

Table of Contents

CHAPTER 10. CORPORATE SECURITY AND PRIVACY DUTIES, POLICIES AND FORMS

I. INTERNAL SECURITY AND PRIVACY

- § 10:1 Internal security and privacy generally
- § 10:2 Duty of confidentiality for internal corporate information and trade secrets
- § 10:3 Duty to shareholders
- § 10:4 —SEC disclosures
- § 10:5 ——Management’s discussion and analysis
- § 10:6 ——Risk factors
- § 10:7 ——Description of business
- § 10:8 Fiduciary duty of due care
- § 10:9 Duty to customers to enable unhindered use of system
- § 10:10 —Security from viruses, Trojan horses, and other malware
- § 10:11 Duties owed by ISPs, OSPs, and ASPs
- § 10:12 Data risk and cloud computing
- § 10:13 Corporate policies—Forms

II. CONFIDENTIAL AND PRIVATE THIRD-PARTY INFORMATION

- § 10:14 Responsibility for data security—Contractual issues
- § 10:15 Fiduciary and other common-law obligations to protect information belonging to others
- § 10:16 Confidentiality agreements and issues therein
- § 10:17 Encrypted channels for maintenance and transfer of customer information
 - § 10:18 —Internally
 - § 10:19 Maintenance and transfer of customer information—By third-party commerce partners
- § 10:20 Privacy policy—In general
- § 10:21 —Notice/awareness
- § 10:22 Privacy policy regarding internal use of third-party information—Choice/consent: consumers’ ability to opt out
- § 10:23 —Access/participation: consumers’ ability to access/ change their information

- § 10:24 —Integrity/security: information on how data will be kept confidential
- § 10:25 —Enforcement: explanation to consumers of internal enforcement policies
- § 10:26 —Sending and receipt of unsolicited email
- § 10:27 —Liability for disclosing private information

III. DAMAGE CAUSED TO THIRD-PARTY SYSTEMS

- § 10:28 Damage caused to third-party systems generally
- § 10:29 Security from spreading viruses, Trojan horses, and other malware
- § 10:30 Security from employee/contractor intentional abuse of third-party systems
- § 10:31 Third-party policies and forms generally
- § 10:32 Click-wrap agreements—Website visitors/customers
- § 10:33 Information-sharing agreements
- § 10:34 Online/offline privacy and security policy: checkbox short form
- § 10:35 Sample privacy policy: form
- § 10:36 Disclosure of effect of sale of business: short form version 1
- § 10:37 Disclosure of effect of sale of business: short form version 2
- § 10:38 Choice/opt-out disclosure: short form
- § 10:39 Security disclosure: Sample
- § 10:40 Hosting agreement: security provisions
- § 10:41 Notice of security breach: form
- § 10:42 Notice of security breach: short form
- § 10:43 HITECH sample data breach notification letter to individual
- § 10:44 HITECH sample data breach notification to the media
- § 10:45 Notification for Public Companies
- § 10:46 Miscellaneous Federal Notification Laws
- § 10:47 Computer use policy: long form for MIS department personnel
- § 10:48 Computer use policy: short form version 1
- § 10:49 Computer use policy: short form version 2
- § 10:50 IT policy acknowledgment: short form for all personnel
- § 10:51 Blogging and Social Media Policy

IV. DEVELOPING BEST PRACTICES AND LEGAL INFORMATION SECURITY STRATEGY

- § 10:52 Information security policies
- § 10:53 Creation of legal information security strategy

TABLE OF CONTENTS

- § 10:54 —Legal threat modeling
- § 10:55 ——Data-intensive business
- § 10:56 ——Extent of internal information sharing; policy of least information privilege
- § 10:57 ——Extent of external information sharing and external legal dependencies
- § 10:58 ——History of strict data handling norms and good information security practices
- § 10:59 ——Reactive vs. proactive legal culture
- § 10:60 —Selling the legal benefits of good security practices to businesspeople
- § 10:61 —Drafting a corporate data security policy document
- § 10:62 Adherence and evolution
- § 10:63 —Success of incident response to most recent security incident
- § 10:64 —Success of last audit and efficacy of current data management systems
- § 10:65 —Impact of legal developments related to data security and privacy
- § 10:66 —Likely future uses for collected data and adequacy of current privacy policies
- § 10:67 —Adequacy of existing contracts regarding data security and potential for liability
- § 10:68 Legal information security threat modeling checklist

CHAPTER 11. EUROPEAN UNION DATA PROTECTION

I. OVERVIEW

- § 11:1 European Union Data Protection Directive 95/46/EC and the General Data Protection Regulation
- § 11:2 General Data Protection Regulation 2016/679
- § 11:3 GDPR—Scope and main provisions
- § 11:4 —Remedies, liability and sanctions
- § 11:5 —Transfer of personal data outside EU
- § 11:6 ——Standard contractual clauses
- § 11:7 —Transfers of Personal Data to the United States
- § 11:8 Rules on data protection for email marketing
- § 11:9 The Data Retention Directive 2006/24/EC: Rules on retention of communications data

