

# Privacy for the Pharmaceutical and Medical Device Industry: An Introduction

## Information Privacy

Of all the compliance topics addressed in these chapters, privacy may be the most pervasive. Privacy involves governing the use and protection of personal information, and there are few aspects of pharmaceutical and medical device companies that do not involve personal information in some ways.

Let us step back to better understand privacy. Four general categories of privacy are often considered:

- ❑ **Body.** The individual's body, including its external and internal characteristics, including genetics and health.
- ❑ **Environs.** The individual's location and presence in that location.
- ❑ **Communications.** The individual's communications with others, including interactions that form indirect communications.
- ❑ **Information.** Information about the individual.

This chapter focuses on information privacy as encountered by pharmaceutical and medical device companies.

The focus on privacy is the individual. An individual, sometimes referred to as a data subject, is a natural person.<sup>1</sup> An individual may be granted rights to privacy that the organization must honor. Personal information is any information about an identified or identifiable individual. That is, any information about an individual should be considered as personal information. The concept of an "identified" individual is straightforward: an individual is identified by a name or other identifier, an address or other contact method, or through some other manner directly in the information. The concept of an "identifiable" individual is often more difficult to comprehend. An identifiable individual is one, although not directly named in associated information, whose identity could be deduced through the information, directly or indirectly, to identify, contact, or locate. The concept of "identifiable" allows for the involvement of multiple parties perhaps each holding a piece of the information that can ultimately be used to identify the individual. For example, according to this very broad definition of personal information, in principle, coded trial records could be considered as personal information, as there is a chain of parties who could be traversed to ultimately link trial records to an investigator and ultimately a trial participant. The concept of identifiable individuals will be raised again concerning research and clinical operations, including secondary research.

Privacy, again, involves governing and protecting the use of personal information. There are two definitions of privacy that are specifically worth studying. The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) describe

---

<sup>1</sup> Some regulations apply privacy-like rights to legal persons (e.g., corporations, sole proprietorships, partnerships). This chapter does not address that aspect of privacy.

## Privacy for the Pharmaceutical and Medical Device Industry

privacy as, “The rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and destruction of personal information.”<sup>2</sup> In this definition, we note oftentimes a tension between the rights of the individual and the obligations of the organization, and that privacy extends through the lifespan of personal information—from its collection, through its use and retention, to its transfer to other parties and its ultimate disposal.

The International Association of Privacy Professionals (IAPP) defines privacy as, “The appropriate use of personal information under the circumstances. What is appropriate will depend on context, law, and the individual’s expectations.”<sup>3</sup> The appropriateness is related to the rights and obligations described in the AICPA/CICA definition, and is what makes privacy such a complex topic. What are the rights and obligations of the individual and the organization? What is appropriate use of personal information?

The key to determining appropriateness and responding with all that an organization needs to do to effectively manage privacy is first understanding the nature and intended uses of personal information throughout the enterprise. When personal information is identified, you can then ask, “Now, what are our obligations?” Different personal information about different individuals in different contexts carry different rights to the individual and different obligations to the organization. Managing privacy involves understanding all those differences and meeting the obligations.

One difference that affects privacy rights and obligations is that of the sensitivity of the personal information—to what extent would the unauthorized or unintended disclosure or use of personal information affect the individual? The European Commission sets forth special categories of personal data that include racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life, and data relating to offenses, or criminal convictions. Processing these special categories of personal data involves honoring additional rights to the individual and meeting additional obligations. From a United States (US) perspective, federal and state

**The European Perspective.** The European Commission set forth a comprehensive data protection directive mandating that member nations of the European Union (EU) enact and enforce data protection laws to govern the use of personal data. The European Commission’s definition of personal data pervades the laws of the member nations and of other countries with European-style privacy law.

“Personal Data. Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.”<sup>1</sup>

What is especially of interest in this definition is the fact that other factors may be used to relate to an identity besides a name or identification number. These factors may be significant related to the sales and marketing, patient and healthcare professional interactions, and clinical operations, where coded information may be used but obligations over the information remain.

European Commission, “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,” 1995.

<sup>2</sup> AICPA/CICA, “Generally Accepted Privacy Principles,” August 2009.

<sup>3</sup> IAPP, “IAPP Information Privacy Certification Glossary of Common Privacy Terminology,” 2010.

## Privacy for the Pharmaceutical and Medical Device Industry

regulations over privacy pay particular attention to health information, non-public personal financial information, and information that if misappropriated could be misused to commit identity theft and identity fraud. In general, when sensitive personal information is involved, the organization should recognize that there would be additional limitations on and obligations regarding the collection, use, retention, and disclosure of the personal information.

With personal information prevalent throughout pharmaceutical and medical devices companies and their extended enterprises and business partners, it is no surprise that privacy is such a pervasive issue. Personal information is used extensively and increasingly in the sales and marketing, clinical operations, and human resources management segments of pharmaceutical and medical device companies; and new sources and repositories of personal information are continuously being developed across the industry.

### Business Drivers

In general, businesses take on privacy to manage compliance with a growing number of laws and regulations that affect personal information, to manage business risks including those to brand and reputation, and to address increasing expectations of individuals over the use of information about them. Compliance is the primary driver, as privacy and data protection laws and regulations are gaining increasing coverage and are demanding reasonable processes and controls over personal information. Most major markets in which global pharmaceutical and medical device companies operate impose some form of privacy regulation, and many of those regulations govern as well the trans-border transfer of personal information. Multinational companies, therefore, must not only comply in their local operations, but must also address the exporting and importing ends related to the transfer of personal information across national borders.

Business risk management is also a significant driver, especially when personal information is a significant asset to the company and its effective operations. Privacy risk addresses the possible negative outcomes should personal information be inappropriately collected, misused, or disclosed to unauthorized parties. In addition to the business risks associated with enforcement should a law or regulation be violated, companies must understand and contend with risks associated with direct financial loss, lawsuits, damage to customer and business partner relationships, and damage to brand and reputation.

