HIPAA Desk Reference

April 2004
<table>
<thead>
<tr>
<th>Topic</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Addition of information on role-based access control</td>
</tr>
</tbody>
</table>
| Administrative Simplification             | Addition of information on national provider identifier  
Updated dates for publication of regulations, based on the semiannual regulatory agenda                                                            |
| Administrative Simplification Compliance Act| Addition of information regarding transmittal 44—confusion over end of CMS contingency plan versus requirements under ASCA                        |
| Authorization                              | Addition of HIPAA compliance tool—sample authorization form                                                                                          |
| Credentials/Certifications                 | New topic—Discusses the credentials offered by:  
- AHIMA  
- HIMSS  
- ISC2                                                                                                                                             |
| CMS                                       | Inserted information about CMS responsibility for the NPI                                                                                            |
| Companion Guides                          | Addition of “Sample Companion Guide” page                                                                                                                                 |
| Complaints/Grievances                      | Addition of “Complaints to the Government” section  
Cross reference to the “Enforcement” section                                                                                                        |
| Compliance Dates                          | Updated compliance dates for identifiers with information on the NPI                                                                              |
| Covered Entity                            | Added information from the CMS covered-entity decision tools online, as well as the CMS covered-entity flow charts                                         |
| Electronic Signatures                     | Addition of information on the AHIMA best practice standard for electronic signatures                                                               |
| Enforcement                               | Addition of information on submission of privacy complaints to OCR  
Addition of information on submission of T & CS complaints to CMS, through the ASET online system, or on paper |
| Health Plan Identifiers                   | Updated dates for release of regulations, based on the semiannual regulatory agenda                                                                    |
| Information Access Management             | Addition of information on role-based access control                                                                                                 |
| Marketing Under HIPAA                    | Addition of information from OCR frequently asked questions                                                                                           |
| Minimum Necessary                        | Addition of information on how role-based access control can help with the privacy rule minimum necessary standard                                    |
| Provider Identifiers                      | Completely revised topic, based on the new NPI final rule                                                                                             |
| Risk Analysis/Management                  | Addition of information on the NIST “Risk Management Guide for Information Technology Systems”                                                         |
| Security Incident Procedures              | Reorganized topic  
Addition of information on the NIST “Computer Security Incident Handling Guide”                                                                       |
| Training Requirements                     | Addition of information on educational opportunities from CMS and OCR                                                                                 |
| Transaction Standards                     | Addition of information on claims testing issues found by Medicare  
Updated dates for publication of claims attachment regulations                                                                                      |
| Appendix E                                | Revisions to list of medical and nonmedical code sets                                                                                                 |
Introduction

The new Updateable HIPAA Desk Reference is the most comprehensive HIPAA resource library offering a simplified solution to compliance with the Health Insurance Portability and Accountability Act. This all-in-one portable desk reference is ideal for the facility or physician practice looking for answers regarding HIPAA and its many components.

This book was written for the people who will have to live with HIPAA. It describes the provisions that will have the most impact on health care providers, and it explains the implications of many of those provisions in an everyday context.

Readers who require greater depth on, or up-to-the-minute developments affecting, particular aspects of HIPAA are directed throughout the book to specific sections of the regulations or government Web sites for current information. Ingenix, Inc., also offers a wide range of HIPAA materials in printed and electronic formats. A catalog of resources is available at www.ingenixonline.com.

How HIPAA Got to Be What It Is Today

HIPAA of 1996 was passed by Congress and enacted into law in August of 1996. Its original purpose was basically to enable Americans covered by group health plans to take their health care coverage with them from employer group to employer group—that's what the term “portability” refers to.

While portability is the primary subject of one section of HIPAA, however, it is a relatively small aspect of the overall legislation. In fact, portability is totally separate from—and unrelated to—the subject matter of this book, which is Title II of HIPAA. Title II consists of the so-called “administrative simplification provisions” governing privacy and security of health data and related subjects involving the transmission and processing of those data.

In the tradition of a great deal of federal legislation, HIPAA is lengthy, complicated, and confusing largely because lawmakers grafted many provisions onto it that have little or nothing to do with its name and original purpose. As it evolved, HIPAA grew larger and larger as Congress first added provisions to enhance federal efforts to combat fraud and abuse, and then adopted HIPAA as a vehicle for promoting the replacement of paper-based transactions with more efficient electronic transactions.

Again, this book focuses exclusively on the administrative simplification, or Title II, provisions of HIPAA. The term “HIPAA,” as used in this book, refers to the Title II provisions.

Bringing Order to Chaos?

In the pre-HIPAA era, individual health plans have been free to create and require compliance with their own proprietary systems and processes for submitting claims. One of HIPAA’s purposes is to replace the resulting non-system of paper-based transactions with a single, uniform set of standards for electronic transactions.

HIPAA’s supporters expect the adoption of uniform standards for transactions to yield significant savings over time for providers and other players in the health care system. The premise is simple: if all billing transactions use a single set of data elements, one set of rules for coding information, and universal standards for formatting and transmitting data, providers will no longer be required to keep track of each payer’s peculiar requirements. Therefore, they will no longer have to customize their information systems to support a wide variety of requirements.

Since the early 1960s, various organizations have worked to develop and promote the use of standard forms for billing and other common health care transactions. The uniform bill and uniform claim form were products of this effort.

In the 1980s, a number of industry groups started promoting the replacement of paper-based transactions with electronic transactions. Among the most prominent of these efforts was
system, its most direct impact will be felt by health care providers, health plans, and health care clearinghouses. This is the triumvirate that HIPAA refers to as the “covered entities.”

HIPAA also indirectly affects the business partners and business associates of the covered entities.

**Keeping Up with HIPAA**

However great the challenge of developing the several sets of HIPAA standards may have been, keeping them current will be that much more difficult. The standards described in this book, as well as the standards that have yet to be developed, will require constant revision to reflect changing needs.

In fact, the standards adopted by the secretary recognize the inevitability of change and include specific updating procedures. Before any new standards can go into effect, however, they must be adopted by the secretary in a formal rule published in the Federal Register.

The bottom line is that health care providers and others affected by the HIPAA standards will need to be alert for the issuance of revisions, particularly in the standards for transactions and coding of medical diagnoses and procedures. Since the updating of these standards is largely the responsibility of nongovernment organizations like associations of medical professionals that actually use the standards, change should reflect the real-world needs of providers, health plans, and others.

In addition to routine maintenance of the standards, covered entities should be on the alert for adoption of the HIPAA standards that are still on the drawing board. These include a standard for claims attachments, one for the uniform health plan identifier, and one for the uniform individual identifier. Additional details of civil and criminal penalties for noncompliance with HIPAA also have yet to be developed.

Beyond the routine maintenance of the standards, providers and other entities covered by HIPAA should be aware of legislative action that may add to, or alter, HIPAA’s requirements. Legislative action is particularly likely in the area of privacy protections, which remains a significant issue on the congressional agenda. The potential abuse of sensitive personal information and the damage that inappropriate disclosure of this information can cause continues to worry many consumers. It is likely that Congress will continue to tinker with privacy protections for many years to come.