II. WORLD TREATIES AND COOPERATIVE INITIATIVES

- § 11:10 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
- § 11:11 —Privacy principles

- § 11:12 Council of Europe Convention 108
- § 11:13 —Data protection guidelines
- § 11:14 UN Guidelines for the Regulation of Computerized Personal Data Files

III. INFORMATION SECURITY ISSUES

- § 11:15 OECD guidelines for the security of information systems and networks: toward a culture of security
- § 11:16 OECD recommendation on Digital Security Risk Management for Economic and Social Prosperity-Principles
- § 11:17 Common criteria for information technology security evaluation
- § 11:18 —Overview
- § 11:19 —Structure
- § 11:20 —Key constructs
- § 11:21 —General security context
- § 11:22 Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
- § 11:23 —Substantive issues
- § 11:24 —Dispute resolution
- § 11:25 European Union regulatory instruments for network and information security
- § 11:26 —Network and information security
- § 11:27 —Attacks against information systems
- § 11:28 Council of Europe Convention on Cyber-Crime
- § 11:29 —Terms
- § 11:30 —Substantive criminal law
- § 11:31 —Criminal offenses
- § 11:32 —Ancillary liability and sanctions
- § 11:33 —Procedural law issues
- § 11:34 —International cooperation
- § 11:35 —Other provisions
- § 11:36 Major Decisions in EU Member States relating to the GDPR (2018–2021)
- § 11:37 Major decisions in EU member states relating to the EU data protection directive 95/46/EC (1998–2012)

CHAPTER 12. HEALTH CARE PRIVACY AND THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

- § 12:1 Introduction
- § 12:2 HIPAA privacy regulations generally
- § 12:3 Entities covered under HIPAA privacy regulations

TABLE OF CONTENTS

§ 12:4	—Health plans
§ 12:5	—Health care clearinghouses
§ 12:6	—Covered health care providers
§ 12:7	Information covered under HIPAA privacy regulations
§ 12:8	—De-identified information
§ 12:9	— —Limited data set
§ 12:10	Uses and disclosures of protected health information under HIPAA privacy regulations
§ 12:11	—Treatment
§ 12:12	—Payment
§ 12:13	—Health care operations
§ 12:14	— —Uses and disclosures for treatment, payment and health care operations of a third party
§ 12:15	—Required by law
§ 12:16	—Other exceptions to authorization requirement
§ 12:17	— —Public health activities
§ 12:18	— —Abuse, neglect or domestic violence
§ 12:19	— —Health oversight activities
§ 12:20	— —Judicial and administrative proceedings
§ 12:21	— —Law enforcement purposes
§ 12:22	— —Decedents
§ 12:23	— —Cadaveric organ, eye or tissue donation
§ 12:24	— —Research
§ 12:25	— —Threat to health or safety
§ 12:26	— —Specialized government functions
§ 12:27	— —Workers' compensation
§ 12:28	—Opportunity to agree or object
§ 12:29	—Incidental uses and disclosures
§ 12:30	—Authorization requirement
§ 12:31	Individual rights under HIPAA privacy regulations
§ 12:32	—Right to access and copy information in designated record set
§ 12:33	—Right to request amendment or correction
§ 12:34	—Right to accounting of disclosures
§ 12:35	—Right to request restriction
§ 12:36	—Right to specify how confidential information is communicated
§ 12:37	Notice requirement under HIPAA privacy regulations (notice of privacy practices)
§ 12:38	Notice requirement under HIPAA privacy regulations—Required elements
§ 12:39	—Revisions to notice of privacy practices
§ 12:40	—Dissemination of notice and written acknowledgment of receipt
§ 12:41	Minimum necessary standard under HIPAA privacy regulations