The case of Eli Lilly demonstrates the business risk impacts in addition to those from regulatory enforcement.<sup>4</sup> In 2002, Eli Lilly inadvertently sent an e-mail notice to all subscribers of its Medi-messenger service that contained in the To: field the e-mail addresses of all 669 registered subscribers. The US Federal Trade Commission (FTC) complaint alleged that Eli Lilly failed to implement or maintain reasonable and appropriate measures to protect consumer information including a failure to properly train employees, provide oversight, and implement appropriate checks and controls. Eight state attorneys general made a similar complaint. The enforcement outcomes included specific requirements for Eli Lilly's information security program and the requirement for that program to be audited by an independent third party every other year for 20 years. The event also contributed to the increased attention of foreign data

---

<sup>4</sup> Privacy and Information Management Services – Margaret P. Eisenhauer, P.C., “A Global Survey of Privacy and Security Enforcement Actions with Recommendations for Reducing Risks,” 2009.

## Privacy for the Pharmaceutical and Medical Device Industry

protection authorities (those agencies who oversee and enforce data protection law) on Eli Lilly and other multi-national pharmaceutical companies operating in their jurisdictions. A single process control failure contributed not only to an enforcement action but also to significant financial costs, an audit requirement, increased scrutiny for the company and the industry, and damage to the company's brand and reputation.

Privacy risk, however, is a very inexact process. Whereas privacy compliance obligations are specified in laws and regulations, and supported by common principles and industry standards, privacy risk management lacks a common approach and standards. When privacy risk is measured and managed, it is unlikely to be a mature, tested process or well integrated (if at all) into an organization's enterprise risk management approach. Whereas privacy risk should be actively and effectively managed, the current practices are informal, irregular, and poorly integrated. Improvements in privacy risk management are needed soon so that the significant business risks can be directly addressed.

The third category of privacy driver, managing the expectations of individuals, is the most difficult to measure and apply. Expectations vary greatly by individual and category of individual, and change over time. In some cases, such as with clinical trials and secondary research, the company may not even have a direct relationship with the individual. However, the social, cultural, and individual expectations related to privacy must be considered. Focus groups, surveys, and market research techniques may be applied to better understand expectations and the value of managing to those expectations.

## Privacy and the Business of Healthcare

Privacy is an issue everywhere personal information is collected, used, retained, and disclosed throughout the pharmaceutical or medical device company's extended enterprise. This includes from investigators to clinical research programs, from field sales forces to global customer relationship management systems, from local market customer care to global drug safety and reporting systems, and from local human resources (HR) management to global HR systems. Privacy extends across the corporate headquarters, through division headquarters to local market operating companies, shared services centers, joint ventures, co-marketing partners, and service providers. There are, in fact, few parts of the organization that have no impact related to privacy, no obligations over personal information, or no business risk associated with privacy.

For pharmaceutical and medical device companies, privacy issues may be divided into these main areas of focus:

- ❑ **Sales and marketing.** In this area, the data subjects include healthcare professionals and consumers to whom the company promotes its products, including key opinion leaders (KOL) and even marketing research participants. Business functions that involve personal information include sales force management, customer relationship management, marketing research, direct-to-healthcare professional marketing, direct-to-consumer marketing, sales management, prescribing history analysis, KOL management, event management, payment management, customer care, and brand or product web sites and online services. This area is increasingly complicated by sales and marketing regulations for both consumers and healthcare professionals, new aggregate spend reporting requirements, integrated and global customer relationship management and

## Privacy for the Pharmaceutical and Medical Device Industry

sales force management systems, globalization of markets, and use of new and innovative marketing techniques (e.g., web sites, social media).

- ❑ **Clinical operations.** In this area, the data subjects are participants in clinical trials and other research, and the investigators as well. Business functions that involve personal information include trial and research planning and management, clinical research organization and site selection and management, contract and authorization (including participant consent) management, participant recruiting and management, adverse event and medical device event reporting, pharmacovigilance, research and trial analysis and reporting, medical affairs, and medical information services. Clinical operations privacy is increasingly complicated by the execution of multi-national trials, secondary research<sup>5</sup>, centralized research facilities, and global research management systems.
- ❑ **Human resources.** In this area, the data subjects are employees and others engaged in the business of the company. Business functions that involve personal information span HR processes and include HR management, performance management, benefits management, talent management, recruiting and on-boarding, succession planning, payroll, and compensation management. This area gets increasingly complicated as industry harmonizes global HR processes and systems and at the same time relies on contractors, outsourced service providers, independent sales representatives, and other ventures and partnerships to supply its human resources.
- ❑ **External relations.** In this area, the data subjects are investors, facility visitors, regulators, public and patient advocates, and other external parties that the company may have records about, but with whom it usually does not have a direct relationship. Business functions that involve personal information include investor management (often relying on a service provider), facility management, events and external programs, corporate communications and outreach, and executive and facility protection. As with the other areas, this area is increasingly complicated through the use of global systems to support these business functions.

The industry, however, is embarking on innovative product and service development, including intelligent and interactive devices, integrated web services, expanded product and service lines, personalized medicine, and other exciting evolutions. These enhanced products and services are starting to blur the lines between the areas of focus described above, and will continue to add to the complexity and pervasiveness of privacy in the industry.

With all these areas of focus, however, the pharmaceutical industry is relatively mature in its approach to privacy compliance, especially with respect to those companies operating on a multi-national basis. With varying levels of effort and internal targets, the global pharmaceutical companies embarked on corporate privacy compliance programs between 2000 and 2004, with significant investments in governance, compliance programs, policies, and training from 2002 through 2008. Afterward, those programs have generally evolved as the markets expanded, mergers were undertaken, and even more complex issues arose. However, the large

---

<sup>5</sup> Association of the British Pharmaceutical Industry, "Guidelines for the Secondary Use of Data for Medical Research Purposes," 2007.

## Privacy for the Pharmaceutical and Medical Device Industry

pharmaceutical companies had established in the last decade solid foundations upon which they continue to build.

For the next decade, the top issues span a wide range from information security to privacy in new technologies. The main themes include:

- ❑ **Security of personal information.** Although computer security research has its roots in the late 1960s, information security in practice has proved a difficult undertaking. Many information security programs are stuck in the past, not addressing more modern threats and vulnerabilities and focusing too narrowly on information technology infrastructure. Companies must evolve to be able to address the specific threats to personal information—to the company and the individual. It must also evolve to be able to address the fact that the company is involved in an ongoing erosion of control and custody of personal information and computing devices to other parties, including healthcare professionals, consumers, independent sales forces, patients, caregivers, and many others.