**How to Use This Book**

The *Updateable HIPAA Desk Reference* provides organizations with a detailed guide to many of HIPAA’s most difficult issues. Given the rapidly changing regulatory environment, the updateable format provides an economical way to stay on top of the latest developments under HIPAA, without having to repurchase new reference products every quarter. By subscribing to updates, organizations continue to receive the most up-to-date regulatory information, compliance tips, and alerts to possible pitfalls. We also provide a special on-line feature, HIPAA Desk Reference On-line (www.hipaadeskreferenceonline.com), giving organizations access to the latest new articles, updated templates, and policy samples. The Ingenix HIPAA Action Alert allows organizations to receive e-mail alerts of proposed changes to the rules, release dates, and recent industry findings. This guide provides plain-English explanations of the laws, regulations, and guidance issued by the Department of Health and Human Services, Office for Civil Rights, the Centers for Medicare and Medicaid Services (CMS), the CMS Office of HIPAA standards, and other federal and state enforcement organizations.

**Organization**

This book is organized in a simple A-to-Z format, allowing the reader to quickly and easily search for a term or terms they need additional information on. At the beginning of each topic, the set of HIPAA regulations that topic is related to is listed, as well as the regulation citations where the information is found.

Helpful tools for compliance are found throughout the book in a sample format. There are sample policies and procedures, checklists, and many more tools for organizations to use. For customizable versions of these and many other HIPAA compliance tools, see the Ingenix HIPAA Tool Kit.
# Contents

Introduction ............................................................................................................... Introduction–1

Index ........................................................................................................................... Index–1

**A–C**

Access Control ........................................................................................................... 1–1
Access to Data ............................................................................................................. 1–3
Accounting for Disclosures ....................................................................................... 1–6
Accredited Standards Committee ............................................................................. 1–8
Addressable Versus Required .................................................................................. 1–9
Administrative Safeguards ......................................................................................... 1–12
Administrative Simplification .................................................................................... 1–14
Administrative Simplification Compliance Act ....................................................... 1–20
Affiliated Covered Entities ....................................................................................... 1–21
Amendments to PHI .................................................................................................. 1–22
ANSI .......................................................................................................................... 1–24
ASC X12N ................................................................................................................... 1–25
Audit Controls ............................................................................................................. 1–26
Authentication ............................................................................................................ 1–27
Authorization .............................................................................................................. 1–28
Business Associate ................................................................................................. 1–32
CMS ............................................................................................................................ 1–36
Code-Set Maintaining Organization ......................................................................... 1–37
Code Sets .................................................................................................................... 1–38
Companion Guides .................................................................................................... 1–44
Complaints/Grievances ............................................................................................ 1–46
Compliance Dates ...................................................................................................... 1–49
Consent ..................................................................................................................... 1–50
Contingency Plan ...................................................................................................... 1–52
Covered Entity ............................................................................................................ 1–55
Credentials/Certifications ......................................................................................... 1–58

**D–G**

Data Element .............................................................................................................. 2–1
Data Segment ............................................................................................................. 2–2
Decedents ................................................................................................................... 2–3
De-identified Information ......................................................................................... 2–4
Designated Record Set ............................................................................................. 2–5
Device and Media Controls ....................................................................................... 2–6
Direct Data Entry ....................................................................................................... 2–9
Direct Versus Indirect Treatment Relationship ....................................................... 2–10
Disclosure .................................................................................................................. 2–11
Documentation Requirements .................................................................................. 2–13
DSMO ........................................................................................................................ 2–14
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDI</td>
<td>2–15</td>
</tr>
<tr>
<td>Electronic Media</td>
<td>2–16</td>
</tr>
<tr>
<td>Electronic Signatures</td>
<td>2–16</td>
</tr>
<tr>
<td>Electronic Transactions</td>
<td>2–18</td>
</tr>
<tr>
<td>Employer Identifiers</td>
<td>2–19</td>
</tr>
<tr>
<td>Enforcement</td>
<td>2–20</td>
</tr>
<tr>
<td>Evaluation</td>
<td>2–28</td>
</tr>
<tr>
<td>Facility Access Controls</td>
<td>2–29</td>
</tr>
<tr>
<td>Fundraising Under HIPAA</td>
<td>2–32</td>
</tr>
<tr>
<td>Government Access to Information</td>
<td>2–34</td>
</tr>
<tr>
<td>Health Care</td>
<td>3–1</td>
</tr>
<tr>
<td>Health Care Clearinghouse</td>
<td>3–6</td>
</tr>
<tr>
<td>Health Care Operations</td>
<td>3–10</td>
</tr>
<tr>
<td>Health Care Provider</td>
<td>3–11</td>
</tr>
<tr>
<td>Health Information</td>
<td>3–14</td>
</tr>
<tr>
<td>Health Plan</td>
<td>3–15</td>
</tr>
<tr>
<td>Health Plan Identifiers</td>
<td>3–18</td>
</tr>
<tr>
<td>HHS</td>
<td>3–19</td>
</tr>
<tr>
<td>Hybrid Entity</td>
<td>3–23</td>
</tr>
<tr>
<td>Implementation Guides</td>
<td>3–24</td>
</tr>
<tr>
<td>Implementation Specifications</td>
<td>3–26</td>
</tr>
<tr>
<td>Incidental Disclosures</td>
<td>3–29</td>
</tr>
<tr>
<td>Individual Identifiers</td>
<td>3–31</td>
</tr>
<tr>
<td>Information Access Management</td>
<td>3–33</td>
</tr>
<tr>
<td>Information System Activity Review</td>
<td>3–35</td>
</tr>
<tr>
<td>Integrity</td>
<td>3–36</td>
</tr>
<tr>
<td>Limited Data Set</td>
<td>3–37</td>
</tr>
<tr>
<td>Loop</td>
<td>3–40</td>
</tr>
<tr>
<td>Marketing Under HIPAA</td>
<td>3–42</td>
</tr>
<tr>
<td>Media Re-Use</td>
<td>3–46</td>
</tr>
<tr>
<td>Minimum Necessary</td>
<td>3–48</td>
</tr>
<tr>
<td>Mitigation</td>
<td>3–51</td>
</tr>
<tr>
<td>NCPDP Format</td>
<td>4–1</td>
</tr>
<tr>
<td>NDC</td>
<td>4–4</td>
</tr>
<tr>
<td>Notice of Privacy Practices</td>
<td>4–5</td>
</tr>
<tr>
<td>Organized Health Care Arrangement</td>
<td>4–11</td>
</tr>
<tr>
<td>Paper Transactions</td>
<td>4–12</td>
</tr>
<tr>
<td>Payment</td>
<td>4–15</td>
</tr>
<tr>
<td>Personal Representatives</td>
<td>4–18</td>
</tr>
<tr>
<td>Physical Safeguards</td>
<td>4–20</td>
</tr>
<tr>
<td>Pre-emption</td>
<td>4–21</td>
</tr>
<tr>
<td>Privacy Official</td>
<td>4–23</td>
</tr>
</tbody>
</table>
Access Control

Security—45 CFR §164.312(a)(1)

Under the technical safeguards in the security rule, there is a standard for access control. Within this topic, we will discuss this standard, including:

- Definition of access control
- Required implementation specifications
- Unique user identification
- Emergency access procedures
- Addressable implementation specifications
- Encryption and decryption of personal health information
- Role-based access control

Definition of Access Control
The access control standard pertains to technical access to system information, as opposed to physical access to workstations and computer terminals. This standard requires all covered entities to implement technical policies and procedures for electronic information systems that house electronic protected health information. These policies and procedures govern the organization's control over access to the electronic PHI, allowing access only to those persons or software programs that have been granted access rights through the information access management standard that is part of the administrative safeguards. As with all other security standards, there are several implementation standards, some of which are considered required and some of which are considered addressable.

