Skip Navigation

United States Department of Health & Human Services

Fact Sheet

October 15, 2002

Contact: HHS Press Office
(202) 690-6343

ADMINISTRATIVE SIMPLIFICATION UNDER HIPAA: NATIONAL STANDARDS FOR TRANSACTIONS, SECURITY AND PRIVACY

Overview: *To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 included a series of "administrative simplification" provisions that required the Department of Health and Human Services (HHS) to adopt national standards for electronic health care transactions. By ensuring consistency throughout the industry, these national standards will make it easier for health plans, doctors, hospitals and other health care providers to process claims and other transactions electronically. The law also requires the adoption of security and privacy standards in order to protect personal health information. HHS is issuing the following major regulations:*

- *Electronic health care transactions (final rule issued);*
- *Health information privacy (final rule issued);*
- *Unique identifier for employers (final rule issued);*
- *Security requirements (proposed rule issued; final rule in development);*
- *Unique identifier for providers (proposed rule issued; final rule in development);*
- *Unique identifier for health plans (proposed rule in development); and*
- *Enforcement procedures (proposed rule in development).*

Although the HIPAA law also called for a unique health identifier for individuals, HHS and Congress have indefinitely postponed any effort to develop such a standard.

Under HIPAA, most health plans, health care clearinghouses and health care providers who engage in certain electronic transactions have two years from the time the final regulation takes effect to implement each set of final standards. More information about the HIPAA standards is available at http://aspe.hhs.gov/admnsimp/ and http://www.cms.gov/hipaa.

BACKGROUND

Today, health plans, hospitals, pharmacies, doctors and other health care entities use a wide array of systems to process and track health care bills and other information. Hospitals and doctor's offices treat patients with many different types of health insurance and must spend time and money ensuring that each claim contains the format, codes and other details required by each insurer. Similarly, health plans spend time and money to ensure their systems can handle transactions from various health care providers and clearinghouses.

Enacted in August 1996, HIPAA included a wide array of provisions designed to make health insurance more affordable and accessible. With support from health plans, hospitals and other health care businesses, Congress

included provisions in HIPAA to require HHS to adopt national standards for certain electronic health care transactions, codes, identifiers and security. HIPAA also set a three-year deadline for Congress to enact comprehensive privacy legislation to protect medical records and other personal health information. When Congress did not enact such legislation by August 1999, HIPAA required HHS to issue health privacy regulations.

Security and privacy standards can promote higher quality care by assuring consumers that their personal health information will be protected from inappropriate uses and disclosures.

In addition, uniform national standards will save billions of dollars each year for health care businesses by lowering the costs of developing and maintaining software and reducing the time and expense needed to handle health care transactions.

COVERED ENTITIES

In HIPAA, Congress required health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions electronically (such as eligibility, referral authorizations and claims) to comply with each set of final standards. Other businesses may voluntarily comply with the standards, but the law does not require them to do so.

COMPLIANCE SCHEDULE

In general, the law requires covered entities to come into compliance with each set of standards within two years following adoption, except for small health plans, which have three years to come into compliance. For the electronic transaction rule only, Congress in 2001 enacted legislation allowing a one-year extension for most covered entities provided that they submit a plan for achieving compliance. As a result, covered entities that qualify for the extension will have until Oct. 16, 2003 to meet the electronic transaction standards instead of the original Oct. 16, 2002 deadline. (Small health plans must still meet the Oct. 16, 2003 compliance date and are not eligible for an extension under the new law.) The legislative extension does not affect the compliance dates for the health information privacy rule, which remains April 14, 2003 for most covered entities (and April 14, 2004 for small health plans).

DEVELOPING STANDARDS

Under HIPAA, HHS must adopt recognized industry standards when appropriate. HHS works with industry standard-setting groups to identify and develop consensus standards for specific requirements. For each set of standards, HHS first develops proposed requirements to obtain public feedback. After analyzing public comments, HHS makes appropriate changes before issuing a final set of standards. The law also allows HHS to propose appropriate changes to the HIPAA regulations to ensure that the standards can be implemented effectively and be maintained over time to continue to meet industry needs.