Information security programs must be reengineered to protect personal information and the services and technology used to process that information, wherever they are in the extended enterprise. Confidentiality and integrity are classic protections, governing who may view or modify the information. Use controls are the next level of needed protections, determining not just who, but how, the personal information may be used. Information security monitoring and controls also need to be extended to remote and portable devices, third parties, and other elements of ever-extending enterprises. Information security for personal information is a critical element of the privacy and data protection regime for all pharmaceutical or medical device companies.

- ❑ **Process globalization and harmonization.** In many ways, process harmonization—whether in sales processes, clinical operations, or HR management—simplifies privacy compliance efforts. A single process and set of systems are put in place globally to perform the selected business functions. Privacy notices, consents, protections, and other controls may be standardized and even monitored from a central location. The challenge, however, comes from the global characteristics of the harmonized processes: personal information may now be more fluidly transferred across national borders, used by shared services or centralized service centers, and made available to a global workforce. When personal information crosses national borders, the transfer or remote access needs to be specifically legitimized with respect to local privacy and data protection laws and regulations. What was once a non-issue because of the variety of local and partitioned processes has now become exponentially challenging through such global flow of personal information.

The industry began the major efforts of sales, marketing, clinical, and HR process harmonization in the early 2000s. As the processes are increasing harmonized and globalized, the privacy and data protection compliance and risk management aspects become even more critical for the success of those projects. The industry will be addressing these challenges throughout the next decade as the processes continue to evolve.

## Privacy for the Pharmaceutical and Medical Device Industry

- ❑ **Third parties.** The industry has always had complex relationships among the various parties. In addition to traditional third-party service providers, pharmaceutical and medical device companies have been involved in complex business relationships with joint ventures, joint marketing and sales programs, independent sales forces, healthcare professionals, clinical research organizations, independent researchers, and complex global corporate structures. This industry competes only with the financial services industry in the scope and complexity of these third-party relationships.

Common practice involves focusing privacy due diligence and ongoing attention to a limited set of third parties: the service providers. As companies further cede control and custody of personal information throughout the entire healthcare system, they will need to expand their privacy compliance and risk management to deliberately address these other parties. Today, this is a significant undertaking, and it is only increasing in complexity and risk as the enterprise increases in complexity. The next decade must be marked with increasing maturity in the treatment of privacy compliance and risk management across all of the industry's third parties.

- ❑ **Expanded regulations.** The pace of new laws and regulations governing personal information has not slackened. In the first decade of the 21st century, we saw the creation of a firm foundation of national privacy and data protection laws across most of the northern hemisphere, in Australia and New Zealand, and beachheads made in South America, Africa, the Middle East, and South Asia. In the United States, without a national privacy law, we saw instead a patchwork of federal industry-sector-oriented laws and hundreds of state and local laws affecting how organizations may manage and use personal information, and how the information must be protected. In fact, the most complex privacy and security rules for personal information is embodied in those related to the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA), which initially took effect in 2001 and was updated into the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). HIPAA had limited effect on pharmaceutical and medical device companies. The HITECH Act, however, changed that considerably, when coupled with the industry's innovation of products and services, by extending many of the rules to the business associates of healthcare providers and payers.

At the end of 2009, much of the developed world was covered by some form of privacy and data protection law, and the powerhouse economies of Brazil, India, and China had significant public policy activity around privacy.<sup>6</sup> The net effect is that where the market is predominately regulated, or is expected to be regulated over the next decade. The industry, therefore, is faced with increased regulation in markets where it had not been specifically regulated before.

- ❑ **Smart and networked medical devices.** Another area of increasing scope for privacy compliance is the proliferation of smart and networked medical devices, which generate, store, process, and transfer increasing amounts of personal information. These devices

---

<sup>6</sup> A summary of the nature of privacy laws and regulations is provided later in this chapter.

## Privacy for the Pharmaceutical and Medical Device Industry

are not just used by healthcare providers, but are also used increasingly in home healthcare environments, in employee wellness programs, and by consumers using over-the-counter products. Pharmaceutical and medical device companies encounter these new sources of personal information in device maintenance, networked services, and portals and other web-based methods through which patients, consumers, and healthcare professionals share and process the medical device information.

As with third parties, the challenge includes not only the increase in personal information and its sources, but also the increasing loss of control and custody over the personal information. It is increasingly challenging for the company to extend its policies and controls over devices that are not in its possession or control. These smart devices, however, are increasingly prevalent and increasingly part of the peripheral services that the industry provides to patients, consumers, and healthcare professionals.

- ❑ **Global KOL accounting systems and transparency programs.** With the strong attention on the integrity of the industry's sales and marketing practices, transparency in spending related to KOLs and other healthcare professionals has become a significant requirement. Privacy comes into play as global companies consolidate payment and reimbursement information across a global base of KOLs and healthcare professionals, and report that information to advocacy groups, regulators, and other on a global basis. As mentioned, any time personal information (in this case, about the KOLs and healthcare professionals) is transferred across national borders, additional privacy requirements may come into play. The nature of relationships with KOLs and other healthcare professionals are undergoing transformation, as are the methods through which those relationships are managed. Even to get aggregate spend information, the company needs to process individual level information. As these accounting and reporting systems and processes are put in place and improved, privacy considerations and compliance obligations will play important roles.
- ❑ **New brand and market presence.** The industry spent most of the early 2000s with limitations on its sales and marketing efforts via websites and email, especially with respect to direct-to-consumer communications. By the end of 2009, web-based technologies had evolved and triggered new initiatives throughout the industry to engage patients, consumers, and healthcare providers more directly and more persistently, such as through interactive websites, and increased use of email and social media. As the next decade opens, the industry is leveraging its experience with its products and services into new ties with the healthcare providers, insurers, disease management firms, and others to create online services that will transform the industry's roles.

With these new technologies comes the need to extend what can now be considered old Internet privacy programs to be able to address the transition from static, brochure-oriented websites into interactive web-based services, oftentimes involving third-party websites and web services or even end-user technology such as smart medical devices, smart telephones, and kiosks. Transforming the old methods of covering Internet privacy to address these new methods will be a significant undertaking.

## Privacy for the Pharmaceutical and Medical Device Industry

Although each of these issues provides significant new and evolving challenges for pharmaceutical and medical device companies, the companies are also faced with the challenges of day-to-day management of privacy and data protection over the quite extensive and traditional portions of their businesses. These new challenges represent a significant increase in the level of effort and sophistication required of the industry over existing levels.