Required Implementation Specifications
There are a number of required implementation specifications that a covered entity must employ under the access control portion of the security regulation.

Unique user identification—Each entity must assign unique user names or numbers for identifying or tracking user identity. In most cases, this requirement means that organizations must implement operating systems that support user IDs and passwords and/or incorporate user IDs and passwords into the applications that process PHI.

People who use the Internet are familiar with the core technologies of access control. All Internet service providers give their customers a user name and require a secure password before making the connection. Many Web sites require a user name and password to restrict usage to registered users.

There is a distinction between an operating system that employs user IDs and passwords, and an application that employs user identification. Network operating systems such as Microsoft Windows 2000 or XP and Novell NetWare require a user to log on to the network using a unique user ID and password. The operating system may then restrict the ability of a user to use specific applications or access specific information based on the permissions that have been granted that user.

This same capability can be implemented by individual applications. An accounting application may, for example, require a user to log on with a unique user ID and password—even if the operating system does not. Both approaches are means of achieving the same goal: restricting use of a specific application and/or database only to authorized users. And both approaches may be used simultaneously. A user might log on to an organization's network and also be required to use another user ID and password to access specific information or applications.

Emergency access procedure—Each entity must establish and be able to implement procedures for obtaining necessary electronic PHI during an emergency.
<table>
<thead>
<tr>
<th>Type of Safeguard</th>
<th>Security Standard</th>
<th>Implementation Specification</th>
<th>Required (R) or Addressable (A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative</td>
<td>Security management process</td>
<td>Risk analysis</td>
<td>R</td>
</tr>
<tr>
<td>Administrative</td>
<td>Security management process</td>
<td>Risk management</td>
<td>R</td>
</tr>
<tr>
<td>Administrative</td>
<td>Security management process</td>
<td>Sanction policy</td>
<td>R</td>
</tr>
<tr>
<td>Administrative</td>
<td>Security management process</td>
<td>Information system activity review</td>
<td>R</td>
</tr>
<tr>
<td>Administrative</td>
<td>Assigned security responsibility</td>
<td>Same as standard</td>
<td>R</td>
</tr>
<tr>
<td>Administrative</td>
<td>Workforce security</td>
<td>Authorization and/or supervision</td>
<td>A</td>
</tr>
<tr>
<td>Administrative</td>
<td>Workforce security</td>
<td>Workforce clearance procedure</td>
<td>A</td>
</tr>
<tr>
<td>Administrative</td>
<td>Workforce security</td>
<td>Termination procedures</td>
<td>A</td>
</tr>
<tr>
<td>Administrative</td>
<td>Information access management</td>
<td>Isolating health care clearinghouse functions</td>
<td>R</td>
</tr>
<tr>
<td>Administrative</td>
<td>Information access management</td>
<td>Access authorization</td>
<td>A</td>
</tr>
<tr>
<td>Administrative</td>
<td>Information access management</td>
<td>Access establishment and modification</td>
<td>A</td>
</tr>
<tr>
<td>Administrative</td>
<td>Security awareness and training</td>
<td>Security reminders</td>
<td>A</td>
</tr>
<tr>
<td>Administrative</td>
<td>Security awareness and training</td>
<td>Protection from malicious software</td>
<td>A</td>
</tr>
<tr>
<td>Administrative</td>
<td>Security awareness and training</td>
<td>Log-in monitoring</td>
<td>A</td>
</tr>
<tr>
<td>Administrative</td>
<td>Security awareness and training</td>
<td>Password management</td>
<td>A</td>
</tr>
<tr>
<td>Administrative</td>
<td>Security incident procedures</td>
<td>Response and reporting</td>
<td>R</td>
</tr>
<tr>
<td>Administrative</td>
<td>Contingency plan</td>
<td>Data backup plan</td>
<td>R</td>
</tr>
<tr>
<td>Administrative</td>
<td>Contingency plan</td>
<td>Disaster recovery plan</td>
<td>R</td>
</tr>
<tr>
<td>Administrative</td>
<td>Contingency plan</td>
<td>Emergency mode operation plan</td>
<td>R</td>
</tr>
<tr>
<td>Administrative</td>
<td>Contingency plan</td>
<td>Testing and revision procedure</td>
<td>A</td>
</tr>
<tr>
<td>Administrative</td>
<td>Contingency plan</td>
<td>Applications and data criticality analysis</td>
<td>A</td>
</tr>
<tr>
<td>Administrative</td>
<td>Evaluation</td>
<td>Same as standard</td>
<td>R</td>
</tr>
<tr>
<td>Administrative</td>
<td>Business associate contracts and other arrangement</td>
<td>Written contract or other arrangement</td>
<td>R</td>
</tr>
<tr>
<td>Physical</td>
<td>Facility access controls</td>
<td>Contingency operations</td>
<td>A</td>
</tr>
<tr>
<td>Physical</td>
<td>Facility access controls</td>
<td>Facility security plan</td>
<td>A</td>
</tr>
<tr>
<td>Physical</td>
<td>Facility access controls</td>
<td>Access control and validation procedures</td>
<td>A</td>
</tr>
<tr>
<td>Physical</td>
<td>Facility access controls</td>
<td>Maintenance records</td>
<td>A</td>
</tr>
<tr>
<td>Physical</td>
<td>Workstation use</td>
<td>Same as standard</td>
<td>R</td>
</tr>
<tr>
<td>Physical</td>
<td>Workstation security</td>
<td>Same as standard</td>
<td>R</td>
</tr>
<tr>
<td>Physical</td>
<td>Device and media controls</td>
<td>Disposal</td>
<td>R</td>
</tr>
<tr>
<td>Physical</td>
<td>Device and media controls</td>
<td>Media re-use</td>
<td>R</td>
</tr>
<tr>
<td>Physical</td>
<td>Device and media controls</td>
<td>Accountability</td>
<td>A</td>
</tr>
<tr>
<td>Physical</td>
<td>Device and media controls</td>
<td>Data backup and storage</td>
<td>A</td>
</tr>
<tr>
<td>Technical</td>
<td>Access control</td>
<td>Unique user ID</td>
<td>R</td>
</tr>
</tbody>
</table>
Data Element

Transactions and Code Sets—45 CFR §162.103

Within the standards for electronic transactions, there are many different pieces of information that must be compiled to create the final electronic submission.

In this section, we will discuss the following:

- Definition of a data element
- Data element summary

Definition of a Data Element

The data element is the smallest informational component within a transaction made standard by the transaction standards regulations. Data elements can be compared with the words in a sentence. In this analogy, the sentence would be the data segment.

In many instances a single letter or number can be a data element, but some data elements use scores of characters. Many data elements require that codes be entered. Combinations of numbers or letters that identify a medical condition or that report the identification number of a provider are examples of codes. In total, the HIPAA required transactions use 40 different external code sets, but no single transaction uses all 40. Ordinary text or numbers also appear as data elements. For example, the name of a patient is written as it would appear in any document and so is the dollar value of a service being billed.