ELECTRONIC TRANSACTION STANDARDS

In August 2000, HHS issued final electronic transaction standards to streamline the processing of health care claims, reduce the volume of paperwork and provide better service for providers, insurers and patients. The new standards establish standard data content, codes and formats for submitting electronic claims and other administrative health care transactions. By promoting the greater use of electronic transactions and the elimination of inefficient paper forms, these standards are expected to provide a net savings to the health care industry of $29.9 billion over 10 years. All health care providers will be able to use the electronic format to bill for their services, and all health plans will be required to accept these standard electronic claims, referral authorizations and other transactions.

In December 2001, Congress adopted legislation that allows most covered entities to obtain a one-year extension to comply with the standards, from Oct. 16, 2002 to Oct. 16, 2003. To qualify for the extension, the covered entity must submit a plan for achieving compliance by the new deadline. (The legislation did not change the compliance date for small health plans, which remains Oct. 16, 2003.) HHS' Centers for Medicare & Medicaid Services (CMS) has issued a model compliance plan that covered entities may use to obtain an extension. The model plan is available at *http://www.cms.gov/hipaa*.

PRIVACY STANDARDS

In December 2000, HHS issued a final rule to protect the confidentiality of medical records and other personal health information. The rule limits the use and release of individually identifiable health information; gives patients the right to access their medical records; restricts most disclosure of health information to the minimum needed for the intended purpose; and establishes safeguards and restrictions regarding disclosure of records for certain public responsibilities, such as public health, research and law enforcement. Improper uses or disclosures under the rule are subject to criminal and civil sanctions prescribed in HIPAA.

After considering public comment on the final rule, HHS Secretary Tommy G. Thompson allowed it to take effect as scheduled, with compliance for most covered entities required by April 14, 2003. (Small health plans have an additional year.) In March 2002, HHS proposed specific changes to the privacy rule to ensure that it protects privacy without interfering with access to care or quality of care. After considering public comments, HHS issued a final set of modifications on Aug. 14, 2002. Detailed information about the privacy rule is available at *http://www.hhs.gov/ocr/hipaa*.

EMPLOYER IDENTIFIER

In May 2002, HHS issued a final rule to standardize the identifying numbers assigned to employers in the health care industry by using the existing Employer Identification Number (EIN), which is assigned and maintained by the Internal Revenue Service. Businesses that pay wages to employees already have an EIN. Currently, health plans and providers may use different ID numbers for a single employer in their transactions, increasing the time and cost for routine activities such as health plan enrollments and health plan premium payments. Most covered entities must comply with the EIN standard by July 30, 2004. (Small health plans have an additional year to comply.)

ADDITIONAL STANDARDS

Led by CMS, HHS is currently developing other administrative simplification standards. HHS has published proposed regulations for three other major standards - security standards, national identifiers for health care providers and modifications to the original transaction rule - and is now reviewing public comments and preparing final regulations. HHS also is working to develop other proposed standards, including a national health plan identifier and additional electronic transaction standards. In addition, HHS is developing regulations related to enforcement of the adopted standards. The status of key standards required under HIPAA follows:

Security standards. In August 1998, HHS proposed rules for security standards to protect electronic health information systems from improper access or alteration. In preparing final rules for these standards, HHS is considering substantial comments from the public, as well as new laws related to these standards and the privacy regulations. HHS expects to issue final security standards shortly.

National provider identifier. In May 1998, HHS proposed standards to require hospitals, doctors, nursing homes, and other health care providers to obtain a unique identifier when filing electronic claims with public and private insurance programs. Providers would apply for an identifier once and keep it if they relocated or changed specialties. Currently, health care providers are assigned different ID numbers by each different private health plan, hospital, nursing home, and public program such as Medicare and Medicaid. These multiple ID numbers result in slower payments, increased costs and a lack of coordination.

National health plan identifier and other HIPAA regulations. HHS is working to propose standards that would create a unique identifier for health plans, making it easier for health care providers to conduct transactions with different health plans. HHS is also working to develop additional transaction standards for attachments to electronic claims and for a doctor's first report of a workplace injury. In addition, HHS is developing a proposed rule on enforcement of the HIPAA requirements. As with other HIPAA regulations, HHS will first consider public comment on each proposed rule before issuing any final standards.