### Principles

Although privacy has been described as pervasive and complex, there are common principles of privacy practice that can help an organization simplify its views on privacy. These principles have evolved over time from the early 1970s to the present time and have formed the basis of privacy laws and regulations worldwide to varying degrees.

Privacy was described earlier in the chapter as, “The rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and destruction of personal information.”<sup>7</sup> In fact, the rights of the individual are most often directly translated into obligations for the organization, or at least into business risk related to the use of personal information. Therefore, as the principles are discussed, the focus will be the obligations of the organization—and more specifically, to pharmaceutical and medical device companies—over the lifespan of personal information.

The source of that description of privacy, the AICPA/CICA Generally Accepted Privacy Principles (GAPP) provide a compilation view of privacy and data protection principles from sources worldwide and will serve as the framework for the discussion of privacy principles in this chapter. To start, though, it is useful to have a historic perspective of modern privacy principles and to understand the primary multi-national instruments and standards that influence privacy and data protection across the globe.

- **U.S. Fair Information Practice Principles.**<sup>8</sup> With their foundation in an early 1970s publication by the former Department of Health, Education and Welfare, the Fair Information Practice Principles represents what the U.S. government sees as five common principles among United States, Canadian, and European sources. The application of these principles have evolved over time, but the principles themselves have withstood nearly 40 years of use. The Fair Information Practice Principles include those for:
  - Notice/Awareness
  - Choice/Consent
  - Access/Participation
  - Integrity/Security
  - Enforcement/Redress.

The Fair Information Practice Principles are not typically applied directly by an organization in managing its privacy risk and compliance, but rather have served as a significant source into U.S. and other countries’ privacy and data protection laws and regulations.

---

<sup>7</sup> AICPA/CICA, “Generally Accepted Privacy Principles,” August 2009.

<sup>8</sup> See the Resources section of this chapter for references to each of these sources of principles.

- ❑ **Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.** In 1980, the OECD published its privacy guidelines with the goal to “help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data.” These guidelines have since served as a foundation for national privacy and data protection laws and regulations in many countries. The guidelines are an important source for understanding common privacy principles. See the sidebar for an extract of the principles from the guidelines.<sup>9</sup>
- ❑ **European Union Data Protection Directive.** In 1995, the European Commission established “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data” with the purpose “to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.” In particular, the directive was intended to ensure that the free flow of personal data between member nations was not restricted. The directive impels member nations to establish and enforce national data protection law and supervising authorities (i.e., data protection authorities) consistent with the minimum requirements of the directive. Although companies must comply with applicable laws and regulations rather than with the directive (to which member nations must comply), the directive provides a comprehensive view of the common elements of national data protection law throughout the European Union. The directive has also served as an important foundation for other European Union-like national privacy and data protection laws, such as those in other European but non-Union nations (e.g., Switzerland, Norway, Iceland, Liechtenstein), the Russian Federation, and farther afield in Argentina.

The European Commission has issued other directives that compel member nations to legislate privacy and data protection. These include Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (referred to as the Directive on Privacy and Electronic Communications) and Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use (Clinical Trials Directive). The laws resulting from the Directive on Privacy and Electronic Communications affect the websites and other online services of pharmaceutical and medical device companies. The impact of the Clinical Trials Directive is less direct, as it mandates compliance with the Data Protection Directive and does not establish secondary requirements. However, for global companies, the need to transfer adverse event and medical device reporting to their affiliates in multiple countries and ultimately to the regulators involves significant transborder transfer of personal information, for which it is difficult to comply with both the Clinical Trials Directive and related reporting regulations in conjunction with data protection provisions.

---

<sup>9</sup> See the appendix for a listing of the principles.

## Privacy for the Pharmaceutical and Medical Device Industry

- ❑ **Asia Pacific Economic Cooperation (APEC) Privacy Framework.** In 2005, APEC published a privacy framework intended to “provide clear guidance and direction to businesses in APEC economies on common privacy issues and the impact of privacy issues upon the way legitimate businesses are conducted.” It states that the framework is consistent with the OECD privacy principles. Unlike the OECD privacy principles, the APEC privacy framework has yet to be a significant element of national privacy law in the region, and unlike the EU data protection directive, the APEC privacy framework is not binding on the member economies.
- ❑ **AICPA/CICA Generally Accepted Privacy Principles.** In 2003, and later in 2009, the leading audit associations in North America established the GAPP with the purpose “to be used as an operational framework to help management address privacy in a manner that takes into consideration many local, national, or international requirements.” The 10 principles and supporting criteria represent a common view of the operational requirements for privacy risk management and compliance. See the sidebar for an extract of the principles from the GAPP.<sup>10</sup>

In general, the principles can be divided into the following categories:

- ❑ **Principles related to the data subject.** These principles address the manner through which the organization must interact with the data subject to help fulfill individual rights. In general, this requires providing notice to the individual about what personal information is to be collected, how that information is to be used, to which other parties the information is to be disclosed or transferred, and the identity of the entity or entities processing the information. In the OECD terminology, this equates to purpose specification. It may require the organization to seek the consent of the data subject to permit the collection, use, and/or transfer of the personal information, or to provide choices about the use of the information or perhaps the future contact and communications with the individual, especially related to marketing. Finally, this category of principle addresses data subject access, through which the individual may understand whether the organization holds or processes personal information about the individual, to review that information, to amend the information if it is materially inaccurate, incomplete, or out-of-date, and to object to further processing of the personal information. In the OECD terminology, this is in general the individual participation principle. Although most privacy and data protection laws have common notice and choice/consent provisions, those related to data subject access vary widely.
- ❑ **Principles related to controls over the information.** These principles address the security and quality of the information and the underlying processes and technology used to process the personal information. In this case, security generally refers to the confidentiality, integrity, and availability of the information and the underlying processes and technology. This is the classic information security view and the principle in general requires reasonable controls and countermeasures according to the risk to the information and to the individual. Quality, also sometimes referred to as integrity (but in

---

<sup>10</sup> See the appendix for a summary of the Generally Accepted Privacy Principles.

