

HIPAA

Health Insurance Portability & Accountability Act

Volume I, January 2002

A one-year extension to the electronic Transactions and Code set portion of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was passed by the Senate and House of Representatives December 2001. Under this resolution, affected health care entities can delay use of the new ANSI electronic formats and standard code sets until Oct. 16, 2003, if they formally apply for an extension. As a result, all references to the Oct. 16, 2002 deadline may change.

Law Impacts Providers, Health Plans and Clearinghouses

As a health care provider, you've probably begun to hear the term "HIPAA" at workshops, in publications and in working with other health care organizations. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal statute designed to standardize electronic communication within the health care system. The electronic transaction part of HIPAA Administrative Simplification (AS) goes into effect October 16, 2002. HIPAA AS is also intended to protect the security and privacy of patient health information. Privacy is effective April 14, 2003. HIPAA AS applies to health plans, health care clearinghouses, and health care providers who conduct certain transactions electronically. HIPAA refers to these affected groups as "covered entities."

For providers, HIPAA can affect such things as:

- How you send your claims
- The amount of health care information you are allowed to share with others
- Security on your computer systems

This flyer will provide some basic information about the five sections that make up the Administrative Simplification (AS) portion of HIPAA and help you understand their impact on your organization.

Five Areas of HIPAA-AS May Require Provider Attention

HIPAA regulates the following five areas: Transactions, Code Sets, Identifiers, Privacy and Security.

Transactions – Effective: October 16, 2002

If you are sending claims electronically, you are performing a transaction. Transactions are the standard kinds of electronic data that providers can send to health plans and the data we can return to you. Transactions include claims, remittance advices, referrals, authorizations, claim status and eligibility requests.

HIPAA adopted the American National Standards Institutes (ANSI) format for all electronic transactions. These are the formats that will be used by providers, health plans and clearinghouses across the country beginning this October. The mandated standard formats are:

Transaction	Standard Format
Health Care Claim	ANSI 837
Health Care Remittance Advice	ANSI 835
Referrals and Authorizations	ANSI 278
Eligibility (request from Provider)	ANSI 270
Eligibility (response from Health Plan)	ANSI 271
Health Claim Status (request from Provider)	ANSI 276
Health Claim Status (response from Health Plan)	ANSI 277

In addition, we will be able to accept premium payments and enroll/disenroll members with ANSI 820 and ANSI 834 standard transactions.

Medical (Clinical) Code Sets – Effective October 16, 2002

Standardization will also affect the codes you use when submitting health care information. Under HIPAA, the same standard coding formats will be used at every health plan.

Standard medical (clinical) code sets include:

- ICD-9-CM Volumes 1, 2 and 3
- National Drug Codes (NDC)
- Current Dental Terminology (CDT3)
- Health Care Financing Administration Common Procedure Coding System (HCPCS)
- Current Procedural Terminology, Fourth Edition (CPT-4™)

Like many carriers, BlueCross BlueShield of Tennessee created special codes for its providers to use in filing claims for certain procedures or services. As we work to meet HIPAA requirements for standardized codes, we will eliminate non-standard codes. As a result, all paper and electronic submitters will be required to use standard codes when filing claims to us. We will notify providers of coding changes in future publications.

Privacy Standards – Effective April 14, 2003

Privacy determines **who** should have access to **what** medical information. This part of HIPAA gives patients greater control on the use of their health care data, also referred to as their Protected Health Information or PHI. It applies to information used by covered entities in any form - written, verbal and electronic. Privacy sets boundaries on the amount of information that can be released. HIPAA privacy rules will require providers considered to be covered entities to:

- Provide a written notice of their information practices to patients
- Train employees to protect privacy
- Designate a responsible Privacy Officer
- Use reasonable efforts to limit released information to the minimum necessary

- Obtain consent prior to using or releasing PHI to carry out treatment, payment or health care operations. (Some exceptions are noted in the regulations when information can be released without authorization, such as for public health purposes or averting serious threats to health or safety.)

The Department of Health and Human Services can audit practices for compliance with Privacy regulations. There are civil and criminal penalties for non-compliance.