Personal identifier on hold. Although HIPAA included a requirement for a unique personal health care identifier, HHS and Congress have put the development of such a standard on hold indefinitely. In 1998, HHS delayed any work on this standard until after comprehensive privacy protections were in place. Since 1999, Congress has adopted budget language to ensure no such standard is adopted without Congress' approval. HHS has no plans to develop such an identifier.

# # #

Note: All HHS press releases, fact sheets and other press materials are available at *http://www.hhs.gov/news*.

Last Revised: October 31, 2002

Skip Navigation

United States Department of Health & Human Services

News Release

FOR IMMEDIATE RELEASE
Thursday, Feb. 13, 2003

Contact: CMS Press Office
(202) 690-6145

HHS ADOPTS FINAL SECURITY STANDARDS, TRANSACTION MODIFICATIONS FOR ELECTRONIC HEALTH INFORMATION UNDER HIPAA

HHS Secretary Tommy G. Thompson today announced the adoption of final security standards for protecting individually identifiable health information when it is maintained or transmitted electronically. At the same time, he also announced the adoption of modifications to a number of the electronic transactions and code sets adopted as national standards.

Both final regulations are required as part of the administrative simplification provisions included in the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

"Overall, these national standards required under HIPAA will make it easier and less costly for the health care industry to process health claims and handle other transactions while assuring patients that their information will remain secure and confidential," Secretary Thompson said. "The security standards in particular will help safeguard confidential health information as the industry increasingly relies on computers for processing health care transactions."

Under the security standards announced today, health insurers, certain health care providers and health care clearinghouses must establish procedures and mechanisms to protect the confidentiality, integrity and availability of electronic protected health information. The rule requires covered entities to implement administrative, physical and technical safeguards to protect electronic protected health information in their care.

The security standards work in concert with the final privacy standards adopted by HHS last year and scheduled to take effect for most covered entities on April 14. The two sets of standards use many of the same terms and definitions in order to make it easier for covered entities to comply.

"We took great care to address every detail and produce a rule that health care providers will find easy to understand and implement," said Tom Scully, administrator of HHS' Centers for Medicare & Medicaid Services (CMS).

The security standards will be published as a final rule in the Feb. 20 Federal Register with an effective date of April 21, 2003. Most covered entities will have two full years -- until April 21, 2005 -- to comply with the standards; small health plans will have an additional year to comply, as HIPAA requires.

In a separate final regulation, HHS adopted modifications to the transaction standards, which health plans, certain health care providers and health care clearinghouses by law must use for electronic health care transactions. Covered entities must comply with these modified transaction standards by Oct. 16, 2003.

The final transaction modifications rule, which will also be published in the Federal Register on Feb. 20, combines

two proposed rules published May 31, 2002. HHS worked extensively with the Designated Standards Maintenance Organizations (DSMOs) to revise the proposed changes to the standards, as required by Congress as part of HIPAA.

Major provisions of the final rule include:

- Repealing the National Drug Code (NDC) as the standard medical data code set for reporting drugs and biologics in all non-retail pharmacy transactions.

- Adopting the proposed Addenda to the implementation guides with some technical revisions based upon comments received and consultation with the DSMOs.

- For retail pharmacy transactions:
  - Adopting the National Council for Prescription Drug Programs (NCPDP) Batch Version 1.1 to support the Telecommunications Version 5.1.
  - Adopting the Accredited Standards Committee (ASC) X12N 835 as the standard for payment and remittance advice and the NCPDP Telecommunications Version 5.1 and NCPDP Batch Version 1.1. Implementation Guides as the standard for the referral certification and authorization transaction.
  - Continuing the use of the NDC code set for the reporting of drugs and biologics.

The rule also adopts modified standards for two transactions that were not included in the proposed rules -- premium payments, and coordination of benefits. The modifications were approved by the DMSOs and merely provide explanatory guidance.