## Privacy for the Pharmaceutical and Medical Device Industry

this case in a manner much more broad than in traditional information security practice), involves the accuracy, relevance, and timeliness of the personal information. In information security, integrity is the protection of information from unauthorized alteration. From a privacy perspective, quality and integrity involve the appropriateness of the information for the purposes of processing it. Information should be appropriate, not excessive, and up-to-date. Whereas quality is a condition of the information, it is not necessarily just a technology issue, but rather addresses the suitability of the information for the specified purpose.

- ❑ **Principles related to the information lifespan.** Based on the notice (i.e., purpose specified) and the consent received from the individual, choices selected by the individual, and an understanding of what is further allowed, not-prohibited, and prohibited by law, regulation, or other agreement, the organization can manage the lifespan of personal information. The principles in this category relate to limitations on the collection, use, retention, and disclosure and transfer of the personal information. In general, those lifespan processes are limited to the purpose specified, balanced by consent and choice (if applicable), and what is fair and lawful within the jurisdiction. Even absent specific limitations in laws and regulations, an organization may be obligated to limit processing if it states that it will or will not process the information in a certain manner; in this case, the notice to the individual may become a binding requirement. Concerning the disclosure or transfer of personal information to other parties, the principles consider under what conditions such a transfer is allowed and whether those conditions are met.
- ❑ **Principles related to managing privacy.** Principles pertaining to privacy management involve assigning responsibilities, managing risks and compliance throughout the use of personal information, monitoring programs and controls put in place to uphold the other principles, and enforcing policies and obligations under laws and regulations. Although privacy management principles are usually at a very high level, they involve significant details and complex processes when put into operations. More will be discussed about this in the “Managing Privacy” section.

These principles indicate what conditions need to be upheld when handling personal information; they do not, however, indicate how privacy should be managed. A framework for managing privacy across the enterprise is described in the “Managing Privacy” section below.

### Laws and Regulations

Most modern privacy and data protection laws and regulations embody some or all of the common privacy principles, and have their roots in one or more of the sources described earlier. This gives them certain commonalities and an organization’s response to them considerable consistency. That said, there are routinely differences between privacy laws and regulations, whether in their scope of applicability, the administrative processes required, or the authority and power of the supervising bodies. Therefore, when considering privacy laws and regulations, the following aspects should be understood:

#### Obligations of the Organization

## Privacy for the Pharmaceutical and Medical Device Industry

- ❑ **Notice.** The organization must provide certain notice of its use of personal information, including the nature of information collected, purposes for which it is processed, its exchange with other parties, choices and rights of the individual, methods used to secure the information, and redress methods.
- ❑ **Security.** The organization must provide reasonable security controls over the security of the personal information, including technical, physical, and administrative controls.
- ❑ **Quality.** The organization must ensure that it collects and uses personal information that is relevant, timely, and accurate with respect to the purposes for which it is used.
- ❑ **Limitations on collection, use, retention, and disclosure.** The organization must manage personal information throughout its lifespan as stated in its privacy notice or as otherwise permitted.

### Rights of the Data Subject

- ❑ **Consent and object.** The individual may have the option to provide or withhold consent over the collection, use, and transfer of personal information, and in some cases the right to object to further processing of the personal information.
- ❑ **Access.** The individual may have the right to determine if an organization processes personal information about that individual, to determine the nature of that information, to review that information for accuracy, and to cause its modification or update as warranted.
- ❑ **Redress.** The individual may have the right of redress in case the individual has inquiries, complaints, or cause to believe that the organization has violated the terms of the privacy notice, regulations, or other terms.

### Administration and Enforcement

- ❑ **Powers of the regulators.** Regulators have varying powers, including over such as the powers to investigate, audit, sanction, and make rules.
- ❑ **Penalties and sanctions.** The laws may indicate methods through which penalties and sanctions are imposed (e.g., through courts, direct regulator actions, consent orders) and the ranges and levels of penalties and fines that may be imposed, including whether the penalties are civil or criminal.
- ❑ **Administrative processes.** The laws may impose varying administrative processes, such as for notifying or registering with a data protection authority related to the processing of personal information, seeking authorization or approval for the processing, or certifying compliance with certain requirements.

Most components of privacy and data protection laws and regulations can be considered in these dimensions. There are, however, considerably different approaches taken among laws and regulations.

## Privacy for the Pharmaceutical and Medical Device Industry

The following summarizes the nature of privacy and data protection laws and regulations that are significantly applicable to pharmaceutical and medical device companies operating in various countries and regions. A thorough analysis of applicable rules should be undertaken with competent legal counsel to determine the actual compliance obligations in the very specific context of the companies' operations.

### United States

At the federal level, pharmaceutical and medical device companies are beginning to be more directly affected by the regulations stemming from the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the changes to HIPAA from the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. Originally affecting only those portions of pharmaceutical and medical device companies that were more directly involved with patient care or employee health insurance, more and more of the industry is now affected as business associates to healthcare providers and insurers under the changes from the HITECH Act. These changes compel those organizations affected to meet the HIPAA security rules and to comply with many of the HIPAA privacy rules. The HITECH Act also mandated security breach notification rules related to the loss of protected health information. The US Department of Health and Human Services Office of Civil Rights enforces HIPAA regulations.

Other general industry regulations that affect the industry include those for email marketing under the Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act of 2003, which is enforced by the U.S. Federal Trade Commission. Other federal laws and regulations may affect certain aspects of the industry's operations, but these are the predominate regulations for which to be concerned.

At the state level, a wider range of regulations related to privacy comes into scope. Focused on identity theft protection, most states have enacted security breach notification regulations to compel organizations to notify a consumer protection agency or state attorney general and possibly to individuals potentially affected by the loss of control or unauthorized access to personal information that includes credit card or other financial account numbers, Social Security numbers, or driver license numbers. Although there are common principles among the state laws, there are enough differences to warrant careful review of each state's regulations and reporting requirements.<sup>11</sup>

In 2010, the Commonwealth of Massachusetts began enforcing its Standards for the Protection of Personal Information of Residents of the Commonwealth (Massachusetts 201 CMR 17), which added a set of requirements for a written information security program and certain security controls over personal information (also which was defined to include names with credit card or other financial account numbers, Social Security numbers, and driver license numbers). The important outcome of this regulation is that companies that process such information about a resident of Massachusetts (whether or not the company has local operations) must adequately protect that personal information through an information security program at least as robust as

---

<sup>11</sup> The National Conference of State Legislatures provides listings of current laws and regulations related to privacy. Please see the "Resources" section in this chapter for a reference.