Data Element Summary

The implementation guides display information about each data element using the same format, called the element summary. In general, there are seven descriptors provided for each data element. In the above example, the seven descriptors are the following:

- Required—Notes whether the element must be reported
- Reference description (REF.DES)—The short or abbreviated name of the element
- Data element number—A number assigned to this element, found in appendix E, “Data Element Name Index,” found in all of the guides
- Name—The full name of the element
- M—Indicates that this element is required. The implementation guides are based upon earlier X12N guides for health care. In the non-HIPAA guides, “M” means mandatory. “Required” and “mandatory” have the same meaning, but the terms “optional” and “situational” are not the same. Situational actually means required if a specified business condition exists. In the non-HIPAA guides, optional means the sender may decide when to include the element. For practical purposes, these designations, such as “M,” may be ignored. The highlighted “required” text is the authority on whether a data element must be used or not.
- ID—Indicates that this element is an identifier

<table>
<thead>
<tr>
<th>ELEMENT SUMMARY</th>
</tr>
</thead>
<tbody>
<tr>
<td>REFERENCE IDENTIFICATION QUALIFIER</td>
</tr>
<tr>
<td>128 REF01</td>
</tr>
<tr>
<td>NAME</td>
</tr>
<tr>
<td>CODE QUALIFYING THE REFERENCE IDENTIFICATION</td>
</tr>
<tr>
<td>M ID 2/3</td>
</tr>
<tr>
<td>FUNCTIONAL CATEGORY</td>
</tr>
</tbody>
</table>

A data element generally has six attributes. In the above example, “required” and “M” (or mandatory) have the same meaning.
HIPAA Compliance Tool

Following is a compliance checklist to help an organization develop a compliance work plan regarding the device and media controls standard:

Device and Media Controls

**Standard:** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of a facility, and the movement of these items within the facility.

**Disposal**

**Required implementation specification:** Implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored.

- **Yes**  
  The organization has established policies and procedures to purge security information and PHI from computer equipment and storage media before disposal of equipment and media.

- **Yes**  
  Periodic inspections confirm that procedures are followed to purge PHI from storage media before disposal.

- **Yes**  
  The organization confirms that information that could be used to defeat security safeguards such as user IDs and password lists) has been purged from computer equipment before disposal.

**Action plan for security standard compliance:**

_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________

**Media Re-use**

**Required implementation specification:** Implement procedures for removing PHI from electronic media before the media are made available for re-use.

- **Yes**  
  The organization has established policies and procedures to prevent the re-use of storage media from inadvertently compromising the security of PHI.

- **Yes**  
  The organization has established procedures to ensure that all PHI is completely removed from media that are used to create backup data sets before the media are re-used.

**Action plan for security standard compliance:**

_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
Health Care

General—45 CFR §160.103

The definition of “health care” in the HIPAA regulations is important to determining whether a provider is considered a covered entity. Health care providers are quite simply those that furnish, bills, or are paid, for health care.

Within this topic, the following will be discussed:

- Health care defined
- Other government definitions
- Other services
- Helpful questions and answers

Health Care Defined

Health care is defined as “care, services, or supplies related to the health of an individual.” This includes, but is not limited to:

- “Preventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure of the body”
- “Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription”

Almost every health-related service provided to individuals is included in this very general definition of health care. For additional information on the definition of health care provider, see that section within this book.

Other Government Definitions

An often confusing point about government regulations is that their definitions vary based on the agency or agencies responsible for writing the regulation. For example, the Medicare Carriers Manual and Intermediary Manual do not define “health care” per se. The term they use is “medical and other health services” and comes from the Social Security Act, section 1861, as follows.

The term “medical and other health services” means any of the following items or services:

1. physicians’ services;
2. (A) services and supplies (including drugs and biologicals which are not usually self-administered by the patient) furnished as an incident to a physician’s professional service, of kinds which are commonly furnished in physicians’ offices and are commonly either rendered without charge or included in the physicians’ bills;
   (B) hospital services (including drugs and biologicals which are not usually self-administered by the patient) incident to physicians’ services rendered to outpatients and partial hospitalization services incident to such services;
   (C) diagnostic services which are—
      (i) furnished to an individual as an outpatient by a hospital or by others under arrangements with them made by a hospital, and
      (ii) ordinarily furnished by such hospital (or by others under such arrangements) to its outpatients for the purpose of diagnostic study;
   (D) outpatient physical therapy services and outpatient occupational therapy services;
   (E) rural health clinic services and federally qualified health center services;
Health Care Clearinghouse
General—45 CFR §160.103

Under the HIPAA regulations, there are three main types of covered entities: health plans, health care clearinghouses, and health care providers. This section discusses the definition of a health care clearinghouse.

Within this topic, the following will be discussed:

■ Clearinghouse defined
■ Frequently asked questions

Clearinghouse Defined

Many providers in today’s complex billing environment use health care clearinghouses. They can be public or private entities, such as billing services, repricing companies, community health management information systems, community health information systems, and “value-added” networks and switches. They must perform one of the following functions:

■ Process or facilitate the processing of health information received from another entity in a nonstandard format into standard transactions
■ Receive standard transactions from another entity and process or facilitate the processing of health information into a format the receiving entity can understand (nonstandard format)

In short, health care clearinghouses make nonstandard data fit the standards. Many entities not traditionally seen as clearinghouses perform functions that fit within these parameters. Performance of these functions means that they are considered health care clearinghouses for purposes of the regulations and must meet all requirements met by other clearinghouses.

Frequently Asked Questions

The CMS Web site offers some answers to frequently asked questions, to assist covered entities in making decisions regarding HIPAA compliance. Following are a few of those FAQs related to health care clearinghouses.

Question: A provider conducts no transactions electronically for which the Secretary of Health and Human Services has adopted a standard. Instead, the provider sends paper claims directly to a health plan, and the health plan transforms the paper claims into electronic formats in order to process and pay the claim. In this situation, is the provider a covered entity under HIPAA?

Answer: No. Most, if not all, health plans transform the paper claims they receive into electronic formats for processing. The health plans do this for their own convenience, not on behalf of the providers submitting the paper claims.

The provider described in the question above would be a covered entity if its paper claims were submitted to a health care clearinghouse or a billing service, and, on behalf of the provider, the health care clearinghouse or the billing service transformed them into standard transactions and transmitted them to a health plan.

Question: When would a billing service be considered a health care clearinghouse?

Answer: Many health care providers outsource their claims management functions to billing services. Billing services may provide a wide range of back office services to health care providers including coding, data entry, charge entry, insurance claims submissions, posting receipts, filing secondary insurance claims, balance billing for coinsurance and deductibles, managing accounts receivables, and other practice management services. Sometimes, a billing service may convert a paper claim, received from a health care provider, to an electronic claim, and submit the electronic claim to a health plan as an electronic transaction. In such cases, a billing service may need to aggregate information necessary for claim submission from various sources such as charge...
NCPDP Format

Transactions and Code Sets—45 CFR §162.1102

The National Council for Prescription Drug Programs is the ANSI-accredited standards development organization that has developed the standards for electronic transactions for retail pharmacies. Effective October 16, 2003, its NCPDP Telecommunication Standard Implementation Guide, version 5.1 and its implementation specifications are the standard for transactions between retail pharmacies and other covered entities. Prior to October 16, 2003, there was an earlier version of the same standard used.

Similar to the ASC X12N standards, there are specific data elements detailed in the implementation guides, which are available on the NCPDP Web site at http://www.ncpdp.org. The required guides are as follows:

■ NCPDP Telecommunication Standard Implementation Guide, version 5.1, September 1999

Although this standard is typically used only by retail pharmacies, health care clearinghouses, and insurers paying drug claims, there are some uses in the hospital and physician settings as well. If a hospital or physician is submitting claims for certain drugs to the regional DMERC carriers, those claims must be submitted in NCPDP format. Certified DMERC suppliers must be aware of the transaction standard requirements for the items they are billing.

