for Transaction Standards Applicable to IHS

- Eligibility Inquiry (270) is compliant
- Eligibility Response (271) is being tested
- Health Care Claim (837) and Payment Advice (835) are being developed
- NCPDP 5.0 being converted to 5.1

Code Sets Adopted

Diagnoses Codes—Use

- ICD-9 CM

Procedures Codes—Use

- ICD-9 CM
- CMS Common Procedure Coding System (HCPCS)
- AMA Current Procedural Terminology (CPT-4)
- American Dental Association Codes
- National Drug Codes (NDC)/ J Codes

Meeting Transaction Standard

- Use transaction software that is X12 compliant
- Use a clearinghouse that is HIPAA compliant

Meeting Transaction Standard, cont'd

- IHS will keep with the original schedule; RPMS Transactions will be HIPAA compliant by October 16, 2002
- THIS IS JUST GOOD BUSINESS PRACTICE

Security Standards

- Guaranteeing confidentiality and integrity of protected health information
- Final Rule expected in 2002
- Compliance date will be two years from effective date

Security Standards Major Categories

- Administrative procedures
- Physical safeguards
- Technical security services
- Technical security mechanisms

Current Status – Working on the following Security/Administrative Procedures

- Policies/Procedures
- Certification of Compliance
- Chain of Trust Partner Agreement
- Contingency Plan
- Record processing
- Internal Audit
- Personnel Security/Training/Termination Procedures
- Configuration Management
- Incident Process
- Management Process

Security—Current Programs

Government Organizations must Comply with the Following:

- Government Information Systems Reform Act (GISRA)
- OMB Circulars on security
- JCAHO Accreditation Standards
- When in compliance with GISRA, OMB and JCAHO all but one HIPAA requirement is met
  - We must establish security audit controls

Privacy Standards

- Provisions to protect patients' individual rights to privacy
- Final rules were effective on April 14, 2001
- Compliance date is April 14, 2003

Privacy– Some Requirements of Covered Entities (IHS)

Notices

Notice of Privacy Practices—explaining patient's rights and IHS' legal responsibilities

Minimum Necessary

Intent is to limit protected health information to the minimum necessary to accomplish the intended purpose.

Privacy– Some Requirements of Covered Entities (IHS) cont'd

Consent

Patient's consent prior to using or disclosing protected health information

Authorizations

Patient's authorization to use or disclose protected health information for purposes other than treatment, payment, and health care operations

Privacy – Some Requirements of Covered Entities (IHS) cont’d

Business Associates

Business associates agreements are to be compliant with HIPAA regulations

Privacy Official

IHS must designate privacy officials responsible for establishing policies related to HIPAA privacy regulations

Privacy—Rights of Individuals

Notices

to be informed of the uses and disclosures of their protected health information

Access

to inspect and obtain a copy of their protected health information

Alternate Means of Communication

to request an alternate means of communication regarding their health information

Privacy—Rights of Individuals cont’d

Amendments

to request amendments or corrections to their protected health information

Accounting of Disclosures

to receive an accounting of all disclosures

Right to Restrictions

to request that uses and disclosures of protected health information be restricted

HHS PROPOSES CHANGES TO THE HIPAA PRIVACY RULE

The proposed changes will protect privacy and access to care while removing obstacles to care.

The proposal would make the following revisions:

1. Consent and Notice
2. Minimum Necessary and Oral Communications
3. Business Associates
4. Marketing

5. Parents and Minors

6. Uses and Disclosures for Research Purposes

7. Requests for Comments on an Alternative Approach to De-Identification

8. Uses and Disclosures for which Authorizations are Required

Other Provisions also Proposed

9. **Sale of Business --** The proposal would clarify that the rule permits disclosures in certain circumstances for the sale of a covered entity's business.

10. **Sale of Business --** The proposal would clarify that the rule permits disclosures in certain circumstances for the sale of a covered entity's business.

11. **Accounting of Disclosures of Protected Health Information --** The proposal would not require the covered entity to account for disclosures for which the individual provided written authorization.

12. **Disclosures for Treatment, Payment, or Health Care Operations of Another Entity --** The proposal would clarify that covered entities can disclose protected health information for the treatment, payment and certain health care activities of another covered entity or health care provider.

