



# HEALTH CARE PRIVACY and SECURITY

2013 EDITION

ANDREW SERWIN  
KENNETH MORTENSEN

THOMSON REUTERS  
**WESTLAW**

# Health Care Privacy and Security

**2013 Edition**

Andrew B. Serwin

and

Kenneth P. Mortenson

**WEST®**

A Thomson Reuters business

*For Customer Assistance Call 1-800-328-4880*

Material # 41310766

© 2013 Thomson Reuters

This publication was created to provide you with accurate and authoritative information concerning the subject matter covered; however, this publication was not necessarily prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional.

ISBN 978-0-314-61701-9

## About the Authors

**Kenneth P. Mortensen** is Vice President, Assistant General Counsel & Chief Privacy Officer at CVS Caremark Corporation, where he has enterprise responsibility for information governance strategy to empower the superior application of information as a critical enterprise asset used to optimize risk and facilitate innovation incorporating an approach that protects individual privacy and drives operational compliance. Ken manages the Information Governance organization of the Legal Department, which includes a legal team, privacy operations, and, indirectly, the enterprise information security and risk governance group.

Ken is a member of the board of directors for the International Association of Privacy Professionals or IAPP. Founded in 2000, the IAPP is the world's largest association of privacy professionals with more than 11,000 members in 70 countries. The IAPP helps define, support, and improve the privacy profession through networking, education, and certification.

Before to coming to CVS Caremark, Ken was Boston Scientific Corporation's first ever Chief Privacy Officer and had world-wide responsibility to implement a global corporate privacy and security program, including EU data protection policy, at the medical device manufacturer.

Prior to re-entering the private sector, Ken served in the Administration of President George W. Bush as the Chief Privacy and Civil Liberties Officer for the U.S. Department of Justice, where he was the primary counsel and policy advisor to the Attorney General and Deputy Attorney General on privacy and civil liberties matters, including revisions to the Attorney General Guidelines for Domestic FBI Operations, updates to Executive Order 12333, and the FISA (Foreign Intelligence Surveillance Act) Amendments Act. He created the newest independent office within the Department, the Office of Privacy & Civil Liberties, with responsibilities under the Privacy Act of 1974 and the e-Government Act. Ken negotiated numerous international agreements with privacy and civil liberties safeguards that supported national security and law enforcement activities, including the High Level Contact Group between the U.S. and EU to create an understanding on privacy for government information sharing. Before coming to Justice, Ken joined the U.S. Dep't of Homeland Security early in its existence, first as a Senior Advisor and ending as the Deputy Chief Privacy Officer, counseling on privacy and security issues related to agency programs.

Formerly, Ken was founding/managing law partner at Harvey & Mortensen with clients that ranged from start-ups to state attorneys general, including serving as outside counsel to Pennsylvania Attorney General Mike Fisher for Internet and cyber issues as well as designing and operating the Commonwealth's initial Do Not Call website. Before private practice, Ken was a Teaching Fellow at Villanova University School of Law, where he taught computer and information law and managed operations for a think tank, the Center

for Information Law and Policy. Ken began his career at Burroughs Corporation as an Electrical Engineer performing large system design and test development for mainframe computers. In addition to his J.D. from Villanova University School of Law, he has an M.B.A. from Villanova University and a B.S.E.E. from Drexel University.

**Andrew B. Serwin** is an internationally recognized thought leader regarding information's evolving role in the economy and society, including how businesses can achieve key business objectives through the use of information, strategies companies must implement to protect and secure information, and what are appropriate uses of information. He combines a deep understanding of privacy and security regulatory issues, with advanced certification in business process improvement, as well as privacy. He is also the founding chair of the Privacy, Security & Information Management Practice and is a partner in the San Diego/Del Mar and Washington, D.C. offices of Foley & Lardner LLP. Mr. Serwin has handled a number of high-profile privacy and consumer protection matters, including multiple privacy enforcement matters before the Federal Trade Commission, and is internationally recognized as one of the leading consumer protection and privacy lawyers.

