

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Title II Subtitle F-Administrative Simplification

April, 2002

This document was developed to assist the state agencies of Ohio in understanding the obligations imposed by the Health Insurance Portability and Accountability Act (HIPAA). The State of Ohio provides no guarantee of accuracy or warranties of any kind. Utilization of this information is at the sole risk of the user. As with any matter of law, independent legal counsel should be consulted regarding compliance with the requirements of the HIPAA.

Title II includes Subtitle F, Administrative Simplification that is being implemented by the State of Ohio agencies impacted by its provisions. Administrative Simplification requires that health plans and health care clearinghouses use certain standard transaction formats and code sets for the electronic transmission of health information. Health care providers that transmit any health information in electronic form in connection with a transaction covered in the rules are also required to use the standard transactions and code sets for the electronic transmission of health information. In addition, it establishes standards for the protection and security of individually identifiable health information, and provides penalties for its wrongful disclosure. The purpose of this Subtitle is to enhance health care insurance and delivery systems by making them more efficient, simpler, and less costly. Administrative Simplification is being implemented nationwide through a series of rules promulgated by the federal Department of Health and Human Services (HHS). The following is a **brief overview** of the rules and proposed rules based on the requirements of HIPAA as of April, 2002. For more comprehensive information please read the background papers of the Privacy, Transaction and Code Sets, and Security rules provided on this web site, or for complete information go to the federal Administrative Simplification web site at: <http://aspe.hhs.gov/admsimp/Index.htm>

Privacy

HIPAA Administrative Simplification provisions require the development of standards to protect the privacy of individually identifiable health information. The use of "industry-wide" transaction standards will reduce the amount of translation necessary between the different transaction formats used in the health care industry today. However, improving the ease with which data is transferred carries additional dangers in terms of privacy of that data. Therefore, this rule enhances the protection of individually identifiable health information, and presents standards and procedures with the respect to the rights of individuals in relationship to their individually identifiable health information.

- The rule specifies how covered entities will transfer, disclose, protect or receive protected health care information.
- "Protected Health Information" is individually identifiable health information that is transmitted or maintained in any form or medium.
- The Privacy rule specifies what information should be protected.
- The Privacy Rule addresses the privacy rights of individuals.
- In general, these requirements will preclude disclosure of personal health information without active, informed consent of the individual.

- Non-compliance may result in sanctions, legal liability, public scrutiny and barriers to doing business with trading partners.

Transactions and Code Sets

HIPAA Administrative Simplification provisions require the development and implementation of national standards for electronic health care transactions and data elements for financial and administrative transactions described in HIPAA. The Secretary of Health and Human Services has the authority to establish other financial and administrative transactions through a negotiated rule making process with national standard setting organizations if they are consistent with the goals of improving the operation of the health care system and reducing administrative costs. The implementation date of this rule is October 16, 2002, but an entity can implement October 16, 2003 if it files a compliance plan with HHS. Small health plans are required to implement by October 16, 2003.

Transactions: The rule mandate that standard transaction formats and code sets in connection with the following business functions be implemented by health plans, health care clearinghouses, and health care providers that transmit any health information in electronic form in connection with a transaction covered in the rules. The transactions are to be implemented in a HIPAA compliant American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X12 standard as designated by their number.

- Health Care Claims or Equivalent Encounter Information-837
- Health Care Payment and Remittance Advice-835
- Coordination of Benefits- Not yet a separate transaction but currently included in other transactions, such as the 837, 835, or 270/271 as a business function
- Health Care Claim Status-276 and 277
- Enrollment and Disenrollment in a Health Plan-834
- Eligibility for a Health Plan-270 and 271 (for coverage and benefits)
- Health Plan Premium Payments-820
- Referral Certification and Authorization-278
- Health Claims Attachments-275 On Hold Until Future Version of ANSI ASC X12
- Report of First Injury-In Development
- Other Transactions That the Secretary May Prescribe By Regulation

Code Sets By October 16, 2002 (Note: Public Law 107-105) amended the implementation date to October 16, 2003 if a compliance plan is submitted to HHS), the rule mandates that the following code sets must be used in the transactions by health plans, health care clearinghouses, and health care providers that transmit any health information in electronic format in connection with a transaction covered in the rules. Small health plans are required to implement on October

16, 2003.