13. **Uses and Disclosures Regarding FDA-Regulated Products and Activities --** The proposal would assure that the rule permits covered entities to continue to disclose information to non- government entities subject to FDA jurisdiction about the quality, safety, and effectiveness of FDA-regulated products and activities.

13. **Uses and Disclosures Regarding FDA-Regulated Products and Activities** -- The proposal would assure that the rule permits covered entities to continue to disclose information to non- government entities subject to FDA jurisdiction about the quality, safety, and effectiveness of FDA-regulated products and activities.

14. **Hybrid Entity** -- The proposal would permit any entity that performs covered and non-covered functions to elect to use the hybrid entity provisions and would provide the entity additional discretion in designating its health care component. The proposal would clarify that protected health information does not include employment records.

PRIVACY

UPDATED 07/12/02

Task	Headquarters	Who	Status Comp Date	Area	Who	Status Comp Date	Facility	Who	Status Comp Date
Determine what needs to be done to comply with HIPAA Privacy Standards.	Compare Privacy Act to HIPAA privacy standards and determine what needs to be done to comply with HIPAA.	Privacy Officer Health Records.	Completed – IHS HIPAA Website	**NA**			**NA**		
Make needed changes to Privacy Policy.	Rewrite Privacy Policy so that it is HIPAA compliant.	Privacy Officer	Completed – Legal Review	Rewrite Area Privacy Policy so that it is HIPAA compliant.			**Rewrite facility Privacy Policy so that it is HIPAA compliant.**		
Develop procedures for updated Privacy Policy.	Rewrite privacy procedures so that they follow the new policy.	Privacy Officer	Completed – Draft stage/Legal Review	Rewrite Area privacy procedures so that they follow the new policy.			**Rewrite facility privacy procedures so that they follow the new policy.**		
Revise forms effected by the updated Privacy Policy.	Update forms so they are HIPAA compliant: Consent Form Authorization Form Correction/Amendment for PHI Notice of Privacy Practices <u>See expanded list for all forms.</u>	Privacy Officer Health Records	Completed* Completed* Completed* Pending- *Under Legal Review	Update forms so they are HIPAA compliant: Consent Form Authorization Form Correction/Amendment for PHI Notice of Privacy Practices			**Update forms so they are HIPAA compliant: Consent Form Authorization Form Correction/Amendment for PHI Notice of Privacy Practices.**		
Update contracts to be HIPAA compliant.	Develop Business Associate Agreements (BAA) for HIPAA compliance.	Contracts Office		Develop BAA for HIPAA compliance.			**Develop BAA for HIPAA compliance.**		
Identify contracts that need a BAA clause	Place BAA into all identified contracts.	All Offices		Place BAA into all identified contracts.	All Offices		Place BAA into all identified contracts.	All Offices	
Update Privacy training materials	Develop new Privacy Training materials that are HIPAA compliant.	HIPAA Team	Under development	Develop new Privacy training Materials that are HIPAA compliant.			**NA**		
Train Staff in new privacy procedures	Use newly developed training materials to train staff on privacy standard, policies and procedures.	HIPAA Team		Use newly developed training materials to train staff on privacy standards.			**Use newly developed training materials to train staff on privacy standards.**		

SECURITY UPDATED 07/12/02

Task	Headquarters	Who	Status/ Comp Date	Area	Who	Status/ Comp Date	Facility	Who	Status/ Comp. Date
Trading Partner Security									
Develop needed agreement language for electronic sharing of PHI.	Develop: Chain of Trust Partner Agreements (COT) Trading Partner Agreements (TPA)	Bus. Office Acquisitions Legal		**NA**			**NA**		
Identify business partners where COT and TPA agreements are needed.	Incorporate COT and TPA in contracts and grants that are identified as requiring them.	Acquisitions		Incorporate COT and TPA in contracts and grants that are identified as requiring them.	Acquisitions		Incorporate COT and TPA in contracts and grants that are identified as requiring them.	Acquisitions	
Computer Security									
Identify Risk	Perform a risk analysis of IHSNET, RPMS, NPRS and WEB to identify security risk.	ITSC	In Process	Perform a risk analysis of critical IT systems in the Area	IT Office		Work with the Area Office on the Risk Analysis of the Area IT system.	IT Staff	
Reduce Risk	Based on the Risk analysis, perform needed upgrades to meet HIPAA standards.	ITSC	In Process	Based on the Risk analysis, perform needed upgrades to meet HIPAA standards	IT Office		Based on the Risk analysis, perform needed upgrades to meet HIPAA standards	IT Staff	