CMS is responsible for implementing and enforcing the security standards, the transactions standards and other HIPAA administrative simplification provisions, except for the privacy standards. HHS' Office for Civil Rights is responsible for implementing and enforcing the privacy rule.

The complete text of both final rules will be available at the CMS website at http://www.cms.hhs.gov/hipaa/hipaa2. The full text of the Addenda to the transaction modifications rule will be available at http://hipaa.wpc-edi.com/HIPAAAddenda_40.asp.

More information about HIPAA standards is available at http://www.cms.hhs.gov/hipaa and http://www.aspe.hhs.gov/admnsimp/. A fact sheet summarizing the administrative simplification standards required by HIPAA is available at http://www.hhs.gov/news/press/2002pres/hipaa.html.

###

Note: All HHS press releases, fact sheets and other press materials are available at *http://www.hhs.gov/news*.

Last Revised: February 11, 2003

U.S. Department of Health & Human Services • 200 Independence Avenue, S.W. • Washington, D.C. 20201

IHS HIPAA FORMS/POLICY & PROCEDURES

The following is a current list of forms and policy/procedures the IHS has under development:

FORMS:

1. Authorization for Use or Disclosure of Health Information—45 CFR 164.502 **(FORM IHS 810)**
2. Request for an Accounting of Disclosures—45 CFR 164.528; 45 CFR 5b.9(c) **(FORM)**
3. Request for Correction/Amendment of Protected Health Information—5 USC 522a(d), 45 CFR 164.526 **(FORM)**
4. Request for Restriction(s)/Request for Revocation of Restriction(s)—42 CFR 164.522(a) **(FORM)**

POLICIES & PROCEDURES:

1. Use or Disclosure of Health Information Pursuant to Authorization or Valid Written Request–(Form IHS 810)—45 CFR 164.502
2. Creating a Limited Data Set—45 CFR 164.514(e)
3. De-Identification of Protected Health Information and Subsequent Re-Identification—45 CFR 164.514(a)-(c)
4. HIPAA Delegation of Authority Memo
5. Instructions for Developing Policies and Procedures to Implement HIPAA's Administrative Requirements—45 CFR 164.530
6. Limiting the Use/Disclosure of and Requests for Protected Health Information to the Minimum Necessary—45 CFR 164.502(b)
7. Maintenance, Use and Disclosure of Psychotherapy Notes—45 CFR 164.508(a)(2), (a)(3)
8. Matters Related to Accountings of Disclosures of Protected Health Information—45 CFR 164.528; 45 CFR 5b.9(c)
9. Notice of Privacy Practices
10. Patients' Rights to Access, Inspect and Obtain a Copy of Their Protected Health Information—45 CFR 164.524, 45 CFR 5b5, 5b6
11. Protected Health Information of Un-emancipated Minors—45 CFR 164.502(g); 45 CFR Part 5b
12. Providing Indian Health Service Notice of Privacy Practices—45 CFR 164.520
13. Requests for Correction/Amendment of Protected Health Information—45 CFR 164.526; 5 U.S.C. 552a(d)
14. Requests for Restrictions on the Use and Disclosures of Protected Health Information—45 CFR 164.522(a)
15. Sending and Receiving Medical Records Information by Facsimile
16. Transmittal of Confidential Communication by Alternate Means—45 CFR 164.522(b)(2)
17. Use and Disclosure for Directory Purposes—45 CFR 164.510(a)
18. Use and Disclosure of Protected Health Information for Disaster Relief Purposes—45 CFR 164.510(b)(4)
19. Use and Disclosure of Protected Health Information for Research Purposes—45 CFR 164.512(i), 5 USC 552a(b)(5)
20. Uses and Disclosures of Protected Health Information for Involvement in the Patient's Care and for Notification Purposes—45 CFR 164.510(b)(1-3)
21. Verification of Identity Prior To Disclosure of Protected Health Information—45 CFR 164.514(h)

people who have received products that have been recalled or withdrawn), or post marketing surveillance.

Workers Compensation: IHS may use or disclose your health information for workers compensation purposes as authorized or required by law.

