

Contents

Foreword	ix
Chapter 1 INTRODUCTION	1
1.1 Electronic Transactions and Code Sets	
1.2 Privacy	
1.3 Security Requirements	
1.4 Where Are the Savings?	
1.5 HIPAA Has Two Flaws	
1.6 Opportunity Exists	
Chapter 2 HIPAA OVERVIEW	9
2.1 Legislation	
2.2 Standard-Setting Organizations	
2.3 Standards to Enable Electronic Exchange	
2.4 HIPAA Timetable	
2.5 Statutory Penalties	
2.6 Privacy and Preemption	
2.7 Regulations	
2.8 Bush Administration	
2.9 HIPAA Compliance—Benefits	
2.10 HIPAA Compliance—Costs/Risks	
2.11 Implementation Sequence	
Action Items	
Chapter 3 STANDARDS FOR ELECTRONIC TRANSACTIONS AND CODE SETS	23
3.1 Covered Entities	
3.2 Covered Transactions	
3.3 Standards and Compliance Dates	
3.4 Maintenance and Modification of Standards	
3.5 Trading Partner Agreements	
3.6 Requirements for Covered Entities	
3.7 Additional Rules for Health Plans	

- 3.8 Additional Rules for Healthcare Clearinghouses
- 3.9 Radical Industry Change
- 3.10 Medical Data Code Sets
- 3.11 Nonmedical Data Code Sets
- 3.12 Unique Health Identifiers

Action Items

Chapter 4 STANDARDS FOR HEALTHCARE CLAIMS 45

- 4.1 Healthcare Claims Transactions
- 4.2 What Is ANSI ASC X12N?
- 4.3 837 Institutional Claims
- 4.4 837 Professional Claims
- 4.5 837 Dental Claims
- 4.6 Comparison with Current HCFA Billing Procedures
- 4.7 Obsolete Focus on Electronic Data Interchange
- 4.8 Direct Data Entry Exception

Action Items

Chapter 5 USING THE STANDARDS IN EXTENSIBLE MARKUP LANGUAGE (XML) 59

- 5.1 What Is XML?
- 5.2 What Is a Document Type Definition (DTD)?
- 5.3 Benefits of Standardized XML Data Elements
- 5.4 XML Tools
- 5.5 Sample 837-Institutional Healthcare Claim in XML
- 5.6 Structure of the 837-Institutional
- 5.7 Sample DTD for 837-Institutional Healthcare Claim
- 5.8 Required vs. Situational
- 5.9 Comparison with UB-92/HCFA 1450 Paper Form
- 5.10 Implementation and Conversion Issues
- 5.11 837 Professional Standards
- 5.12 837 Dental Standards

Action Items

Chapter 6 OTHER COVERED TRANSACTIONS 79

- 6.1 Eligibility for a Health Plan Transaction
- 6.2 Referral Certification and Authorization Transaction
- 6.3 Healthcare Claim Status Transaction
- 6.4 Enrollment and Disenrollment in a Health Plan Transaction

- 6.5 Healthcare Payment and Remittance Advice Transaction
- 6.6 Health Plan Premium Payments Transaction
- 6.7 Coordination of Benefits Transaction
- 6.8 XML Applications for Other Covered Transactions

Action Items

Chapter 7 PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION 93

- 7.1 Background of Privacy and Security Regulations
- 7.2 Who Is Covered?
- 7.3 What Information Is Protected?
- 7.4 Uses and Disclosures of Protected Health Information—General Rules
- 7.5 Business Associates
- 7.6 Patient Consent for Treatment, Payment, and Healthcare Operations
- 7.7 Required Authorizations
- 7.8 Opportunities for the Patient to Object
- 7.9 Permitted Uses and Disclosures

Action Items

Chapter 8 PRIVACY COMPLIANCE PROCEDURES 119

- 8.1 De-identification of Health Information
- 8.2 Minimum Necessary Uses and Disclosures of Protected Health Information
- 8.3 Verification
- 8.4 Notice of Privacy Practices
- 8.5 Accounting of Disclosures of Protected Health Information
- 8.6 Chief Privacy Officer
- 8.7 Training
- 8.8 Administrative, Technical, and Physical Safeguards to Protect Privacy
- 8.9 Complaint Process
- 8.10 Sanctions
- 8.11 Mitigation
- 8.12 No Retaliatory Acts or Waiver of Privacy Rights
- 8.13 Written Privacy Procedures
- 8.14 Integration with Corporate Compliance Program

Action Items

Chapter 9 PATIENT PRIVACY RIGHTS 139

- 9.1 Patient Rights to Request Privacy Protection

9.2 Patient Right to Access Protected Health Information

- 9.3 Patient Right to Request Amendment of Protected Health Information
- 9.4 Limited Federal Preemption
- 9.5 Importance of State-Level Privacy Laws
- 9.6 Compliance Dates

Action Items

Chapter 10 SECURITY COMPLIANCE PROCEDURES 155

- 10.1 Statutory Background
- 10.2 What Is Covered?
- 10.3 Administrative Procedures
- 10.4 System Certification
- 10.5 Chain-of-Trust Partner Agreement
- 10.6 Contingency Plan for System Emergencies
- 10.7 Formal Mechanisms for Processing Records
- 10.8 Information Access Control
- 10.9 Internal Security Audit
- 10.10 Personnel Security
- 10.11 Security Configuration Management
- 10.12 Security Incident Procedures
- 10.13 Security Management Process
- 10.14 Termination Procedures
- 10.15 Training

Action Items

Chapter 11 PHYSICAL SAFEGUARDS AND TECHNICAL SECURITY MECHANISMS 169

- 11.1 Physical Safeguards
- 11.2 Access Controls
- 11.3 Audit Controls
- 11.4 Authorization Control
- 11.5 Data Authentication
- 11.6 Entity Authentication
- 11.7 Communication/Network Controls
- 11.8 Encryption
- 11.9 Electronic Signature
- 11.10 Compliance Dates

Action Items

Chapter 12 IMPLEMENTING A HIPAA COMPLIANCE PROGRAM 179

- 12.1 HIPAA Sanctions
- 12.2 Assessment
- 12.3 Initial Education Regarding HIPAA Compliance Program
- 12.4 Action Steps—Electronic Transactions
- 12.5 Action Steps—Privacy
- 12.6 Action Steps—Security
- 12.7 Implementation Costs
- 12.8 Maintaining an Effective HIPAA Compliance Program
- 12.9 Integration with Other Compliance Efforts
- 12.10 Conclusion

Glossary 191

Internet Links 193

Index 195

Appendices A-E (available at www.ache.org/pubs/withapp.html)