SECURITY UPDATED 07/12/02

Task	Headquarters	Who	Status/ Comp Date	Area	Who	Status/ Comp Date	Facility	Who	Status/ Comp Date
Personnel Security									
Policy Development	Establish a national policy for security checks of personnel that is HIPAA compliant.	PIES	02/30/02	Establish an Area Personnel Security Policy based on the National Policy.			Establish a Facility Personnel Security Policy based on the Area Policy.		
Develop procedures for personnel security.	Develop personnel security procedures based on the Personnel Security Policy.	PIES	06/30/02	Develop personnel security procedures based on the Personnel Security Policy.			Develop personnel security procedures based on the Personnel Security Policy.		
Physical Security									
Develop a policy.	Establish a physical security policy for computer equipment.	ITSC	In Process	Establish a physical security policy for computer equipment.			Establish a physical security policy for computer equipment.		
Develop procedures based on policy	Establish IT physical security procedures based on the newly developed policy.	ITSC	In Process	Establish IT physical security procedures based on the newly developed policy.			Establish IT physical security procedures based on the newly developed policy.		
Develop a building security policy.	Establish a building security policy that incorporates HIPAA requirements.	OMS		Establish a building security policy that incorporates HIPAA requirements.			Establish a building security policy that incorporates HIPAA requirements.		
Develop Building Security procedures	Establish building security procedures based on the new newly developed policy.	OMS		Establish building security procedures based on the new newly developed policy.			Establish building security procedures based on the new newly developed policy.		

TRANSACTIONS and CODE SETS

UPDATED 07/12/02

Task	Headquarters	Who	Status/ CompDate	Area	Who	Status/ Comp Date	Facility	Who	Status/ Comp. Date
Write forms in HIPAA compliant language using HIPAA compliant codes.	Format all forms in X.12 format with correct codes. 270/271 835/837 NCPDP 5.1 276/277	ITSC	Done 9/01 Done 6/02 Done 6/02	NA			NA		
Distribute HIPAA compliant software to I/T/U.	Announce availability of HIPAA Compliant software available to the field.	ITSC	Projected to be in August 2002.	Install HIPAA compliant forms on Area and Service Unit Servers.	ISO		Assure HIPAA compliant forms are installed at the facility.	IT Systems Manager	
Inform staff of software installation and provide any needed T/A on their use.	NA			Inform and train appropriate staff in the use of the HIPAA compliant forms.	ISO		Inform and train business office and clinical staff in the use of the HIPAA compliant forms.	IT Systems Manager	
Check with third party payers and CHS providers and determine which will be HIPAA compliant by October 2002.	Develop list of third party payers that the National program exchanges PHI with and note those who will be HIPAA compliant.	Buss. Off. CHS Off.	Area Survey sent out 06/25/02	Develop list of third party payers and CHS providers that the Area Office either bills or pays for services and note those who will be HIPAA compliant.	Buss. Off. CHS Off.	Responding to 6/25/02 survey.	Develop list of third party payers and CHS providers that the facility either bills or pays for services directly and note those who will be HIPAA compliant.	Buss. Off. CHS Off.	

Task	Headquarters	Who	Status/ Comp Date	Area	Who	Status/ Comp Date	Facility	Who	Status/ Comp Date
Develop a sample EDI letter of agreement for use with third party payers and contract providers who exchange HIPAA transactions	Develop the sample letter and share it with the Area Offices.	Buss. Off. CHS Off.		**NA**			**NA**		
Obtained signed EDI Letters of Agreement from third party payers and CHS providers that are going to be HIPAA compliant.	Negotiate EDI letters of agreement with payers at the National level that are going to be HIPAA compliant.	Buss. Off. CHS Off.		Based on the sample letter from HQ negotiate EDI letters of agreement with payers and providers at the Area level that are going to be HIPAA compliant.	Buss. Off. CHS Off.		Based on the sample letter from HQ negotiate EDI letters of agreement with payers and providers at the facility level that are going to be HIPAA compliant.	Buss. Off. CHS Off.	