## Privacy for the Pharmaceutical and Medical Device Industry

is indicated in the regulation. The standard in effect regulates information security programs over such information.

Some states also regulate marketing, the use of pharmacy and prescribing physician information, and healthcare privacy as a whole. For example, Maine and Vermont both have regulations that allow healthcare professions to choose whether their prescribing data may be disclosed for the purpose of marketing purposes. Similar regulations are being considered by other states, and the practice of allowing physicians to opt out of such use of prescribing data is already part of the American Medical Association's self-regulatory Physician Data Restriction Program. This topic is tangential to the privacy of individuals, but it is managed using many of the same practices with which individual privacy is managed.

Overall, the states represent a chaotic collection of such laws and regulations that mandate the industry's attention. Frequent additions and modifications to laws and regulations only complicate that chaos.

### Canada

At the federal level, Canada issued the Personal Information Protection and Electronic Documents Act (PIPEDA) of 2000 that governs the use and protection of personal information, covering among other entities those that process personal information in their commercial activities. The principles of the act are similar to those outlined above, and the Office of the Privacy Commissioner of Canada has enacted implementing regulations and offers detailed guidance on the rules. If the provinces in which the commercial activity is undertaken have substantially similar privacy laws, compliance with those provincial laws is mandated.<sup>12</sup> As of 2010, British Columbia, Alberta, and Quebec are the only provinces with laws recognized as substantially similar to PIPEDA. These laws regulate the collection, use, and disclosure of personal information by businesses and other organizations and provide individuals with a general right of access to, and correction of, their personal information. Ontario, meanwhile, has adopted privacy legislation to protect personal health information that has been recognized as substantially similar. However, PIPEDA applies to personal information in inter-provincial and international transactions by all organizations engaged in commercial activities.

### Europe

The majority of European nations are members of the European Union. The other European nations in general have data protection laws that are substantially similar to those required by the EU Data Protection Directive. European Union member-nations have enacted data protection law in accordance with at least the minimum provisions of the EU Data Protection Directive and EU Privacy and Electronic Communications Directive. In addition, the national, and in some cases, state level data protection authorities issue additional regulations and guidance over data protection.

As mentioned earlier, European Union member-nations have also enacted laws to implement the EU Clinical Trials Directive. They require adherence to national data protection regulations in the execution of the provisions of the clinical trial-related laws.

---

<sup>12</sup> Information about Canadian provincial and territorial privacy laws and regulators can be found at [http://www.priv.gc.ca/resource/prov/index\\_e.cfm](http://www.priv.gc.ca/resource/prov/index_e.cfm).

## Privacy for the Pharmaceutical and Medical Device Industry

Another source of guidance and opinion for European Union data protection is the so-called Article 29 Working Party of the European Commission, made up of representatives of the EU national data protection authorities. The Article 29 Working Party interprets the EU Data Protection Directive for specific issues, and has established a wide range of guidance over the topic of data protection.

A key provision of EU data protection is the requirement for data exporters to legitimize the trans-border transfer of personal information outside the European Union and broader European Economic Area. In addition to the various derogations that can be used—including contract provisions or consent of the individual—U.S.-based companies may be able to join and self-certify to the U.S. Safe Harbor Privacy Program<sup>13</sup>, established by the U.S. Department of Commerce in 2001, to provide a basis for such legitimate transfer. The U.S. has also established a similar program to assist with legitimate transfers of personal information from Switzerland to the U.S.

### Asia-Pacific

Unlike Europe, the Asia-Pacific region exhibits little commonality in its approach to privacy laws and regulations. The APEC Privacy Framework does not mandate national privacy law but rather is intended to guide member economies when considering such a law. Hong Kong, Australia, and New Zealand were in the leading wave with privacy laws and were followed by Japan and more recently Malaysia. In India and China, provisions for privacy-related law have been part of legislative debate, but have yet to reach maturity. Other nations in the region lack general privacy laws and regulations, but may have certain provisions, such as in banking secrecy laws, that affect other industries.

### Middle East and Africa

This region predominately lacks regulation over personal information. Therefore, like the Asia-Pacific region, the diversity in the Middle East and Africa will likely ensure that the future treatment of privacy and data protection will remain inconsistent. Morocco, Tunis, Israel, South Africa, and the International Finance Center in Dubai have national data protection laws. The principles are similar to those found in Europe, but to date the countries have not been determined by the European Commission to be adequate for more seamless transfer of personal information from the European Union.

### South and Central America

Like the Asia-Pacific region, South and Central America are a patchwork of different treatments for privacy and data protection. Argentina led the region by enacting a national data protection law in 2000 that was modeled generally on European Union principles. Later, Argentina was deemed “adequate” by the European Commission, which among other things helps to legitimize the transfer of personal information from the European Union to Argentina without additional legal and regulatory burdens. By 2010, Mexico had followed Columbia, Uruguay, and Chile with some form of general, national privacy, or data protection law. The scope, principles, authority, and enforcement varies significantly, as do the rights of the individuals.

---

<sup>13</sup> Information about the U.S. Safe Harbor Privacy Program may be found at <http://www.export.gov/safeharbor>.

## Privacy for the Pharmaceutical and Medical Device Industry

In summary, much of the world's largest markets are governed by significant privacy and data protection laws and regulations, and the largest of the emerging economies of Brazil, India, and China have been exploring such legislation. Although there are common principles, outside of Europe there remains a significantly varied approach to implementing those principles in the laws and regulations, and significant differences in the administrative processes, authorities, and enforcement climates. These differences result in a situation allowing organizations to govern privacy with a global set of privacy principles and policies but require them to operationalize those principles and policies differently in each jurisdiction.

### Managing Privacy

Privacy is driven by an increasingly complex and pervasive set of rules and risks affecting nearly every aspect of the organization. Complexity comes from a vast set of national and local laws and regulations, corporate policies, operational procedures, contractual terms, and service agreements over the use of personal information. Complexity is also derived from the diverse business functions that process personal information and the information technology used to collect, create, process, store, and transfer the information, especially so for pharmaceutical and medical device companies.