Public Health: IHS may use or disclose your health information to public health or other appropriate government authorities as follows: (1) IHS may use or disclose your health information to government authorities that are authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, or conducting public health surveillance, investigations, and interventions; (2) IHS may disclose your health information to government authorities that are authorized by law to receive reports of child abuse or neglect, and (3) IHS may disclose your health information to government authorities that are authorized by law to receive reports of other abuse, neglect, or domestic violence as required by law, or as authorized by law if IHS believes it is necessary to prevent serious harm. Where authorized by law, IHS may disclose your health information to an individual who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition. In some situations (for example, if you are employed by IHS or another component of the Department of Health and Human Services, or if necessary to prevent or lessen a serious and imminent threat to the health and safety of an individual or the public), IHS may disclose to your employer health information concerning a work-related illness or injury or a workplace-related medical surveillance.

Correctional Institution: If you are an inmate of a correctional institution, IHS may use or disclose to the institution, health information necessary for your health and the health and safety of other individuals such as officers or employees or other inmates.

Law Enforcement: IHS may use or disclose your health information for law enforcement activities as authorized by law or in response to a court of competent jurisdiction.

Members of the Military: If you are a member of the military services including the Commissioned Corps of the United States Public Health Service, IHS may use or disclose your health information if necessary to the appropriate military command authorities as authorized by law.

Health Oversight Authorities: IHS may use or disclose your health information to health oversight agencies for activities authorized by law. These oversight activities include: investigations, audits, inspections and other actions. These are necessary for the government to monitor the health care system, government benefit programs, and entities subject to government regulatory programs and/or civil rights laws for which health information is necessary to determine compliance. IHS is required by law to disclose protected health information to the Secretary of HHS to investigate or determine compliance with the HIPAA privacy standards.

Compelling Circumstances: IHS may use or disclose your health information in certain other situations involving compelling circumstances affecting the health or safety of an individual. For example, in certain circumstances: (1) we may disclose limited protected health information where requested by a law enforcement official for the purpose of identifying or locating a suspect, fugitive, material witness or missing person; (2) if you are believed to be a victim of a crime, a law enforcement official requests information about you and we are unable to obtain your agreement because of incapacity or other emergency circumstances, we may disclose the requested information if we determine that such disclosure would be in your best interests; (3) we may use or disclose protected health information as we believe is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person; (4) we may use or disclose protected health information in the course of judiciary and administrative proceedings if required or authorized by law; (5) we may use or disclose protected health information to report a crime committed on IHS health facility premises or when IHS is providing emergency health care; and (6) we may make any other disclosures that are required by law.

Non Violation of this Notice: IHS is not in violation of this Notice or the HIPAA Privacy Rule if any of its employees or its contractors (business associates) discloses protected health information under the following circumstances:

1. **Disclosures by Whistleblowers:** If an IHS employee or contractor (business associate) in good faith believes that IHS has engaged in conduct that is unlawful or otherwise violates clinical and professional standards or that the care or services provided by IHS has the potential of endangering one or more patients or members of the workplace or the public and discloses such information to:
   a. A Public Health Authority or Health Oversight Authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions, or the suspected violation, or an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by IHS; or
   b. An attorney on behalf of the workforce member, or contractor (business associate) or hired by the workforce member or contractor (business associate) for the purpose of determining their legal options regarding the suspected violation.
2. **Disclosures by Workforce Member Crime Victims:** Under certain circumstances, an IHS workforce member (either an employee or contractor) who is a victim of a crime on or off the hospital premises may disclose information about the suspect to law enforcement official provided that:
   a. The information disclosed is about the suspect who committed the criminal act.
   b. The information disclosed is limited to identifying and locating the suspect.

Any other uses and disclosures will be made only with your written authorization, which you may later revoke in writing at any time. (Such revocation would not apply where the health information already has been disclosed or used or in circumstances where IHS has taken action in reliance on your authorization or the authorization was obtained as a condition of obtaining insurance coverage and the insurer has a legal right to contest a claim under the policy or the policy itself.)