Mr. Serwin advises a number of *Fortune* 500 companies regarding global privacy compliance, including: state, federal and international restrictions on the use and transfer of information; behavioral advertising; social gaming; security breach compliance; mobile marketing; incident response resulting from data misuse and hacking; COPPA compliance; EHR/PHR concerns; marketing restrictions; HIPAA and state medical privacy laws; social media and blogging policies; Do-Not-Call restrictions; compliance with CAN-SPAM and state e-mail laws; employee monitoring; pretexting; location-based services; the drafting and implementation of privacy and security policies; risk assessments; compliance with ECPA and FISA; content monitoring; compliance with the CFAA and state computer crime laws; as well as information governance guidance in the context of M&A and technology transactions.

Mr. Serwin has provided advice to companies in a diverse set of industries, including advising: a leading Internet auction company; a nation-wide health insurer; ISPs; leading online retailers; major hospital chains; genetics companies; a leading social network; an international security company; data aggregators; a leading chain of international health and fitness clubs; a nation-wide auto retailer; one of the nation's largest home builders; a number of major utilities; medical device manufacturers; several major telecommunications companies; behavioral advertising companies; software-as-a-service providers; a leading retail pharmacy chain and PBM; several major hotel and resort companies; and several nationally-recognized universities. Mr. Serwin also has unique experience in representing emerging technology companies, having served as the founder and president of an internet start-up.

Mr. Serwin also has extensive litigation and enforcement experience, having served as lead counsel in a number of FTC matters, matters before the Office of Civil Rights, as well as state consumer protection matters and consumer privacy litigation matters based upon the alleged misuse of personal information.

Mr. Serwin was named to *Security Magazine's* "25 Most Influential Industry Thought Leaders" for 2009—he is the only lawyer in private practice to ever receive this award, and was ranked second in the 2010 *Computerworld* survey of top global privacy advisors. He is recognized by *Chambers USA* as one of the top privacy & data security attorneys nationwide (2009-2012), where he has described by clients as "*a tireless worker, holding onto the ever-shifting puzzle pieces of the law in this area in a way that other privacy lawyers cannot.*", and noted as "an excellent privacy lawyer, a real expert in the field," by *Chambers Global* 2012. The *Legal 500* recognized Mr. Serwin as a Leading Lawyer in data protection and privacy (2010-2011), where clients stated that he "understands business concerns and provides practical, to-the-point, advice." He has been Peer Review Rated as AV® Preeminent™, the highest performance rating in Martindale-Hubbell's peer review rating system, and was selected for inclusion in the *San Diego Super Lawyers®* lists (2007-2012), and was selected by his peers for inclusion in *The Best Lawyers in America®* in the field of information technology law (2010-2012).

Mr. Serwin serves as Executive Director of the Lares Institute, a think-tank focused on privacy and information management issues, as well as general counsel of the RIM Council of the Ponemon Institute, LLC, as well as the privacy and the legal subcommittees of the PSAB of the California Health and Human Services Agency by the California Office of HIPAA Implementation. He previously served as Co-Chair of the California State Bar's Cyberspace Law Committee and as a member of the Committee of Administration of Justice, as well as a member of the Publications Board for the Business Law Section of the American Bar Association.

Mr. Serwin has written a number of books, including the leading treatise on privacy, "Information Security and Privacy: A Guide to International Law and Compliance", a book that was named one of Thomson-Reuters' Best-Selling Books for 2010, and "Information Security and Privacy: A Guide to Federal and State Law and Compliance," which collectively are a three-volume, 4,000 page series that examines all aspects of privacy and security laws, published by Thomson-Reuters, which have been called "*the best privacy sourcebook,*" "*an indispensable resource for privacy professionals at all levels,*" and "*a book that everybody in the information privacy field should have on their desk,*" and has been cited by *Ostergren v. Cuccinelli*, 615 F.3d 263 (4th Cir. 2010). He is also the author of several leading law review articles: "Privacy 3.0—The Principle of Proportionality," 42 *U. Mich. J.L. Reform* 869 (2009), "Poised on the Precipice: A Critical Examination of Privacy Litigation," 25 *Santa Clara Computer & High Tech. L.J.* 883 (2009), cited by *Hammond v. The Bank of New York Mellon Corp.* 2010 WL 2643307, (S.D.N.Y., June 25, 2010), and *Joseph Oat Holdings, Inc. v. RCM Digesters, Inc.*, 2010 WL 5065037, (3rd Cir. December 13, 2010), and "The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices", 48 *San Diego L. Rev.* 809 (2011). He has written over 100 articles and presented over 100 times on litigation and privacy.