- § 12:42 Administrative obligations under HIPAA privacy regulations
 - § 12:43 —Privacy officer
 - § 12:44 —Training
 - § 12:45 —Security
 - § 12:46 ——Electronic protected health information
 - § 12:47 ——Flexible and scalable
 - § 12:48 ——Security requirements
 - § 12:49 ——Administrative safeguards
 - § 12:50 ——Physical safeguards
 - § 12:51 ——Technical safeguards
 - § 12:52 —Complaints
 - § 12:53 —Mitigation
 - § 12:54 —Breach notification analysis under the HITECH Act
 - § 12:55 —Breach notification obligations under the HITECH Act
 - § 12:56 —Sanctions
 - § 12:57 —Policies and procedures
 - § 12:58 Business associates under HIPAA privacy regulations
 - § 12:59 Organizational rules under HIPAA privacy regulations: Hybrid entities
 - § 12:60 Organizational rules under HIPAA privacy regulations: Affiliated covered entities
 - § 12:61 Organizational rules under HIPAA privacy regulations: Organized health care arrangements
 - § 12:62 Special requirements for group health plans under HIPAA privacy regulations
 - § 12:63 Research under the HIPAA privacy regulations
 - § 12:64 Marketing under HIPAA privacy regulations
 - § 12:65 Fundraising under HIPAA privacy regulations
 - § 12:66 Enforcement of HIPAA privacy regulations
 - § 12:67 State privacy laws
 - § 12:68 —Regulation by user
 - § 12:69 —Privilege
 - § 12:70 —Condition-specific confidentiality laws
 - § 12:71 —Comprehensive state privacy laws
 - § 12:72 —Breach notification under state privacy laws
 - § 12:73 State law claims based on HIPAA violations
 - § 12:74 Other federal privacy laws
 - § 12:75 —Genetic Information Nondiscrimination Act
 - § 12:76 —Gramm-Leach-Bliley Act
 - § 12:77 —Substance abuse regulations
 - § 12:78 —Privacy Act of 1974
 - § 12:79 Federal Agency Enforcement
 - § 12:80 Conclusion
 - § 12:81 Group health plan obligations under HIPAA privacy regulations

TABLE OF CONTENTS

§ 12:82	Significant definitions under HIPAA privacy regulations
§ 12:83	Administrative safeguards
§ 12:84	Physical safeguards
§ 12:85	Technical safeguards

CHAPTER 13. BANKING, FINANCIAL, AND INSURANCE INDUSTRIES

§ 13:1	Introduction
§ 13:2	Gramm-Leach-Bliley Act
§ 13:3	—Financial institutions
§ 13:4	—Nonpublic personal information
§ 13:5	—Affiliates
§ 13:6	—Consumers
§ 13:7	—Customers
§ 13:8	—Affiliated financial institutions
§ 13:9	—Contents of privacy policy notice
§ 13:10	—Method of delivery of privacy policy notice
§ 13:11	—Timing of initial privacy policy notice
§ 13:12	—Annual privacy policy notices
§ 13:13	—Exceptions to notice and opt-out
§ 13:14	— — Service processors
§ 13:15	— — Joint agreements
§ 13:16	— — Necessary to effect, administer, or enforce a transaction
§ 13:17	— — Consent of consumer
§ 13:18	— — Special relationships
§ 13:19	— — Other exceptions
§ 13:20	— — Reuse and redisclosure
§ 13:21	— Disclosure of account numbers
§ 13:22	— Enforcement
§ 13:23	Fair Credit Reporting Act
§ 13:24	— Scope
§ 13:25	— Investigative consumer reports
§ 13:26	— Business credit transactions
§ 13:27	— Consumer reporting agency
§ 13:28	— Prescreening
§ 13:29	— Obsolete information
§ 13:30	— Limits on investigative consumer reports
§ 13:31	— Medical information
§ 13:32	— Assuring that consumer reports are provided for permissible purposes
§ 13:33	— Accuracy
§ 13:34	— Disclosures to consumers
§ 13:35	— Resolution of credit reporting disputes
§ 13:36	— Nature of adverse action

- § 13:37 —Adverse action based on third-party information
- § 13:38 —The Fair and Accurate Credit Transactions Act of 2003
- § 13:39 —Affiliate sharing
- § 13:40 —Risk-based pricing
- § 13:41 —Identity theft prevention
- § 13:42 —Civil liability for willful noncompliance
- § 13:43 State financial privacy laws
- § 13:44 —Constitutional guarantees of privacy
- § 13:45 —Statutory approaches to financial privacy
- § 13:46 —Common law rights to financial privacy
- § 13:47 Electronic Funds Transfer Act: Initial disclosures
- § 13:48 Health Insurance Portability and Accountability Act:
 - Applicability to financial institutions
- § 13:49 Children's Online Privacy Protection Act:
 - Applicability to financial institutions
- § 13:50 Other federal privacy statutes: Electronic Communications Privacy Act
- § 13:51 Regulatory guidelines: Agency guidelines on safety and soundness
- § 13:52 Trends in cybersecurity and data protection litigation
- § 13:53 The future of breach notification laws: federal legislation
- § 13:54 The future of data security legislation: state legislation

CHAPTER 14. PERSONAL DATA PROTECTION LAWS AROUND THE WORLD

- § 14:1 Introduction
- § 14:2 Common themes among personal data protection laws
- § 14:3 Personal data protection laws around the world

Table of Laws and Rules

Table of Cases

Index