DRAFT
INTERNAL HIPAA ASSESSMENT

DRAFT INTERNAL ASSESSMENT

Indian Health Service
Health Insurance Portability & Accountability Act (HIPAA) DRAFT 6/28/02

Internal Assessment

Name of Facility:	**Yes**	**No**	**N/A**
1. Does your facility have a group or individual responsible for HIPAA compliance?			
2. Has your facility completed an assessment for HIPAA compliance in the following areas?			
Privacy Standards?			
Security Standards (Final Rule pending)?			
Transactions and Code Sets (TCS)?			
3. Has your facility determined resources required to comply with HIPAA standards? (Training funds, IT security devices, coding and billing software, etc.)			
4. Has your facility developed an action plan as a result of conducting an assessment?			

	Yes	No	N/A
5. Is your action plan consistent with Information System and program planning?			
6. Have you developed a step-by-step implementation work plan?			
7. Has your facility identified all business associates? (e.g. transcription services, reference lab, tribal health programs, etc.)			
8. Has your facility included HIPAA provisions in its contracts with business associates?			
Health Information Management (Health Records)			
1. Is your facility able to identify which information is protected health information (PHI)?			
2. Does your facility have policies & procedures to coordinate patient care with tribal health programs?			
Consent			
1. Does your facility have policies and procedures for obtaining individual consent before using or disclosing protected health information for treatment, payment, or other healthcare operations?			
2. Does your facility have policies and procedures for using and disclosing only the **minimum amount** of protected information **necessary** to accomplish the purpose of the use or disclosure?			
3. Does your facility have policies and procedures for using and disclosing protected health information at the authorized request of the individual?			

Does your policy address the following:	**Yes**	**No**	**N/A**
4. Does your facility have policies and procedures for allowing the use and disclosure of protected health information without patient consent or authorization for the following?			
Judicial administrative release (e.g. subpoena/court order)			
Health oversight release (e.g. Tribal Health Authority, accreditation organization, etc.)			
Research release			
Law enforcement release			
Public health activities (Tribal, Federal, State, County Public Health)			
To coroners and medical examiners for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law, and to funeral directors as necessary to carry out their duties with respect to the decedent			
Other disclosures as required by law (e.g. communicable diseases)			
Disclosures about victims of abuse, neglect, or domestic violence as required by law			
Disclosures to organ procurement facilities or other entities engaged in the procurement, banking, or transplantation of organs for the purpose of facilitating organ donation and transplantation			
Disclosures to workers' compensation or other similar programs, as required by law			
Disclosures to workers' compensation or other similar programs, as required by law			

Does your policy address the following:	Yes	No	N/A
Policies and procedures are in place for verifying the identity and authority of a person requesting protected health information, when the request is from a person who is not known to your facility?			
Policies and procedures are in place for allowing the individual an opportunity to agree, prohibit, or restrict the disclosure of protected health information for the following?			
For the release of limited PHI for a facility directory.			
To a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's healthcare.			
To notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death.			
Has your facility developed policies and procedures for using or disclosing protected health information of decedents?			
Does your facility have policies and procedures for disclosing PHI to representatives of the individual who is the subject of the information?			
Does your facility have policies and procedures for obtaining the proper authorization for using or disclosing protected health information for marketing practices, if applicable (Tribal Programs)?			
Have you established a Master Personal (Patient) Index (MPI) (or have it completed/current)? (duplicates, name changes, deaths, etc.)			
Is your facility active in improving and monitoring the accuracy of all data entered in the patient registration system?			
Are ongoing data integrity checks in place? (e.g. RPMS error reports)			

Does your policy address the following:	**Yes**	**No**	**N/A**
Is the charge description master (CDM) (superbill) kept up to date (if applicable)?			
Has your facility conducted **risk assessments** on **security?**			
Has your facility conducted a comprehensive analysis of current procedures in coding and billing?			
Has your facility made available HIPAA training and continuing education to the staff?			
Rights of Individuals			
1. Does your facility have policies and procedures for allowing patients to request to revoke authorization to use or disclose protected health information at any time.			
2. Does your facility have policies and procedures for allowing patients to request and receive communications of protected health information from the facility by alternative means or at alternative locations.			