His works have been cited by numerous law reviews and treatises, including: American Law Reports (ALR); American Jurisprudence 3rd; California Law Review; Callmann on Unfair Competition; Harvard Journal of Law & Technology; Iowa Law Review;

Southern California Interdisciplinary Law Journal; Stanford Law Review; and Wright & Miller, Federal Practice and Procedure—Criminal.

Mr. Serwin is a graduate of the University of San Diego School of Law (J.D., *cum laude*, 1995), where he was a member of the Order of the Coif. He earned his B.A. in political science, *cum laude*, from the University of California, San Diego in 1992. Mr. Serwin is admitted to practice law in California and the District of Columbia.

**Tammy H. Boggs** is an associate with Foley & Lardner LLP, where she represents clients in a variety of industries in consumer class action litigation, privacy and security litigation, and general business disputes. Ms. Boggs has substantial experience in all stages of litigation and civil procedure, including complex e-discovery issues, depositions, motion practice, trial preparation and alternative dispute resolution. She represents clients in both state and federal court proceedings. Ms. Boggs has also defended clients in patent litigation pending in district courts and the International Trade Commission. She is a member of the Privacy Litigation; Business Litigation & Dispute Resolution; Intellectual Property Litigation; and Privacy, Security & Information Management Practices. She serves on the firm's Diversity Committee.

Ms. Boggs has represented clients in a number of high-profile privacy and consumer protection matters brought by regulatory agencies, and has experience in coordinating incident responses to security breaches. She advises clients on compliance with privacy laws and best practices for information governance.

Ms. Boggs is also a member of the firm's Pro Bono Asylum/Immigration Practice, and has won asylum for numerous pro bono clients before the San Diego Immigration Court.

Prior to joining Foley, Ms. Boggs was an associate at Heller Ehrman LLP. While attending law school, she was a judicial extern to the Honorable Vaughn Walker, United States District Court Chief Judge in 2005. Before beginning her legal career, Ms. Boggs was a lead accounting analyst for Silicon Valley Bank, and provided financial auditing and tax services at Deloitte & Touche LLP. As a Certified Public Accountant (inactive), she performed audits of large corporations, including companies in the high tech, manufacturing, financial services, and insurance industries.

Ms. Boggs earned her law degree from the University of California, Hastings College of the Law (J.D., *cum laude*, 2007) where she was a member of the Prince Evidence and Jessup International Law Moot Court Competition Teams, and received accolades in Appellate Advocacy, Moot Court, and Legal Writing & Research. She is a graduate of the University of California, Los Angeles with a degree in business economics and an accounting minor (B.A., *magna cum laude*, 1999).

Ms. Boggs is admitted to practice law in California, before all District Courts of California, and before the Ninth Circuit Court of Appeals. She is fluent in spoken Mandarin Chinese.



Representative Present and Past Clients: WellPoint/Anthem Blue Cross, CVS Caremark, Bank of America, Disney, Old Republic Home Protection Company, Online Guru, Sony Electronics, AmeriCredit Financial Services, Clarendon National Insurance Company, and Kyocera Wireless.