To exercise your rights under this Notice, to ask for more information, or to report a problem contact the Service Unit Director/Chief Executive Officer or the Service Unit Privacy official at:

If you believe your privacy rights have been violated, you may file a written complaint with the above individual(s) or the Secretary of Health and Human Services, U.S. Department of Health and Human Services, Washington, D.C. 20201. There will be no retaliation for filing a complaint.

Effective Date: April 14, 2003

HIPAA
Health Insurance Portability and Accountability Act
PRIVACY RULE

INDIAN HEALTH SERVICE

NOTICE OF PRIVACY PRACTICES

April 14, 2003

HIPAA
Health Insurance Portability and Accountability Act
PRIVACY RULE

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

SUMMARY OF YOUR PRIVACY RIGHTS

I. Understanding Your Health Record/Information

Each time you visit an Indian Health Service facility for services, a record of your visit is made. If you are referred by the Indian Health Service through the Contract Health Service (CHS) program, IHS also keeps a record of your CHS visit. Typically, this record contains your symptoms, examination, test results, diagnoses, treatment, and a plan for future care. This information, often referred to as your health record, serves as a:

- Plan for your care and treatment
- Communication source between health care professionals
- Tool with which we can check results and continually work to improve the care we provide
- Means by which Medicare, Medicaid or private insurance payers can verify the services billed
- Tool for education of health care professionals
- Source of information for public health authorities charged with improving the health of the people
- Source of data for medical research, facility planning and marketing
- Legal document that describes the care you receive

Understanding what is in your health record and how the information is used helps you to:

- Ensure its accuracy
- Better understand why others may review your health information
- Make an informed decision when authorizing disclosures

II. Your Health Information Rights

Although your health record is the physical property of the Indian Health Service, the information belongs to you.

You have the right to:

- **Inspect and receive a copy of your health record**
- **Request a restriction** on certain uses and disclosures of your health information. For example, you may ask that we not disclose your health information and or treatment to a family member. IHS is not required to agree to your request; but if we do, we will comply with your request unless the information is needed to provide you with emergency services.
- **Request a correction/amendment to your health record** if you believe the health information we have about you is incorrect or incomplete, we may amend your record or include your statement of disagreement.
- **Request confidential communications about your health information.** You may ask that we communicate with you at a location other than your home or by a different means of communications such as telephone or mail.
- **Receive a listing of certain disclosures IHS has made** of your health information upon request. This information is maintained for six years or the life of the record, whichever is longer.
- **Revoke your written authorization to use or disclose health information.** This does not apply to health information already disclosed or used or in circumstances where we have taken action on your authorization or the authorization was obtained as a condition of obtaining insurance coverage and the insurer has a legal right to contest a claim under the policy or the policy itself.
- **Obtain a paper copy of the IHS Notice of Privacy Practices** upon request.
- **Obtain a paper copy of the IHS Health and Medical Records; System Notice # 09-17-0001 upon request.**

III. IHS' Responsibilities

The Indian Health Service is required by law to:

- Maintain the privacy of your health information
- Inform you about our privacy practices regarding health information we collect and maintain about you
- Notify you if we are unable to agree to a requested restriction
- Accommodate reasonable requests you may have to communicate health information by alternative means or at alternative locations
- Honor the terms of this notice or any subsequent revisions of this notice

IHS reserves the right to change its privacy practices and to make the new provisions effective for all protected health information it maintains. If IHS makes any significant changes to this Notice, it will send you a copy within 60 days. IHS also will post any revised Notice of Privacy Practices at public places in its health care facilities and on its web site at www.ihs.gov and you may also request a copy of the notice.

IHS understands that health information about you is personal and is committed to protecting your health information. **IHS will not use or disclose your health information without your permission, except as described in this notice and as permitted by the Privacy Act and the IHS Health and Medical Records; System Notice 09-17-0001.**

IV. How IHS may use and disclose health information about you.

The following categories describe how we may use and disclose health information about you.

We will use and disclose your health information to provide your treatment.

For example: Your personal information will be recorded in your health record and used to determine the course of treatment for you. Your health care provider will document in your health record her/his instructions to members of your healthcare team. The actions taken and the observations made by the members of your healthcare team will be recorded in your health record so your health care provider will know how you are responding to treatment.