If you have concerns about your current office practices and how they will be affected, you can review the Office of Civil Rights guide on Privacy regulations on their Internet Web site at www.hhs.gov/ocr/hipaa/finalmaster.html. The guide provides a brief description of each section of the regulations and includes a series of questions and answers.

Additionally, you may want to consult legal counsel on your specific privacy issues.

Security – Pending Final Rules

The final rules for security are still pending. Security is how health information is protected.



It can include having written procedures for handling health information and training your staff on security (Administrative Security).

It also includes having secure building and work area access (Physical Security). And finally security for your electronic transmission system (Technical Security). Technical security includes such things as encryption, which is scrambling data in case it is intercepted by someone other than the intended receiver.

Identifiers – Pending Final Rules

The final rules on national identifier numbers are still pending. Identifiers include:

Identifiers – Pending Final Rules (Cont'd)

- National Provider Identifier (NPI) – Expected to be an eight to ten-digit number assigned to the provider for use with all transactions.
- National Employer Identifier – Expected to be the nine-digit tax identification number assigned to employers.
- National Health Plan Identifier – Expected to be a nine-digit number assigned to health plans.

Tips for Testing

Transaction testing is planned to begin early this year with the claim submission transaction (ANSI 837). All transactions must be tested and approved by October 16, 2002.

If you use a software vendor, billing agency or clearinghouse, you should contact them to determine their plans for complying with HIPAA requirements.

Our plans to begin testing early in the year will allow electronic submitters enough time to thoroughly test and make any necessary adjustments to their systems prior to the October deadline.

Providers and/or vendors are encouraged to submit tests that reflect the true scope of their normal claims transmissions. For UB-92 providers, test files should include each type of bill that is routinely submitted.

Claims for each type of carrier normally sent (BlueCross BlueShield of Tennessee, BlueCare[®], WebMD/ENVOY, Riverbend Medicare) should also be included. HCFA-1500 providers should submit claim examples that reflect the nature of their practice, including examples for each type of carrier normally transmitted (BlueCross BlueShield of Tennessee, BlueCare, WebMD/ENVOY, Cigna Medicare, Xantus).

Software vendors may transmit tests with data from one of their clients. Once approved, all clients under the approved vendor will be considered tested and approved. We will not require each provider using the approved software to test with us.

BlueCross BlueShield of Tennessee will accept HIPAA testing certifications from nationally recognized testing agencies once the agency has successfully tested with us.

For technical questions, please contact the Electronic Commerce e-Business Service Center at (423) 755-5717 from 8 a.m. to 5:30 p.m. EST.

For More Information

BlueCross BlueShield of Tennessee will continue to provide information and updates on HIPAA to the provider community via:

- *BlueAlert* newsletter
- *Policy Review and News* (PRN) magazine
- HIPAA section of the Provider's page of our Web site – www.bcbst.com
- Provider letters
- Provider workshops

The following Internet links provide additional information on HIPAA:

U.S. Department of Health and Human Services - Administrative Simplification

This site provides background information on the Administrative Simplification portion of HIPAA including frequently asked questions on Privacy, Security, Transactions, and Code Sets.

<http://aspe.hhs.gov/admsimp/>

Office of Civil Rights

This site concentrates specifically on patient privacy, including patient consent.

<http://www.hhs.gov/ocr/hipaa/>

Washington Publishing Company

Free ANSI implementation guides may be downloaded from this site.

www.wpc-edi.com/HIPAA_40.asp

For More Information (Cont'd)

Workgroup for Electronic Data Interchange (WEDI)

WEDI works to improve health care through Electronic Commerce. This site features a glossary of HIPAA terms, a copy of the Health Insurance and Portability Act of 1996 and other related information.

<http://wedi.org>

National Uniform Claim Committee

Provider taxonomy and frequently asked questions on HIPAA Administrative Simplification are addressed on this site.

www.nucc.org

Southern HIPAA Administrative Regional Process (SHARP)

SHARP is a combined public and private workgroup to assist with regional HIPAA readiness.

<http://www.sharpworkgroup.com>

**Information provided in this document is based on regulations as of December 2001*