Representative Publications and Presentations:

- "Analysing proposed changes to COPPA: the operator's role," *Data Protection Law & Policy*, September 2012
- Contributing Author, "Expert Analysis" column, *Class Action Law360*, 2011
- "Class v. Merits Discovery in Consumer Class Actions," prepared for Bridgeport California Consumer Class Action Conference, January 2011
- "Two Recent Class Action Decisions Further Develop Pleading Requirements Under California's Unfair Competition Law," Bloomberg's *Antitrust & Trade Law Report*, August 2010
- "Discovery in Class Actions: Privacy Implications and Best Practices," prepared for Bridgeport Class Action Litigation Conference, August 2010

**Matthew Haddad** is Associate General Counsel at WellPoint, Inc. He advises WellPoint and its affiliates on matters including Privacy and Security; HIPAA Standard Transactions and Code Sets; Pharmaceutical, Government and Academic Research; and Contract Negotiation. Mr. Haddad is a member of the Virginia State Bar, the International Association of Privacy Professionals and the Association of Corporate Counsel.

**Molly McCoy**, JD, MPH, CIPP/US is Senior Counsel at WellPoint, Inc. She advises WellPoint and its affiliated health plans and other subsidiaries on matters including Privacy and Security, HIPAA and HITECH, state privacy law, Business Associate Agreement negotiations, and proposed international, federal and state privacy law. Ms. McCoy is a member of the New York and Colorado State Bars and the International Association of Privacy Professionals.

**Peter McLaughlin** is senior counsel with Foley & Lardner, LLP in the firm's Boston office, where he is a member of the Privacy and Healthcare practices. He regularly advises clients on their understanding of and compliance with healthcare privacy and security, in addition to representing clients against federal and state regulatory matters. Before joining the firm, Mr. McLaughlin had been Assistant General Counsel - Privacy & Security and privacy leader for Cardinal Health, Inc., a Fortune 20 healthcare company. He is a graduate of Columbia University and the Georgetown University Law Center.

**Megan E. O'Sullivan** is an associate with Foley & Lardner LLP and a member of the Business Litigation & Dispute Resolution Practice and Privacy, Security & Information Management Practices.



Ms. O'Sullivan has represented clients in a number of privacy and consumer protection matters, including: the drafting and implementation of privacy and information security policies; security breach compliance; incident response; drafting and negotiating privacy agreements; and advising clients on general compliance obligations under both state and federal privacy and data security legislation.

Ms. O'Sullivan was a summer associate for Foley (2009) and also obtained experience with the San Francisco Superior Court in the Alternative Dispute Resolution Program where she assisted in the planning and implementation of the Asbestos Alternative Dispute Resolution Program. Prior to entering law school, Ms. O'Sullivan served as a staff assistant for the Office of Congresswoman Susan Davis.

Ms. O'Sullivan earned her law degree, *cum laude*, from the University of California, Hastings College of the Law (J.D., 2010) where she earned a CALI Award (top student of the class) in negotiations and ADR Externship Class. She was also a board member of the U.C. Hastings Negotiation Team. Ms. O'Sullivan graduated Phi Beta Kappa with a degree in political science and a minor in Spanish from the University of California, Berkeley (B.A., 2006). While at Berkeley, she completed an honors thesis and received numerous honors recognitions. Ms. O'Sullivan spent one year of undergraduate study at the Autonomous University of Barcelona, in Spain.

Ms. O'Sullivan is admitted to practice in California and before the Northern, Southern, Central, and Eastern Districts of California.

**Eileen R. Ridley** is a partner with Foley & Lardner, LLP where she serves on the firm's National Management Committee and is Vice Chair of the Litigation Department. She is a member of the firm's Privacy, Security & Information Management practice group and is the co-chair of the Privacy Litigation Task Force. Ms. Ridley has tried over 20 matters and has handled in excess of 40 class actions including matters involving the healthcare industry and privacy and information security issues. Ms. Ridley is a contributing author on Antitrust and Unfair Competition Law Section, The State Bar of California, CALIFORNIA STATE ANTITRUST AND UNFAIR COMPETITION LAW, Chapter 29, *The Consumers Legal Remedy Act*, (Cheryl Lee Johnson, ed., Matthew Bender & Co. 2009) and Protecting Personally Identifiable Information: A Guide for College and University Administrators, Chapter 2, *Recent Trends in Data Security and Regulatory Enforcement*, (Peter McLaughlin, ed., Council on Law in Higher Education, 2011). Ms. Ridley was also recognized by the *Legal 500* for her work in insurance: advice to insurers.