If IHS refers you to another health care facility under the Contract Health Service (CHS) program, IHS may disclose your health information to that health care provider for treatment decisions.

If you are transferred to another facility for further care and treatment, IHS may disclose information to that facility to enable them to know the extent of treatment you have received and other information about your condition.

Your health care provider(s) may give copies of your health information to others to assist in your treatment.

We will use and disclose your health information for payment purposes.

For example: If you have private insurance, Medicare, or Medicaid coverage, a bill will be sent to your health plan for payment. The information on or accompanying the bill will include information that identifies you, as well as your diagnosis, procedures, and supplies used for your treatment.

If IHS refers you to another health care provider under the Contract Health Service (CHS) program, IHS may disclose your health information with that provider for health care payment purposes.

We will use and disclose your health information for health care operations.

For example: We may use your health information to evaluate your care and treatment outcomes with our quality improvement team. This information will be used to continually improve the quality and effectiveness of the services we provide. This includes health care services provided under Contract Health Services (CHS) program.

Business Associates: IHS provides some healthcare services and related functions through the use of contracts with business associates. For example, IHS may have contracts for medical transcription. When these services are contracted, IHS may disclose your health information to business associates so that they can perform their jobs. We require our business associates to protect and safeguard your health information in accordance with all applicable federal laws.

Directory: If you are admitted to an IHS facility, IHS may use or disclose your name, general condition, religious affiliation, and location within our facility, for facility directory purposes, unless you notify us that you object to this information being listed. IHS may provide your religious affiliation only to members of the clergy.

Notification: IHS may use or disclose your health information to notify or assist in the notification of a family member, personal representative or other authorized person(s) responsible for your care, unless you notify us that you object.

Communication with Family: IHS health providers may use or disclose your health information to others responsible for your care unless you object. For example, IHS may provide your family members, other relatives, close personal friends or any other person you identify with health information which is relevant to that person's involvement with your care or payment for such care.

Interpreters: In order to provide you proper care and services, IHS may use the services of an interpreter. This may require the use or disclosure of your personal health information to the interpreter.

Research: IHS may use or disclose your health information for research purposes that has been approved by an IHS Institutional Review Board (IRB) that has reviewed the research proposal and established protocols to ensure the privacy of your health information. IHS may also use or disclose your health information for research purposes based on your written authorization.

Uses and Disclosures about Decedents: IHS may use or disclose health information about decedents to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. IHS also may disclose health information to funeral directors consistent with applicable law as necessary to carry out their duties. In addition, IHS may disclose protected health information about decedents where required under the Freedom of Information Act or otherwise required by law.

Organ Procurement Organizations: IHS may use or disclose your health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs for the purpose of facilitating organ, eye or tissue donation and transplant.

Treatment Alternatives and Other Health-related Benefits and Services: IHS may contact you to provide information about treatment alternatives or other types of health-related benefits and services that may be of interest to you. For example: we may contact you about the availability of new treatment or services for diabetes.

Appointment Reminders: IHS may contact you with a reminder that you have an appointment for medical care at an IHS facility or to advise you of a missed appointment.

Food and Drug Administration (FDA): IHS may use or disclose your health information to the FDA in connection with an FDA-regulated product or activity. For example: we may disclose to the FDA information concerning adverse events involving food, dietary supplements, product defects or problems, and information needed to track FDA-regulated products or to conduct product recalls, repairs, replacements, or lookbacks (including locating