In fact, privacy is an issue in all situations where personal information is handled, from data centers and production systems to third parties and end user devices well outside the control and custody of the organization. This pervasiveness also means that privacy is not the domain of an isolated compliance group, but rather an enterprise-wide concern, spanning research and development, products and services, sales and marketing, clinical operations, information technology operations, human resources, and the third-parties with whom the enterprise exchanges personal information. The net result is that privacy has become one of the most demanding business issues facing organizations today.

The larger pharmaceutical and medical device companies to date have at least put foundational privacy governance, risk management, and compliance (GRC) functions in place; that is, most have done something to manage privacy, at least at the level of the corporate office and for global processes and business units. For these organizations, investment in privacy GRC, therefore, should be focused on evolving from the functions being in place to being effectively managed. This is even more critical for organizations with multiple business units, in multiple countries or jurisdictions, or with multiple regulators. Enhanced privacy GRC means that the processes in response to risk and compliance obligations are done well and operate with efficiency. To do this, organizations should:

- ❑ **Formalize privacy GRC functions.** The Sarbanes-Oxley era ushered in the saying, "If it isn't documented, it isn't done." The saying implied that there was a lack of assurance that something was being done if there was no record of it, and if it was actually done there was little evidence that it was done well and could be done again with a similar outcome. Business functions worth doing are worth documenting. This goes for privacy GRC functions as well. Therefore, the first objective is refining and documenting the supporting processes.
- ❑ **Monitor privacy GRC functions.** There are several truths relevant to monitoring. The first is, "Anything that can be done can be measured." In fact, the biggest challenge is

## Privacy for the Pharmaceutical and Medical Device Industry

taking measurements that matter. That saying is further supported with the following, “That which gets measured gets done.” If you do something but do not measure it, you cannot demonstrate that your privacy GRC initiatives are in place, complete, compliant or effective. The next objective, therefore, is adding monitoring to privacy GRC functions, not just at a central point but also throughout the organization where the functions are performed. This monitoring could be performed through administrative procedures, but technology-enablement is fundamental.

- ❑ **Automate privacy GRC functions.** Dozens of national laws and hundreds of implementing regulations and good practice guidelines affect multinational companies. If you add to that burden the U.S. states, Canadian provinces, industry standards, corporate policies, and contractual requirements, you get more than will fit neatly in a chart or spreadsheet. The key to technology enablement is to automate an effective process. It has been said of automation that, “Automation applied to an efficient operation will magnify the efficiency, whereas automation applied to an inefficient operation will magnify the inefficiency.” Automation is needed for policy management, risk management, compliance management, incident management, monitoring, and internal control itself, if nothing else but to streamline the non-value-added and administratively burdensome activities. The third objective is enabling privacy GRC functions with technology to support their effective performance and monitoring.

These objectives form a triumvirate for enhancing privacy GRC. Organizations with a mandate for effective and efficient business processes need to formalize, monitor, and automate the functions in privacy programs and those that operationalize privacy GRC within the business units themselves.

With those objectives in mind, a structured and complete view of privacy GRC is required. This privacy framework offers a method to organize privacy GRC. It is briefly illustrated below.

Governance Level		
Governance	Risk Management	Compliance

Control Level					
Policy	Internal Control	Technology Management	Third Party Management	Incident Management	Training and Awareness

Information Level		
Process	Entities	Technology

Starting at the **Information Level** as a foundation, the organization must understand and account for the processes that handle personal information, the entities that perform those processes (i.e., the first, second, third, and even fourth parties), and the technology and media used to collect, create, use, store, and transfer the personal information. Without such an

## Privacy for the Pharmaceutical and Medical Device Industry

understanding, the organization cannot effectively apply controls or govern the use and protection of the personal information.

At the **Control Level**, the organization establishes business rules (e.g., through policies and procedures) over personal information, implements an environment of internal control, manages the technology and other parties involved, manages incidents and other events including those that might be indicative of a breach, and undertakes the training and education of users of personal information. The Control Level includes the following components:

- ❑ **Policy** addresses the various corporate, business unit, and affiliate policies, procedures, guidelines, and standards that govern the use, protection, and retention of personal information throughout the operations. In addition to addressing the privacy policy, the assessment also covers aspects of other policy that is related to the use of personal information.
- ❑ **Internal Control** addresses the core privacy principles (e.g., the AICPA Generally Acceptable Privacy Principles) over the organization's lifecycle handling of personal information. Internal Control is often implemented within specific business units and affiliates (e.g., human resources management, marketing, country operations), and within specific business functions (e.g., consumer sales, consumer marketing, benefits management, call center operations).
- ❑ **Technology Management** addresses the traditional aspects of information security along with risk management and compliance processes related to information technology management and operations. It extends to all information technology used by the organization and other parties (e.g., third parties, individuals) to process personal information. It addresses technology used in all environments, including production, test, development, and maintenance environments, whether performed in-house, outsourced, in the hands of end users, or in events of contingency operations (e.g., when executing business continuity response plans). In addition, Technology Management accounts for logical controls (e.g., provided in software and hardware) and physical and administrative controls over technology.
- ❑ **Third Party Management** addresses the risk, compliance, and control environments related to third parties that process personal information related to the organization across all business functions and affiliates. It includes traditional service providers, business partners, and other parties that have control or custody of the personal information (e.g., cloud and utility computing and information service providers).
- ❑ **Incident Management** addresses the extent to which the organization has established effective processes to identify and resolve incidents and other events involving personal information.
- ❑ **Training and Awareness** addresses the organization's approach to informing users of personal information of the policies, practices, and other obligations over that information.

## Privacy for the Pharmaceutical and Medical Device Industry

At the **Governance Level**, the organization establishes the roles and responsibilities throughout the enterprise, identifies and assesses privacy risk, and establishes compliance functions associated with privacy and personal information. The Governance Level includes the following components:

- ❑ **Governance** addresses the roles, responsibilities, and authorities across the organization related to privacy and the use of personal information. The roles may span from rule making and monitoring, to coordinating, and to enabling and consultative at the corporate levels, and to operational responsibilities in the business units and affiliates.
- ❑ **Risk Management** addresses the processes that the organization has put in place to identify, assess, and manage risks related to personal information throughout the enterprise. This could be accomplished through the enterprise risk management, IT risk management, privacy risk management, internal audit, or other processes, either integrated with broader risk management efforts or as a discrete initiative.
- ❑ **Compliance** addresses the establishment of processes, monitoring, and review of privacy and data protection with respect to policy, law, regulation, and other compliance obligations.