## **Table of Contents**

### **CHAPTER 1. INTRODUCTION**

- § 1:1 The rise of information security and privacy
- § 1:2 General privacy principles
- § 1:3 The rise of HIPAA
- § 1:4 Costs and benefits of the new Rule
- § 1:5 Organization for economic co-operation and development guidelines: a beginning
- § 1:6 Scope of OECD guidelines
- § 1:7 Collection limitation principle
- § 1:8 Data quality principle
- § 1:9 Purpose specification principle
- § 1:10 Security safeguards principle
- § 1:11 Openness principle
- § 1:12 Individual participation principle
- § 1:13 Accountability principle
- § 1:14 International application-- Free flow and legitimate restrictions
- § 1:15 National implementation
- § 1:16 International cooperation
- § 1:17 Principles adopted by the Asia-Pacific Economic Cooperation
- § 1:18 APEC information privacy principles
- § 1:19 Privacy and security-- The seven U.S. privacy principles

### **CHAPTER 2. HEALTH INFORMATION AND PRIVACY AND SECURITY**

- § 2:1 A preliminary matter-Health Information Technology for Economic and Clinical Health Act of 2009
- § 2:2 Health Information Technology for Economic and Clinical Health Act-Increased civil penalties

#### **I. INTRODUCTION**

- § 2:3 Importance of health privacy
- § 2:4 Health record interoperability
- § 2:5 An overview of California's approach
- § 2:6 Thoughts on interoperability models
- § 2:7 Personal health records
- § 2:8 Restrictions on disclosure of prescription drug information

## II. HIPAA

### A. In general

- § 2:9 Background
- § 2:10 Compliance dates for implementation of new or modified standards and implementation specifications
- § 2:11 Overview of HIPAA
- § 2:12 Inapplicability to employers
- § 2:13 An overview of recent changes to HIPAA
- § 2:14 Changes to the definition of business associate
- § 2:15 Changes to the definition of electronic media
- § 2:16 Enforcement for business associates
- § 2:17 Time for compliance
- § 2:18 Sections 160.306, 160.308, 160.310, and 160.402 regarding complaints to the secretary, compliance reviews, restrictions on certain conduct, and civil monetary penalties
- § 2:19 Factors for assessing civil monetary penalties
- § 2:20 Affirmative defenses and waiver of penalties
- § 2:21 Changes to the applicability language
- § 2:22 Changes regarding hybrid entities—Organizational requirements
- § 2:23 Security and safeguards
- § 2:24 Agreements with business associates
- § 2:25 Physical and technical safeguards
- § 2:26 Organizational requirements
- § 2:27 Policies procedures and documentation requirements
- § 2:28 Administrative requirements and burden of proof
- § 2:29 Applicability of section 164.500
- § 2:30 Use and disclosures of protected health information
- § 2:31 Sale of protected health information and minimum necessary
- § 2:32 Satisfactory assurances and decedent's information
- § 2:33 Organizational requirements
- § 2:34 Uses and disclosures for treatment, payment or health care operations
- § 2:35 Uses and disclosures for which authorization is required
- § 2:36 Genetic information
- § 2:37 Uses and disclosures requiring an opportunity to agree or to object
- § 2:38 Uses and disclosures for which an authorization or opportunity to agree or to object is not required
- § 2:39 Other requirements relating to uses and disclosures of protected health information
- § 2:40 Notice of privacy practices
- § 2:41 Rights to request privacy protection for protected health information
- § 2:42 Access of individuals to protected health information
- § 2:43 Administrative requirements
- § 2:44 Transition provisions
- § 2:45 Costs and benefits
- § 2:46 Privacy and security requirements