Does your policy address the following:	Yes	No	N/A
Security Standards			
Administrative Procedures			
1. Have you done a risk analysis of your security and implemented security plans based on the analysis?			
2. Do you have Chain of Trust agreements with all business partners with which your program exchanges PHI?			
3. Is there a contingency plan in the event that your computer system is lost and does the plan include a data backup plan?			
4. Is there a formal (written) mechanism for routine and non-routine receipt, management, storage, dissemination, transmission and/or disposal of health records?			
5. Is there a formal mechanism for health record access authorization, establishment and modification of access to medical records?			
6. Have internal audit procedures been established so that the administrator can determine which staff are accessing health records?			

Administrative Procedures	Yes	No	N/A
7. Is there procedures established to assure that all personnel who have access to sensitive information have the required authorities as well as all appropriate clearances?			
8. Is there procedures established to assure that all personnel who have access to sensitive information have the required authorities as well as all appropriate clearances?			
9. Are there formal documented instructions for reporting security breaches?			
10. Are there administrative and oversight procedures of policies to ensure the prevention, detection, containment, and correction of security breaches involving risk analysis and risk management?			
11. Do you have formal documented instructions, which include appropriate security measures, for the ending of employee's employment or prohibiting an internal/external user's access to your computer system?			
12. Do you provide training to all employees , agents and contractors concerning the vulnerabilities of the health information at your facility and present ways to ensure the protection of that information?			
Physical Security			
1. Does your facility have policies and procedures to manage and supervise the execution and use of security measures to protect data and to manage and supervise the conduct of personnel in relation to data protection?			
2. Do you have formal, documented policies and procedures that govern the receipt and removal of hardware/software into and out of the facility?			

Physical Security	**Yes**	**No**	**N/A**
3. Do you have policies and procedures to be followed to limit physical access to an entity while ensuring that properly authorized access is allowed?			
4. Do you have instructions/procedures delineating 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 special computer terminal site or type of site, dependent on the sensitivity of the information accessed from the site?			
5. Are there physical safeguards at the facility to eliminate or minimize the possibility of unauthorized access to information? (For example, locating a terminal used to access sensitive information in a locked room and restricting access to that room to authorized personnel, not placing a terminal used to access patient information in an area where patients or visitors can view the screen.)			
Technical Security Services			
1. Does your facility currently require a process or procedure for obtaining necessary patient information during an emergency?			
2. Does your facility have an access control procedure based on context of a transaction (as opposed to being based on the attributes of the initiator or target?			
3. Does your facility use audit control for patient information? (Mechanisms employed to record and examine system activity as related too individual health records.)			
4. Does you facility use either role-based or user-based access controls for obtaining consent for the use and disclosure of health information?			
5. Is there a formal (written) mechanism for processing health records?			

Technical Security Services	**Yes**	**No**	**N/A**
6. Does your facility corroborate that data has not been altered or destroyed in an unauthorized manner? (Examples include the use of check sum, double keying, message authentication code, or digital signature.)			
7. Does your facility have a way to assure that an entity is the one claimed? (Examples include the use of automatic logoff, unique user identification, password, and biometric identification.			
Technical Security Mechanisms			
1. Are there policies and procedures at your facility to outline procedures for to prevent tampering with health information?			
2. Are there procedures for routinely measuring data accuracy?			
3. Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?			
4. Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions?			
5. Is message authentication used in applications to ensure that the sender of a message is known and that the message has not been altered? (e.g. digital signatures)			
6. Are sensitive communications transmissions over open or private networks protected so they cannot be easily intercepted and interpreted by parties other than the intended recipient? (e.g. secure shell)			
7. If encryption is used, does it meet federal standards?			
8. Is any device used that can sense an abnormal condition within the system and provide, either locally or remotely, a signal indication the presence of the abnormality? (e.g. (IDS) Intrusion Detection System)			