Details on the Standards
The NCPDP Web site, as mentioned above, gives a great deal of information to the public about the standards as named in the standards for electronic transactions regulations. Following are excerpts from an NCPDP document provided for general information on implementation of the telecommunication standard on their Web site.

Implementation of the Telecommunication or Batch Standard
NCPDP has created documentation to assist in the implementation of the HIPAA-named NCPDP transactions. For the most comprehensive information, it is suggested to become a member of NCPDP, to receive bi-weekly email updates with news of HIPAA and the organization, to receive notification of updates on the Web site, and to be involved in work group updates and activities.

NCPDP Web Site
The NCPDP Web site (www.ncpdp.org) has many areas devoted to public knowledge. There is also a section for members only. The Members section contains the standards documents available for download, and information from each of the work groups of activities currently underway.

NCPDP has provided HIPAA information in the public section of the NCPDP Web site. This information is updated whenever there is news to report, so check frequently. Also on the main page of the Web site, there is an “Updates” section which lists changes to the Web site at a glance. The public HIPAA menu item has submenus, for various HIPAA topics.

NCPDP also provides a HIPAA informational section for Members only. This section is a submenu item under the “Government Related” section.

Final Rule Information on Electronic Transactions as It Relates to the Pharmacy Industry
For a general overview of the transactions and code sets named in HIPAA, as it relates to pharmacy, the document “Final Rule Information on Electronic Transactions as It Relates to the Pharmacy Industry” is available at http://www.ncpdp.org/frame_news_hipaa_trans.htm

©2004 Ingenix, Inc.  April 04 4–1
Notice of Privacy Practices

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.

Uses and Disclosures

Treatment. Your health information may be used by staff members or disclosed to other health care professionals for the purpose of evaluating your health, diagnosing medical conditions, and providing treatment. For example, results of laboratory tests and procedures will be available in your medical record to all health professionals who may provide treatment or who may be consulted by staff members.

Payment. Your health information may be used to seek payment from your health plan, from other sources of coverage such as an automobile insurer, or from credit card companies that you may use to pay for services. For example, your health plan may request and receive information on dates of service, the services provided, and the medical condition being treated.

Health care operations. Your health information may be used as necessary to support the day-to-day activities and management of [name of organization]. For example, information on the services you received may be used to support budgeting and financial reporting, and activities to evaluate and promote quality.

Law enforcement. Your health information may be disclosed to law enforcement agencies to support government audits and inspections, to facilitate law-enforcement investigations, and to comply with government-mandated reporting.

Public health reporting. Your health information may be disclosed to public health agencies as required by law. For example, we are required to report certain communicable diseases to the state's public health department.

Other uses and disclosures require your authorization. Disclosure of your health information or its use for any purpose other than those listed above requires your specific written authorization. If you change your mind after authorizing a use or disclosure of your information you may submit a written revocation of the authorization. However, your decision to revoke the authorization will not affect or undo any use or disclosure of information that occurred before you notified us of your decision to revoke your authorization.

Additional Uses of Information

Appointment reminders. Your health information will be used by our staff to send you appointment reminders.

Information about treatments. Your health information may be used to send you information that you may find interesting on the treatment and management of your medical condition. We may also send you information describing other health-related products and services that we believe may interest you.

Fundraising. Unless you request us not to, we will use your name and address to support our fund-raising efforts. If you do not want to participate in fund-raising efforts, please check off the following box.

- Please do not use my information for fund-raising purposes.
Technical Safeguards

Security—45 CFR §164.312

The intent of this regulation is to provide standards for the protection of electronic protected health information in accordance with the act. In order to do this, covered entities are required to implement administrative, physical, and technical safeguards.

Within this topic the following will be discussed:
- Definition of technical safeguards
- Purpose of technical safeguards
- Implementation of technical safeguards

Definition of Technical Safeguards
The security regulations define technical safeguards as "the technology and the policy and procedures for its use that protect electronic protected health information (PHI) and control access to it."

Purpose of Technical Safeguards
The technical safeguards are in place to govern the technical access to electronic PHI via computer or electronic media, as well as to verify the identity of those trying to access that information. It also governs technology auditing procedures, and helps to protect the integrity of the information both in house and bring transmitted.

Implementation of Technical Safeguards
This is a section of the security regulations where input is needed from information systems or information technology staff. They will be the experts on what levels of security can be built into your systems, what types of audit logs can be generated, what types of authentication can be built in, and what levels of security can be put on electronic transmissions. Technical experts will be key to accomplishing any level of compliance with the technical safeguards in the security regulations.

The technical safeguards as given in the final security rule are shown in the table below. Each of these standards will be discussed in further detail in its own section of this book, with details on the required and addressable implementation specifications for each.

<table>
<thead>
<tr>
<th>Standards</th>
<th>Sections</th>
<th>Implementation Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Controls</td>
<td>164.312(a)(1)</td>
<td>Unique user identification (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Emergency access procedure (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Automatic Logoff (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encryption and decryption (A)</td>
</tr>
<tr>
<td>Audit Controls</td>
<td>164.312(b)</td>
<td>(R)</td>
</tr>
<tr>
<td>Integrity</td>
<td>164.312(c)(1)</td>
<td>Mechanism to authenticate electronic protected health information (A)</td>
</tr>
<tr>
<td>Person or Entity Authentication</td>
<td>164.312(d)</td>
<td>(R)</td>
</tr>
<tr>
<td>Transmission Security</td>
<td>164.312(e)(1)</td>
<td>Integrity controls (A) Encryption (A)</td>
</tr>
</tbody>
</table>
OCR Training
The Office for Civil Rights also offers educational materials through its Web site at http://www.hhs.gov/ocr/hipaa/. Some of the educational information found on the site is:

- OCR Powerpoint presentations from HHS’s National Conferences on the HIPAA Privacy Rule, February/March 2003 in San Diego, Atlanta, New York, and Chicago
- OCR cautions about misleading marketing on HIPAA training
- Guidance for writing plain-language notices
- HHS’s National Institute of Health’s “Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule”
- Privacy guidance about authorizations for research and institutional review boards
- OCR summary of HIPAA privacy rule
- Health information privacy frequently asked questions (FAQs)
- How to file a health information privacy complaint with the office for civil rights
- The Centers for Disease Control and Prevention (CDC) guidance on the privacy rule
- OCR guidance explaining significant aspects of the privacy rule, December 4, 2002
- Am I a covered entity? HHS helps answer this question with a new, easy-to-use questionnaire-and-answer decision tool
- “Standards for Privacy of Individually Identifiable Health Information - Final Changes to Rule,” HHS fact sheet, August 9, 2002
- Sample business associate contract provisions
- Keep watching the OCR Web site, as it regularly updates the educational options.

HIPAA Compliance Tool
Following is a helpful checklist to help organizations develop and document a security training program:

Security Awareness and Training
Standard: Implement a security awareness and training program for all members of the organization’s workforce (including management).

☐ Yes  ☐ No  A security awareness and training program has been developed for the medical practice.