§ 2:47 New statutory requirements under ARRA  
§ 2:48 Annual guidance  
§ 2:49 Education on health information privacy  
§ 2:50 Application of knowledge elements associated with contracts  
§ 2:51 Application of civil and criminal penalties  
§ 2:52 Business associate contracts required for certain entities  
§ 2:53 Improved enforcement under the Social Security Act  
§ 2:54 Effective date and regulations  
§ 2:55 Distribution of certain civil monetary penalties collected  
§ 2:56 Establishment of methodology to distribute percentage of CMPS collected to harmed individuals  
§ 2:57 Effective date  
§ 2:58 Audits  
§ 2:59 Relationship to other laws-- HIPAA state preemption  
§ 2:60 Relationship to other laws—HIPAA  
§ 2:61 Construction of law  
§ 2:62 Reports on compliance  
§ 2:63 Study and report on application of privacy and security requirements to non-HIPAA covered entities  
§ 2:64 Guidance on implementation specification to de-identify protected health information  
§ 2:65 GAO report on treatment disclosures  
§ 2:66 Report required  
§ 2:67 Study  
§ 2:68 Restrictions on certain disclosures and sales of health information; accounting of certain protected health information disclosures; access to certain information in electronic format  
§ 2:69 Disclosures required to be limited to the limited data set or the minimum necessary  
§ 2:70 Determination of minimum necessary  
§ 2:71 Application of exceptions  
§ 2:72 Exception  
§ 2:73 Accounting of certain protected health information disclosures required if covered entity uses electronic health record  
§ 2:74 Regulations  
§ 2:75 Response to requests for accounting  
§ 2:76 Effective date  
§ 2:77 Prohibition on sale of EHRs or PHI  
§ 2:78 Regulations regarding the prohibition of sale  
§ 2:79 Effective date  
§ 2:80 Access to certain information in electronic format  
§ 2:81 Conditions on certain contacts as part of health care operations—marketing  
§ 2:82 Opportunity to opt out of fundraising  
§ 2:83 Effective date  
§ 2:84 Duties under HIPAA and state law  
§ 2:85 Intent and violations of HIPAA

§ 2:86 Government violations of the Rehabilitation Act

## **B. Scope of HIPAA Regulations and Enforcement**

§ 2:87 Statutory basis and purpose

§ 2:88 Applicability

§ 2:89 Modifications

§ 2:90 General rule and exceptions—Preemption

§ 2:91 Process for requesting exception determinations

§ 2:92 Duration of effectiveness of exception determinations

§ 2:93 Applicability

§ 2:94 Principles for achieving compliance

§ 2:95 Complaints to the Secretary

§ 2:96 Compliance reviews

§ 2:97 Responsibilities of covered entities and business associates

§ 2:98 Secretarial action regarding complaints and compliance reviews

§ 2:99 Investigational subpoenas and inquiries

§ 2:100 Investigational inquiries are non-public investigational proceedings conducted by the Secretary

§ 2:101 Refraining from intimidation or retaliation

§ 2:102 Basis for a civil money penalty

§ 2:103 Amount of a civil money penalty

§ 2:104 Violations of an identical requirement or prohibition

§ 2:105 Factors considered in determining the amount of a civil money penalty

§ 2:106 Affirmative defenses

§ 2:107 Waiver

§ 2:108 Limitations

§ 2:109 Authority to settle

§ 2:110 Penalty not exclusive

§ 2:111 Notice of proposed determination

§ 2:112 Failure to request a hearing

§ 2:113 Collection of penalty

§ 2:114. Notification of the public and other agencies

## **C. Hearings**

§ 2:115 Applicability

§ 2:116 Hearing before an ALJ

§ 2:117 Rights of the parties

§ 2:118 Authority of the ALJ

§ 2:119 Ex parte contacts with the ALJ

§ 2:120 Prehearing conferences

§ 2:121 Authority to settle

§ 2:122 Discovery

§ 2:123 Exchange of witness lists, witness statements, and exhibits

§ 2:124 Subpoenas for attendance at hearing

- § 2:125 Fees
- § 2:126 Form, filing, and service of papers
- § 2:127 Computation of time
- § 2:128 Motions
- § 2:129 Sanctions
- § 2:130 Collateral estoppels
- § 2:131 The hearing
- § 2:132 Statistical sampling
- § 2:133 Witnesses
- § 2:134 Evidence
- § 2:135 The record
- § 2:136 Post hearing briefs
- § 2:137 ALJ's decision
- § 2:138 Appeal of the ALJ's decision
- § 2:139 Stay of the Secretary's decision
- § 2:140 Harmless error