Indian Health Service
Status of HIPAA Formats for EDI

Updated 1/27/03

Electronic Transaction Type	Use of Transaction	RPMS Associated Application Patch	Status of Development	Certified	Available date for Download to Area *
270	Is used by the provider to request eligibility information electronically.	Patient Registration V6.0, P17	Completed	Yes	12/02/02
271	Is used by the health plan to return eligibility information to the provider.	Patient Registration V6.0, P17	Completed	Yes	12/02/02
837	Is used by the provider to submit a claim for payment.	Third Party Billing, V2.6, P 1	Completed	No	12/03/02
835	Is used by the third party payer to notify the provider of the benefit determination.	Accounts Receivable, V1.6 P3	Completed	Yes	12/05/02
278	Is used by CHS to make referrals and provide other information to a provider.	Contract Health Services (CHS), V3.1, P5	Completed	Yes	12/28/02
276	Is used by the provider to inquire about the status of a claim	Accounts Receivable, V1.6, P3	Under development. Exp. Comp. 8/15/02	Yes	12/05/02
277	Is used by the third party payer to report on the status of a claim	Accounts Receivable, V1.6, P3	Under development. Exp. Comp. 8/15/02	Yes	12/05/02
277/275 + HL7	Is used for an electronic claim attachment	Third Party Billing (when applicable)	Waiting for specifications	No	----
NCPDP 5.1	These are the new coding standards for Pharmacy electronic claims.	Pharmacy POS, V1.0, P3 includes capability Sites need separate PO with Web MD	Under development as each Insurer is ready	Yes & No Patches released periodi-cally	10/14/02

* After availability date see the Area Office Information Systems Coordinator or the facility Information Systems Site Manager for installation status at the Area or facility location.

Indian Health Service
Status of HIPAA Formats for EDI

Updated 1/27/03

Electronic Transaction Type	Use of Transaction	RPMS Associated Application Patch	Status of Development	Certified	Available date for Download to Area *
270	Is used by the provider to request eligibility information electronically.	Patient Registration V6.0, P17	Completed	Yes	12/02/02
271	Is used by the health plan to return eligibility information to the provider.	Patient Registration V6.0, P17	Completed	Yes	12/02/02
837	Is used by the provider to submit a claim for payment.	Third Party Billing, V2.6, P 1	Completed	No	12/03/02
835	Is used by the third party payer to notify the provider of the benefit determination.	Accounts Receivable, V1.6 P3	Completed	Yes	12/05/02
278	Is used by CHS to make referrals and provide other information to a provider.	Contract Health Services (CHS), V3.1, P5	Completed	Yes	12/28/02
276	Is used by the provider to inquire about the status of a claim	Accounts Receivable, V1.6, P3	Under development. Exp. Comp. 8/15/02	Yes	12/05/02
277	Is used by the third party payer to report on the status of a claim	Accounts Receivable, V1.6, P3	Under development. Exp. Comp. 8/15/02	Yes	12/05/02
277/275 + HL7	Is used for an electronic claim attachment	Third Party Billing (when applicable)	Waiting for specifications	No	----
NCPDP 5.1	These are the new coding standards for Pharmacy electronic claims.	Pharmacy POS, V1.0, P3 includes capability Sites need separate PO with Web MD	Under development as each Insurer is ready	Yes & No Patches released periodi-cally	10/14/02

* After availability date see the Area Office Information Systems Coordinator or the facility Information Systems Site Manager for installation status at the Area or facility location.

Transactions and Code Sets **UPDATED 01/27/03**

Task	Headquarters	Who	Status/ Comp. Date	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 5.1 276/277 274	ITSC	All formats completed & distributed 12/02						
Distribute HIPAA compliant software to I/T/U.	Email sent out by Director of ITSC on 10/2/2002	ITSC	Completed	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.	Ongoing by ITSC Support staff	ITSC/ Area	Ongoing	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 they will be HIPAA compliant.	Buss. Off. CHS Off.	Area Survey sent out 06/25/02.	Develop list of third payers and CHS providers that the Area Office either bills or pays for services and note those they will be HIPAA compliant.	Buss. Off. CHS Off.	Responding to 6/25/02 survey.	Develop list of third payers and CHS providers that the facility either bills or pays for services directly and note those they will be HIPAA compliant.	Buss. Off. CHS Off.	
Develop a sample EDI letter of agreement to be for use with third party payers and contract providers for use of HIPAA transactions	Develop the sample letter and share it with the Area Offices.	Buss. Off. CHS Off.	Sample EDI letter completed 6/02. Ongoing completion by transaction type.						
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.	Ongoing	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.	