Describe the methods used by the awareness and training program (e.g., PowerPoint presentations, off-site training, written materials, etc.):

____________________________________________________________________________
____________________________________________________________________________

The training program covers:

☐ Yes  ☐ No  The definition of security (availability, integrity, confidentiality)
☐ Yes  ☐ No  Threats to security (natural, human, and environmental)
☐ Yes  ☐ No  Methods of safeguarding security
☐ Yes  ☐ No  Security features of the organization’s information system and applications
☐ Yes  ☐ No  Use of major applications
☐ Yes  ☐ No  Policies on installation and configuration of software
☐ Yes  ☐ No  Controls on access to information
Appendix B—HIPAA Glossary

Contents
Part I, “HIPAA Glossary and Acronyms” gives general definitions and explanations of HIPAA-related terms and acronyms.

Part II “Consolidated HIPAA Administrative Simplification Final Rule Definitions” shows all definitions included in the final HIPAA administrative simplification rules as of February 20, 2003.

Please note that whenever a definition occurs in both part I and part II, the part II entry will be the more legally compelling one.

Resources
WEDI, Author ZonOwen, www.wedi.org, updated by Ingenix, Inc.

Part I. HIPAA Glossary and Acronyms
AAHomecare. See the American Association for Homecare.

Accredited Standards Committee (ASC). An organization that has been accredited by ANSI for the development of American National Standards.

ACG. Ambulatory care group.

ACH. See automated clearinghouse.

ADA. See the American Dental Association.

ADG. Ambulatory diagnostic group.

Administrative code sets. Code sets that characterize a general business situation, rather than a medical condition or service. Under HIPAA, these are sometimes referred to as nonclinical or non-medical code sets. Compare to medical code sets.

Administrative services only (ASO). An arrangement whereby a self-insured entity contracts with a third-party administrator (TPA) to administer a health plan.

Administrative simplification (A/S). Title II, Subtitle F of HIPAA, which gives HHS the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable health care information. This is also the name of Title II, Subtitle F, Part C of HIPAA.

AFEHCT. See the Association for Electronic Health Care Transactions.

AHA. See the American Hospital Association.

AHIMA. See the American Health Information Management Association.

AMA. See the American Medical Association.

Ambulatory payment classification (APC). A payment type for outpatient prospective payment system (OPPS) claims.

Amendment. See Amendments and corrections.

Amendments and corrections. In the final privacy rule, an amendment to a record would indicate that the data are in dispute while retaining the original information, while a correction to a record would alter or replace the original record.

American Association for Homecare (AAHomecare). An industry association for the home care industry, including home IV therapy, home medical services and manufacturers, and home health providers. AAHomecare was created through the merger of the Health Industry Distributors Association’s Home Care Division (HIDA Home Care), the Home Health Services and Staffing Association (HHSSA), and the National Association for Medical Equipment Services ( NAMES).

American Dental Association (ADA). A professional organization for dentists. The ADA maintains a hardcopy dental claim form and the associated claim submission specifications, and
Compliance date means the date by which a covered entity must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.

Covered entity means:
(1) A health plan.
(2) A health care clearinghouse.
(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Disclosure means the release, transfer, provision of, access to, or divulging on any other manner of information outside the entity holding the information.

Electronic media means:
(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private network, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Electronic protected health information means information that comes within paragraphs (1)(i) or (1)(ii) of the definition of protected health information as specified in this section.

Group health plan (also see definition of health plan in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:
(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or
(2) Is administered by an entity other than the employer that established and maintains the plan.

HCFA stands for Health Care Financing Administration within the Department of Health and Human Services. DHHS stands for the Department of Health and Human Services.

Health care means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:
(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and “value-added” networks and switches, that does either of the following functions:
(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42
The following table is the “Security Standards Matrix” from the “final security rule” printed in the Federal Register, February 20, 2003.

<table>
<thead>
<tr>
<th>Administrative Safeguards</th>
<th>Implementation Specifications (R=Required, (A)=Addressable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management Process . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>164.308(a)(1) Risk Analysis (R)</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>Risk Management (R)</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>Security Policy (R)</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>Information System Activity Review (R)</td>
</tr>
<tr>
<td>Assigned Security Responsibility . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>164.308(a)(2) (R)</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>Authorization and/or Supervision (A)</td>
</tr>
<tr>
<td>Workforce Security . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>164.308(a)(3) (A)</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>Workforce Clearance Procedure</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>Transition Procedures (A)</td>
</tr>
<tr>
<td>Information Access Management . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>164.308(a)(4) (R)</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>Identity Validation Function (B)</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>Access Authentication (A)</td>
</tr>
<tr>
<td>Security Awareness and Training . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>164.308(a)(5) (A)</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>Access Establishment and Maintenance (A)</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>Security Reminders (A)</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>Password Account Lockout (A)</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>Login Monitoring (A)</td>
</tr>
<tr>
<td>Security Incident Response . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>164.308(a)(6) (R)</td>
</tr>
<tr>
<td>Contingency Plan . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>164.308(a)(7) (R)</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>Disaster Recovery Plan (R)</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>Business Continuity Plan (R)</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>Testing and Evaluation Plan (A)</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>Applications and Data Criticality Analysis (A)</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>(R)</td>
</tr>
<tr>
<td>Evaluation . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>164.308(a)(8) (R)</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
<td>Written Contract or Other Arrangement (R)</td>
</tr>
<tr>
<td>Business Associate Contracts and Other Arrangements . . . . . . . . . . . . . . . . .</td>
<td>164.308(b)(1) (R)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Physical Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility Access Controls . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
</tr>
<tr>
<td>Workstation Use . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
</tr>
<tr>
<td>Device and Media Controls . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technical Safeguards (see §164.312)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
</tr>
<tr>
<td>Passwords . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
</tr>
<tr>
<td>Security Authentication . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
</tr>
<tr>
<td>. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .</td>
</tr>
</tbody>
</table>
# Appendix D—HIPAA Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADA</td>
<td>American Dental Association</td>
</tr>
<tr>
<td>AHIMA</td>
<td>American Health Information Management Association</td>
</tr>
<tr>
<td>AMIA</td>
<td>American Medical Informatics Association</td>
</tr>
<tr>
<td>ANSI</td>
<td>American National Standards Institute</td>
</tr>
<tr>
<td>ASTM</td>
<td>American Society for Testing and Materials</td>
</tr>
<tr>
<td>ASC</td>
<td>Accredited Standards Committee</td>
</tr>
<tr>
<td>BA</td>
<td>Business associate</td>
</tr>
<tr>
<td>BRA</td>
<td>Balanced Budget Amendment</td>
</tr>
<tr>
<td>CDC</td>
<td>Centers for Disease Control and Prevention</td>
</tr>
<tr>
<td>CFR</td>
<td>Code of Federal Regulations</td>
</tr>
<tr>
<td>CHIM</td>
<td>Center for Healthcare Information Management</td>
</tr>
<tr>
<td>CHIME</td>
<td>College of Healthcare Information Management Executives</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief information officer</td>
</tr>
<tr>
<td>CISO</td>
<td>Chief information security officer</td>
</tr>
<tr>
<td>CMS</td>
<td>Centers for Medicare and Medicaid Services</td>
</tr>
<tr>
<td>CPRI</td>
<td>Computer-Based Patient Record Institute</td>
</tr>
<tr>
<td>HHS</td>
<td>Department of Health and Human Services</td>
</tr>
<tr>
<td>DISA</td>
<td>Data Interchange Standards Association</td>
</tr>
<tr>
<td>EDI</td>
<td>Electronic data interchange</td>
</tr>
<tr>
<td>EHNAC</td>
<td>Electronic Healthcare Network Accreditation Commission</td>
</tr>
<tr>
<td>EIN</td>
<td>Employer identification number</td>
</tr>
<tr>
<td>FERPA</td>
<td>Family Educational Rights and Privacy Act</td>
</tr>
<tr>
<td>GLB</td>
<td>The Gramm-Leach-Bliley Act</td>
</tr>
<tr>
<td>HIC</td>
<td>Health information committee</td>
</tr>
<tr>
<td>HIM</td>
<td>Health information management</td>
</tr>
<tr>
<td>HIMSS</td>
<td>Healthcare Information and Management Systems Society</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act of 1996</td>
</tr>
<tr>
<td>HL7</td>
<td>Health Level Seven</td>
</tr>
<tr>
<td>IIHI</td>
<td>Individually identifiable health information</td>
</tr>
<tr>
<td>NCPDP</td>
<td>National Council for Prescription Drug Programs</td>
</tr>
<tr>
<td>NCQA</td>
<td>National Committee for Quality Assurance</td>
</tr>
<tr>
<td>NCHS</td>
<td>National Center for Health Statistics</td>
</tr>
<tr>
<td>NIH</td>
<td>National Institutes of Health</td>
</tr>
<tr>
<td>NPI</td>
<td>National provider identifier</td>
</tr>
<tr>
<td>NPRM</td>
<td>Notice of proposed rule making</td>
</tr>
<tr>
<td>NPS</td>
<td>National Provider System</td>
</tr>
<tr>
<td>NUBC</td>
<td>National Uniform Billing Committee</td>
</tr>
<tr>
<td>NUCCHIC</td>
<td>National Uniform Claim Committee</td>
</tr>
<tr>
<td>OCR</td>
<td>Office for Civil Rights</td>
</tr>
<tr>
<td>OIG</td>
<td>Office of Inspector General</td>
</tr>
<tr>
<td>PAYERID</td>
<td>Payer identification number</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal digital assistant</td>
</tr>
<tr>
<td>PHI</td>
<td>Protected health information</td>
</tr>
<tr>
<td>SDO</td>
<td>Standards development organization</td>
</tr>
<tr>
<td>SSN</td>
<td>Social Security number</td>
</tr>
<tr>
<td>TPO</td>
<td>Treatment, payment, or health care operations</td>
</tr>
<tr>
<td>UHI</td>
<td>Unique health identifier</td>
</tr>
<tr>
<td>WC</td>
<td>Workers’ compensation</td>
</tr>
<tr>
<td>WEDI</td>
<td>Workgroup for Electronic Data Interchange</td>
</tr>
<tr>
<td>X12N</td>
<td>ANSI Accredited Standards Committee’s EDI Subcommittee on Insurance Standards</td>
</tr>
</tbody>
</table>
# Appendix E—Table of Medical and Nonmedical Code Sets