## **D. Security**

- § 2:141 Statutory basis for security and privacy regulations
- § 2:142 Applicability of regulations
- § 2:143 Organizational requirements-- Hybrid entities
- § 2:144 Safeguard requirements for affiliated covered entities
- § 2:145 Documentation
- § 2:146 Relationship to other portions of the regulations
- § 2:147 Applicability
- § 2:148 In general
- § 2:149 Security management process
- § 2:150 Security management process-- Risk analysis
- § 2:151 Security management process-- Risk management
- § 2:152 Security management process-- Sanction policy
- § 2:153 Security management process-- Information system activity review
- § 2:154 Assigned security responsibility
- § 2:155 Workforce security
- § 2:156 Workforce security-- Authorization and/or supervision
- § 2:157 Workforce security-- Workforce clearance procedure
- § 2:158 Workforce security-- Termination procedures
- § 2:159 Information access management
- § 2:160 Information access management-- Isolating health care clearinghouse functions
- § 2:161 Information access management-- Access authorization
- § 2:162 Access establishment and modification
- § 2:163 Information access management-- Access establishment and modification
- § 2:164 Security awareness and training
- § 2:165 Security awareness and training-- Security reminders
- § 2:166 Security awareness and training-- Protection from malicious software
- § 2:167 Security awareness and training-- Log-in monitoring

- § 2:168 Security awareness and training-- Password management
- § 2:169 Security incident procedures
- § 2:170 Contingency plan
- § 2:171 Contingency plan-- Data backup plan
- § 2:172 Contingency plan-- Disaster recovery plan
- § 2:173 Contingency plan-- Emergency mode operation plan
- § 2:174 Contingency plan-- Testing and revision procedures
- § 2:175 Contingency plan-- Applications and data criticality analysis
- § 2:176 Evaluation
- § 2:177 Business associate contracts and other agreements
- § 2:178 Physical safeguards
- § 2:179 Device and media controls
- § 2:180 Technical safeguards
- § 2:181 Organizational requirements
- § 2:182 Organizational requirements-- Requirements for group health plans
- § 2:183 Policies and procedures

## **E. Privacy**

- § 2:184 Application of privacy provisions and penalties to business associates
- § 2:185 Applicability
- § 2:186 Application to health care clearinghouses
- § 2:187 Exceptions
- § 2:188 Uses and disclosures of de-identified protected health information
- § 2:189 Use and disclosure of genetic information for underwriting purposes
- § 2:190 Sale of protected health information
- § 2:191 Minimum necessary
- § 2:192 Uses and disclosures of PHI subject to an agreed upon restriction
- § 2:193 Creation of not individually identifiable information
- § 2:194 Disclosures to business associates
- § 2:195 Deceased individuals
- § 2:196 Personal representatives
- § 2:197 Adults and emancipated minors
- § 2:198 Deceased individuals
- § 2:199 Confidential communications
- § 2:200 Abuse, neglect, endangerment situations
- § 2:201 Processing and disclosures with notice
- § 2:202 Disclosures by whistleblowers and workforce member crime victims

## **F. Uses and disclosures**

- § 2:203 Business associate contracts
- § 2:204 Other arrangements for business associate agreements
- § 2:205 Business associate contracts with subcontractors
- § 2:206 Requirements for group health plans
- § 2:207 Uses and disclosures by group health plans