Technical Security Mechanisms	Yes	No	N/A
9. Does the information system at your facility allow for audit logs that provide a trace of user action that will support after the fact investigations of how, when and why normal operations ceased?			
10. Is off-line storage of audit logs retained for a period of time, and if so, is access to audit logs strictly controlled?			
11. Are users authenticated uniquely by identity?			
12. Is the identification and authentication method (passwords, tokens, biometrics, etc) commensurate with the risk of compromise?			
13. Are pass words /pass phrases changed at least every ninety days or earlier if needed?			
14. Are event reports dispatched/generated whenever suspicious activity or operational irregularities occur?			
Transaction Standards			
1. Does your facility send or receive patient health data using the most recent HIPAA compliant RPMS packages?			
2. If your facility uses commercial billing packages are they HIPAA compliant?			
3. If your facility uses other that an IHS sponsored clearinghouse for billing, is it certified as being HIPAA compliant?			
4. Has your staff been provided guidance on using HIPAA compliant codes?			
5. Does your facility have Electronic Data Interchange (EDI) agreements with third party payers and CHS providers that PHI is shared with electronically?			

What if we don’t do it?

- IHS patients with less protection than the general public
- IHS patients may seek health care with other providers
- Non-compliance with the law
- Penalties and fines
- May fail to be accredited
- Other organizations could require IHS to be compliant
- Lost revenues

What if we do it?

- We should have been doing it all along
- Many positive benefits for the patient
- Patient TRUST in IHS to protect their health information
- Patient’s will want to use IHS’ health care system
- More efficiency within our health care operations
- Decreases paperwork and errors
- Rapid collection of reimbursements
- Decreased patient complaints

Consents /Authorizations/Notices

Privacy

- IHS is developing Forms for use at all IHS facilities
- No off-the-shelf forms are available
- IHS must include legal reviews of all Forms

EXAMPLES

Current HIPAA Documents in Draft

- Form – 810 Instructions
- Form – Author. Per Patient Request
- Form – Consent for TPO
- Form – Disclose for IHS Use
- Form – Disclose for Research
- Form – Disclose to Others
- Form – Request for Correction of PHI
- HIPAA – Check List
- HIPAA – Delegation of Authority Memo
- Notice of Privacy Practices 8th Draft

ALL are DRAFT!!

- Must be tested for readability
- Printing and shipping requirements to be determined

HIPAA Documents continued

- Policy & Procedure – Accounting of Disclosure
- Policy & Procedure – Delegation of HIPAA Authority
- Policy & Procedure – Confi. Communication By Alter. Means
- Policy & Procedure – De-Identifi. of PHI
- Policy & Procedure – for 810
- Policy & Procedure – for Directory Purposes
- Policy & Procedure – for Minors
- Policy & Procedure – for Research
- Policy & Procedure – Medical Record Fax

ALL are DRAFT!!

HIPAA Documents continued

- Policy & Procedure –Minimum Necessary
- Policy & Procedure – Notice of Privacy Practices
- Policy & Procedure – Re-Identification of PHI
- Policy & Procedure – Request Restrictions
- Policy & Procedure – Right to Access Inspect
- Policy & Procedure – Transmittal by Alternate Means
- Policy & Procedure – Verification of ID Prior Release

ALL are DRAFT!!

HIPAA TRAINING

- Currently Evaluating
  - WEB Based
  - Hard Copy--Booklets
  - Train-the-Trainer
  - Government sponsored Training, e.g., OCR
  - IHS Developed Training
  - Testing and Evaluating New IHS HIPAA Forms

PERSPECTIVES IN CLOSING

HIPAA INTRODUCES NEW ELEMENTS THAT IMPACT THE WAY IHS PROVIDES FOR PATIENT CARE NOT PREVIOUSLY REQUIRED…

- PROTECTS ORAL COMMUNICATIONS
- NOTICE OF PRIVACY PRACTICES
- TRANSACTIONS AND CODE SETS
- SECURITY
- BUSINESS ASSOCIATES AGREEMENTS

PERSPECTIVES IN CLOSING cont’d

PATIENT RIGHTS (EMPOWERING OUR PATIENTS)

- Amend/correct their health records
- Restrict uses and disclosures of their health information
- To receive confidential information/communications
- Complete accounting of disclosures
- Access to various forms of information

PERSPECTIVES IN CLOSING cont’d

- Additional documentation required by providers
- Penalties for NON-COMPLIANCE
- Legal information is translated for patient understanding

BRIEF

READABLE / USABLE

UNDERSTANDABLE

The End