The following table is the “Table of Medical and Nonmedical Code Sets.”

## MEDICAL CODES

<table>
<thead>
<tr>
<th>Ref. Code</th>
<th>Code Set Name</th>
<th>Available From</th>
<th>Status</th>
<th>(All URLs and costs are subject to change.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>131</td>
<td>ICD-9-CM Used in the 837I, 837P, 835, 276/277, 270/271</td>
<td>U.S. National Center for Health Statistics</td>
<td>Unrestricted Access/Available for Purchase</td>
<td><strong>Description:</strong> The International Classification of Diseases, 9th Revision, Clinical Modification is the classification system for reporting diseases, injuries, impairments, other health problems and manifestations, as well as the causes of such injuries and impairments under Volumes 1 and 2. Also, hospital inpatient procedures are reported using Volume 3. <a href="http://www.cdc.gov/nchs/about/otheract/icd9/abticd9.htm">http://www.cdc.gov/nchs/about/otheract/icd9/abticd9.htm</a> or <a href="http://cms.hhs.gov/providers/pufdownload/">http://cms.hhs.gov/providers/pufdownload/</a> <strong>Cost:</strong> Free online. <strong>Note:</strong> Currently, psychiatric disorders would be defined by this code set, but there are debates about using ICD-10 or the DSM-IV instead in future revisions. Additionally, it is likely that ICD-10-CM will be adopted in the near future. This code set is also available from Ingenix. Call 1-800-INGENIX (464-3649).</td>
</tr>
<tr>
<td>Ref. Code</td>
<td>Code Set Name</td>
<td>Available From</td>
<td>Status</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>---------------</td>
<td>----------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>307</td>
<td>National Association of Boards of Pharmacy Number</td>
<td>National Council for Prescription Drug Programs (NCPDP)</td>
<td>Available for Purchase</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Used in the 837I, 835, 270/271</td>
<td></td>
<td>Description: The NCPDP provider number assigned to pharmacies.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="http://www.ncpdp.org/main_frame.htm">http://www.ncpdp.org/main_frame.htm</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cost: Single Media Purchase, one master $2,000 (per media) or $1,000 for subscribers. (Or call the pharmacy.)</td>
<td></td>
</tr>
<tr>
<td>359</td>
<td>Home Health Treatment Codes</td>
<td>CMS</td>
<td>Unrestricted Access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Used in the 837I</td>
<td></td>
<td>Description: Codes used to describe treatments in home health settings.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="http://cms.hhs.gov">http://cms.hhs.gov</a> or <a href="http://cms.hhs.gov/providers/pufdownload/">http://cms.hhs.gov/providers/pufdownload/</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cost: Free online</td>
<td></td>
</tr>
<tr>
<td>411</td>
<td>Remittance Remark Codes</td>
<td>Washington Publishing Company</td>
<td>Unrestricted Access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Used in the 837I, 837P, 835, 270/271</td>
<td></td>
<td>Description: See.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="http://www.wpc-edi.com/codes/Codes.asp">http://www.wpc-edi.com/codes/Codes.asp</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cost: Free online</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Used in the 834</td>
<td></td>
<td>Description: This is a standard code for indicating languages for information exchange purposes. It is based on the Machine-Readable Cataloging (MARC) language codes developed by the Library of Congress.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="http://www.niso.org/standards/index.html">http://www.niso.org/standards/index.html</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cost: Free online</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Used in the 270/277, 276/277</td>
<td></td>
<td>Description: Claim status category codes indicate the general category of the claim’s status (accepted, rejected, additional information requested, etc.), which is then further detailed in the claim status codes. The claim status transaction is not used as a financial transaction.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="http://www.wpc-edi.com/codes/Codes.asp">http://www.wpc-edi.com/codes/Codes.asp</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cost: Free online</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Used in the 270/277, 276/277</td>
<td></td>
<td>Description: Claim status codes communicate information about the status of a claim (i.e., whether it’s been received, is pending, or has been paid. The claim status transaction is not used as a financial transaction.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="http://www.wpc-edi.com/codes/Codes.asp">http://www.wpc-edi.com/codes/Codes.asp</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cost: Free online</td>
<td></td>
</tr>
</tbody>
</table>
Appendix F—Contents—HIPAA Privacy Regulations

The following list shows the contents and organization of the Health Insurance Portability and Accountability Act (HIPAA) privacy regulations.

**PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS**

**Subpart A—General Provisions**
- 160.101 Statutory basis and purpose
- 160.102 Applicability
  - Identifies covered entities
- 160.103 Definitions
  - Act
  - ANSI
  - Business associate
  - Compliance date
  - Covered entity
  - Group health plan
  - HCFA
  - HHS
  - Health care
  - Health care clearinghouse
  - Health care provider
  - Health information
  - Health insurance issuer
  - Health maintenance organization
  - Health plan
  - Implementation specification
  - Individually identifiable health information
  - Modify
  - Secretary
  - Small health plan
  - Standard
  - Standard setting organization
  - State
  - Trading partner agreement
- 160.104 Modifications
  - Procedures secretary must follow to modify

**Subpart B—Pre-emption of State Law**
- 160.201 Applicability
- 160.202 Definitions
  - Contrary
  - More stringent
  - Relates to the privacy of IIHI
  - State law
- 160.203 General rule and exceptions
  - Pre-emption of state law
    - General rule
    - Exceptions to pre-emption
- 160.204 Process for requesting exception determinations
- 160.205 Duration of effectiveness of exception determinations

**Subpart C—Compliance and Enforcement**
- 160.300 Applicability
- 160.302 Definitions (see 164.501)
- 160.304 Principles for achieving compliance
- 160.306 Complaints to the secretary
  - Right to file complaint
  - Requirement for filing complaint
  - Investigation
- 160.308 Compliance reviews
- 160.310 Responsibilities of covered entities
- 160.312 Secretarial action regarding complaints and compliance reviews
PART 164—SECURITY AND PRIVACY

Subpart A—General Provisions
164.102 Statutory basis
164.104 Applicability
164.106 Relationship to other parts

Subparts B–D—[Reserved]

Subpart E—Privacy of Individually Identifiable Health Information
164.500 Applicability
164.501 Definitions
  ■ Correctional institution
  ■ Covered functions
  ■ Data aggregation
  ■ Designated record set
  ■ Direct treatment relationship
  ■ Disclosure
  ■ Health care operations
  ■ Health oversight agency
  ■ Indirect treatment relationship
  ■ Individual
  ■ Inmate
  ■ Law enforcement official
  ■ Marketing
  ■ Organized health care arrangement
  ■ Payment
  ■ Plan sponsor
  ■ Protected health information
  ■ Psychotherapy notes
  ■ Public health authority
  ■ Required by law
  ■ Research
  ■ Treatment
  ■ Use

164.502 Uses and disclosures of protected health information: general rules
  ■ General standard
    □ Permitted uses and disclosures
    □ Required disclosures
  ■ Minimum necessary standard
    □ When it applies
    □ When it does not apply

164.504 Uses and disclosures: organizational requirements
  ■ Definitions:
    □ Common control
    □ Common ownership
    □ Health care components
    □ Hybrid entity
    □ Plan administration function
    □ Summary health information
  ■ Health care component (hybrid entities)
  ■ Application of other provisions to hybrid entities
    □ Safeguard requirements
    □ Responsibilities of the hybrid entity
    □ Affiliated covered entities
    □ Requirements for designation of an affiliated covered entity
Frequently Asked Questions
The Office for Civil Rights privacy guidance provides us with a great number of frequently asked questions and answers on use and disclosure of protected health information. Following are excerpts from that privacy guidance.

Question: My state requires consent to use or disclose health information. Does the HIPAA privacy rule take away this protection?

Answer: No. The privacy rule does not prohibit a covered entity from obtaining an individual’s consent to use or disclose his or her health information and, therefore, presents no barrier to the entity’s ability to comply with state law requirements.

Question: How does the HIPAA privacy rule change the laws concerning consent for treatment?

Answer: The privacy rule relates to uses and disclosures of protected health information, not to whether a patient consents to the health care itself. As such, the privacy rule does not affect informed consent for treatment, which is addressed by state law.

Question: Can a pharmacist use protected health information to fill a prescription that was telephoned in by a patient’s physician without the patient’s written consent if the patient is a new patient to the pharmacy?

Answer: Yes. The pharmacist is using the protected health information for treatment purposes, and the HIPAA privacy rule does not require covered entities to obtain an individual’s consent prior to using or disclosing protected health information about him or her for treatment, payment, or health care operations.

Question: Can health care providers, such as a specialist or hospital, to whom a patient is referred for the first time, use protected health information to set up appointments or schedule surgery or other procedures without the patient’s written consent?

Answer: Yes. The pharmacist may provide advice to customers about over-the-counter medicines. The privacy rule permits a covered entity to disclose protected health information about an individual to the individual. See 45 CFR 164.502(a)(1)(i).

Question: Can a patient have a friend or family member pick up a prescription for her?

Answer: Yes. A pharmacist may use professional judgment and experience with common practice to make reasonable inferences of the patient’s best interest in allowing a person, other than the patient, to pick up a prescription. See 45 CFR 164.510(b). For example, the fact that a relative or friend arrives at a pharmacy and asks to pick up a specific prescription for an individual effectively verifies that he or she is involved in the individual’s care, and the HIPAA privacy rule allows the pharmacist to give the filled prescription to the relative or friend. The individual does not need to provide the
**Question:** Does the HIPAA privacy rule require documentation of Institutional Review Board (IRB) or Privacy Board approval of an alteration or waiver of individual authorization before a covered entity may use or disclose protected health information for any of the following provisions: (1) for preparatory research at 45 CFR 164.512(i)(1)(ii), (2) for research on the protected health information of decedents at 45 CFR 164.512(i)(1)(iii), or (3) a limited data set with a data use agreement as stipulated at 45 CFR 164.514(e)?

**Answer:** No. Documentation of IRB or Privacy Board approval of an alteration or waiver of individual authorization is only needed before a covered entity may use or disclose protected health information under 45 CFR 164.512(i)(1)(i). See the fact sheet and frequently asked questions about the research provisions on this Web site for more information about Institutional Review and Privacy Boards.

**Question:** If research subjects’ consent was obtained before the compliance date, but the Institutional Review Board (IRB) subsequently modifies the informed consent document after the compliance date and requires that subjects be reconsented, is authorization now required from these previously enrolled research subjects under the HIPAA privacy rule?

**Answer:** Yes. If informed consent or reconsent (i.e., asked to sign a revised consent or another informed consent) is obtained from research subjects after the compliance date, the covered entity must obtain individual authorization as required at 45 CFR 164.508 for the use or disclosure of protected health information once the consent obtained before the compliance date is no longer valid for the research. The revised informed consent document may be combined with the authorization elements required by 45 CFR 164.508. See the fact sheet and frequently asked questions about the research provisions on this Web site for more information about Institutional Review Boards.

**Question:** Can covered entities continue to disclose adverse event reports that contain protected health information to the Department of Health and Human Services (HHS) Office for Human Research Protections?

**Answer:** Yes. The Office for Human Research Protections is a public health authority under the HIPAA privacy rule. Therefore, covered entities can continue to disclose protected health information to report adverse events to the Office for Human Research Protections either with patient authorization as provided at 45 CFR 164.508, or without patient authorization for public health activities as permitted at 45 CFR 164.512(b).

**Question:** Can covered entities continue to disclose protected health information to the HHS Office for Human Research Protections for purposes of determining compliance with the HHS regulations for the protection of human subjects (45 CFR Part 46)?

**Answer:** Yes. The Office for Human Research Protections is a health oversight agency under the HIPAA privacy rule. Therefore, covered entities can continue to disclose protected health information to the Office for Human Research Protections for such compliance investigations either with patient authorization as provided at 45 CFR 164.508, or without patient authorization for health oversight activities as permitted at 45 CFR 164.512(d).

**References**

*Federal Register*, December 28, 2000, August 14, 2002