§ 2:208 Requirements for a covered entity with multiple covered functions  
 § 2:209 Uses and disclosures to carry out treatment, payment, or health care operations  
 § 2:210 Treatment, payment, or health care operations  
 § 2:211 Uses and disclosures for which an authorization is required  
 § 2:212 Sale of protected health information  
 § 2:213 Valid authorization  
 § 2:214 Other requirements of authorizations  
 § 2:215 Uses and disclosures requiring an opportunity for the individual to agree or to object  
 § 2:216 Emergency circumstances  
 § 2:217 Uses and disclosures for involvement in the individual's care and notification purposes  
 § 2:218 Uses and disclosures for disaster relief purposes  
 § 2:219 Uses and disclosures when the individual is deceased  
 § 2:220 Uses without consent  
 § 2:221 Uses and disclosures for public health activities  
 § 2:222 Disclosures about victims of abuse, neglect or domestic violence  
 § 2:223 Uses and disclosures for health oversight activities  
 § 2:224 Disclosures for judicial and administrative proceedings  
 § 2:225 Defining satisfactory assurances  
 § 2:226 Disclosures for law enforcement purposes  
 § 2:227 Limited information for identification and location purposes  
 § 2:228 Victims of a crime  
 § 2:229 Decedents  
 § 2:230 Crime on premises  
 § 2:231 Reporting crime in emergencies  
 § 2:232 Uses and disclosures about decedents  
 § 2:233 Uses and disclosures for cadaveric organ, eye or tissue donation purposes  
 § 2:234 Uses and disclosures for research purposes  
 § 2:235 Documentation of waiver approval  
 § 2:236 Uses and disclosures to avert a serious threat to health or safety  
 § 2:237 Uses and disclosures for specialized government functions-- Military and veterans activities  
 § 2:238 Uses and disclosures for specialized government functions-- Separation or discharge from military service  
 § 2:239 Uses and disclosures for specialized government functions-- Foreign military personnel  
 § 2:240 Uses and disclosures for specialized government functions-- National security and intelligence activities  
 § 2:241 Uses and disclosures for specialized government functions-- Protective services for the President and others  
 § 2:242 Uses and disclosures for specialized government functions-- Medical suitability determinations  
 § 2:243 Correctional institutions and other law enforcement custodial situations  
 § 2:244 Covered entities that are government programs providing public benefits  
 § 2:245 Disclosures for workers' compensation

§ 2:246 Re-identification  
§ 2:247 Minimum necessary uses of PHI  
§ 2:248 Minimum necessary disclosures of PHI  
§ 2:249 Minimum necessary requirements for PHI  
§ 2:250 Limited data set  
§ 2:251 Uses for fundraising  
§ 2:252 Uses and disclosures for underwriting and related purposes  
§ 2:253 Verification requirements  
§ 2:254 Verification  
§ 2:255 Right to notice of privacy practices for PHI  
§ 2:256 Requirements for electronic notice  
§ 2:257 Joint notice by separate covered entities  
§ 2:258 Rights to request privacy protection for PHI  
§ 2:259 Confidential communications requirements  
§ 2:260 Access of individuals to PHI  
§ 2:261 Review of denial of access  
§ 2:262 Requests for access and timely action  
§ 2:263 Providing access  
§ 2:264 Time and manner of access  
§ 2:265 Denial of access  
§ 2:266 Amendment of PHI  
§ 2:267 Actions on notices of amendment  
§ 2:268 Documentation  
§ 2:269 Accounting of disclosures of protected health information  
§ 2:270 Content of the accounting  
§ 2:271 Providing the accounting  
§ 2:272 Documentation  
§ 2:273 Personal designation  
§ 2:274 Safeguards  
§ 2:275 Complaints to the covered entity  
§ 2:276 Documentation of complaints  
§ 2:277 Mitigation  
§ 2:278 Refraining from intimidating or retaliatory acts  
§ 2:279 Waiver of rights  
§ 2:280 Policies and procedures  
§ 2:281 Changes to privacy practices stated in the notice  
§ 2:282 Changes to other policies or procedures  
§ 2:283 Documentation  
§ 2:284 Retention period  
§ 2:285 Group health plans  
§ 2:286 Use and disclosure of information  
§ 2:287 Effect of prior contracts or other arrangements with business associates  
§ 2:288 Compliance dates for initial implementation of the privacy standards  
§ 2:289 Public records laws and HIPAA protections  
§ 2:290 State Medicaid restrictions and HIPAA  
§ 2:291 De-identified information