Administrative Simplification

April, 2002

Page 3

- Medical data code sets
 - International Classification of Diseases, 9th Edition, Clinical Modification (ICD-9-CM), Volumes 1, 2, and 3
 - National Drug Codes
 - The Code on Dental Procedures and Nomenclature (ADA)
 - The combination of Health Care Financing Administration Common Procedure Coding System (HCPCS) and Current Procedural Terminology, Fourth Edition (CPT-4) for physician and other health care services.
 - The Health Care Financing Administration Common Procedure Coding System (HCPCS) for all other substances, equipment, supplies, or items used in health care services.
- Nonmedical data code sets that are described in the implementation specifications in the rule and are valid at the time the transaction is initiated.

Security

The Security rule specifies how a health plan, health care clearinghouse, and covered health care provider is to protect and secure health information. The proposed security regulation requires the ability to control access to protected health information (PHI); to protect PHI from the accidental or intentional disclosure to unauthorized individuals, and to protect PHI from alteration, destruction, or loss. The core of this regulation is the national realization that systems, like people, must be accountable for the security of personal health information. Faster access and delivery of this information has the potential to compromise these systems, so protections need to be verifiable. The rule consists of five parts listed below. The Security rule has not yet been published in final form. It is expected to be finalized during the second or third quarter of 2002, with compliance required 24 months after the rule is released in final form. Small health plans must comply within 36 months.

- Administrative Procedures to Guard Data Integrity, Confidentiality, and Availability: These include documented, formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data.
- Physical Safeguards to Guard Data Integrity, Confidentiality, and Availability: These include the protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion.
- Technical Security Services to Guard Data Integrity, Confidentiality, and Availability: These include the processes that are put in place to protect information and to control individual access to information.
- Technical Security Mechanisms: These include the processes that are put in place to guard against unauthorized access to data that is transmitted over a communications network.
- Electronic Signature: The use of an electronic signature is optional. This section contains the

standard for a digital signature. A “digital signature” is an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters so that the identity of the signer and integrity of the data can be verified.

HIPAA Administrative Simplification

April, 2002

Page 4

National Identifiers

HIPAA establishes four unique identifiers for providers, employers, health plans and personal identification. Information regarding the two published, but not final, rules, National Provider Identifier (NPI) and the National Employer Identifier (NEI) are below. The National Health Plan Identifier is in development and the National Individual Identifier is on indefinite hold. The earliest estimate for finalizing the NPI and the NEI is second quarter, 2002 and generally they are required to be implemented 24 months after the effective date of the final rule. Small health plans are required to implement within 36 months of the effective date.

National Provider Identifier (NPI): This rule proposes a standard for a national health care provider identifier and requirements concerning its use by health plans, health care clearinghouses, and health care providers. The health plans, health care clearinghouses, and health care providers would use the identifier, among other uses, in connection with certain electronic transactions (the proposed NPI is an 8-position alphanumeric identifier).

National Employer Identifier (NEI): This rule proposes a standard for a national employer identifier and requirements concerning its use by health plans, health care clearinghouses, and health care providers. The health plans, health care clearinghouses, and health care providers would use the identifier, among other uses, in connection with certain electronic transactions. As a note: employers are not required by HIPAA to use the standard employer identifier or standard health care transactions. However, an employer is required to disclose their EIN when requested to an entity that conducts standard transactions that require that employer’s identifier. The federal HHS is proposing as the standard the employer identification number (EIN), which is assigned by the Internal Revenue Service (IRS), Department of the Treasury.

RULES IN DEVELOPMENT

The following is a list of the rules that are still under development by the Federal HHS. There will be a comment period once they are published, and generally are required to be implemented 24 months after the effective date of the final rule.

- National Health Plan Identifier: It is expected that a 9-digit number will be assigned to all health plans.
- Claims Attachments Rule
- Enforcement Rule
- National Individual Identifier: the NPRM was subsequently placed on indefinite hold pending

further review.

- Privacy Guidance
- Modifications to Standards for Electronic Transactions
- Revisions to Transactions and Code Sets Standards
- Standard for Electronic Signature

HIPAA Administrative Simplification

April, 2002

Page 5

- Report of First Injury
- Exclusion From Medicare
- Medicare Coverage Requirement

Source: Much of the information in this paper is directly from the federal Administrative Simplification web site.