Organizations with privacy GRC in place will have something in each of the components of the framework. Improvements in privacy GRC will require changes not in *what* gets done, but rather in *how* it gets done. Formalization, monitoring, and automation are keys to evolving privacy GRC maturity.

Using the privacy framework, an organization can develop a comprehensive approach to automating privacy GRC. With technology enablement in mind, key considerations include the following:

- ❑ **Information Level**
  - **Process.** Cataloging processes that handle personal information.  
Many organizations focus on information in databases, servers, and workstations. The purpose for which the personal information is used, however, is key to determining privacy requirements, such as those for notice, choice and consent, subject access, and even process and application controls.
  - **Entities.** Cataloging legal entities that handle personal information.  
As legal entities are ultimately responsible for complying with privacy laws and regulations, and the nature of the legal entities is a factor in privacy risk. Entities include affiliated (e.g., parent, subsidiary, and peer companies) parties and unaffiliated (e.g., third and even fourth) parties.
  - **Technology.** Scanning to discover personal information in networks, databases, servers, workstations, and other user devices.

## Privacy for the Pharmaceutical and Medical Device Industry

The presence of personal information can be assessed for its appropriateness, and the protection measures for personal information in the different technologies may be assessed for adequacy.

### □ Control Level

- **Policy.** Creating and registering policies, procedures, and guidelines, and communicating them throughout the organization.

Policy needs to be in the right hands at the right time. Policy management may automate the communications of policy, acknowledgement and certification to its objectives, and updates and clarifications over time.

- **Internal Control.** Implementing and assessing the effectiveness of process and application controls over personal information.

In fact, without automation of internal control, both implementing it and monitoring it, an organization cannot effectively manage privacy. Many organizations need to move beyond automation of internal control solely for financial process and rather deliberately include the myriad of other business processes that use personal information.

- **Technology Management.** Identifying and managing technology assets and their configurations (e.g., related to vulnerability management).

Many organizations have insight regarding core technology assets but lack coverage of portable devices. As we see personal information being processed more and more in end-user devices that are not within the direct control or custody of the organization, technology management becomes an increasingly important element of privacy GRC.

- **Third-Party Management.** Managing the selection, contracts, engagement, ongoing assurance, and termination of third parties that handle personal information for the organization.

It is difficult enough to manage risk, compliance, and internal control within the organization. Tools, therefore, are critical in managing the processes associated with third parties with which you exchange or who access your personal information.

- **Incident Management.** Managing the lifespan of incidents and other events related to personal information, including discovery, analysis, resolution, communication, root cause analysis, and tracking.

Regulations over incident management and breach notification require effective approaches, which cannot be effective unless enabled with technology for recording facts and decisions, and managing workflow throughout the lifespan of an incident.

- **Training and Awareness.** Publishing, communicating, and monitoring privacy-related training programs, including ongoing awareness communications.

## Privacy for the Pharmaceutical and Medical Device Industry

Many organizations already deliver some training and awareness through web-based learning tools, email, and intranets. The next step is monitoring progress and measuring the effectiveness of that delivery.

### □ Governance Level

- **Governance.** Documenting and communicating responsibilities to employees and management, and monitoring performance to those responsibilities as a component of performance management. Reporting on policy and business decisions made related to privacy risk management and compliance.

For many, the first step in improving governance will be formalizing it, especially within business units, and integrating that formalization into role and performance management systems. However, automating governance also involves integrating reviews, decisioning, and authorizations within business processes themselves. Enabling governance with technology, therefore, will involve its integration into other process automation throughout the organization.

- **Risk Management.** Identifying, planning, and assessing privacy risk across the enterprise and in a manner integrated with other enterprise risk management functions.

This aspect of automation often involves applying enterprise risk management and IT risk management tools to specifically address privacy risk. Often the first step is using those tools to discretely address privacy-related risk, whereas more mature organizations will move to integrate privacy-related risk with the management of the other business risks faced by the organization.

- **Compliance.** Managing compliance requirements and correlating them with operational, technical, legal, and administrative controls. Planning and conducting compliance assessments and audits. Implementing technical and process control monitoring, and where feasible continuous controls monitoring.

An initial step to improving the performance of compliance is accounting for the various often-overlapping rules and regulations over personal information. However, real improvement can be seen when those overlapping rules and regulations are correlated so that internal control and monitoring can be rationalized. That rationalization is among the improvements with the highest potential in the effective performance of privacy GRC.

Addressing these dimensions will help you move to an enhanced posture for managing privacy GRC across the enterprise.

Early in the new century, privacy management involved putting key elements of a program in place. A few years later, it was about extending coverage of privacy functions and activities across the enterprise with better integration with the information technology department and liaisons within various business units. For organizations with privacy GRC in place and coverage nearly there, the focus needs to include running the privacy function as would be expected of other parts of the business: effectively and efficiently. A goal for this enhanced privacy GRC in the new decade will require formalizing, monitoring, and automating those privacy GRC functions.

## Privacy for the Pharmaceutical and Medical Device Industry

### Resources

The following are the primary resources useful when addressing privacy and data protection by pharmaceutical and medical device companies.

Organization	Resources	Reference
<b>American Institute of Certified Public Accountants</b>	Generally Accepted Privacy Principles and other resources	<a href="http://www.aicpa.org/privacy">www.aicpa.org/privacy</a>
<b>Asia Pacific Economic Cooperation</b>	APEC Privacy Framework, Privacy Pathfinder Project, and related information	<a href="http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.html">www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.html</a>
<b>Association of the British Pharmaceutical Industry</b>	Guidelines for the Secondary Use of Data for Medical Research Purposes	<a href="http://www.abpi.org.uk/Details.asp?ProductID=315">http://www.abpi.org.uk/Details.asp?ProductID=315</a>
<b>Canadian Institute of Chartered Accountants</b>	Generally Accepted Privacy Principles and other resources	<a href="http://www.cica.ca/privacy">www.cica.ca/privacy</a>
<b>Department of Health &amp; Human Services</b>	HIPAA resources	<a href="http://www.hhs.gov/ocr/privacy">www.hhs.gov/ocr/privacy</a>
<b>European Commission</b>	Data protection resources	<a href="http://ec.europa.eu/justice/policies/privacy/index_en.htm">ec.europa.eu/justice/policies/privacy/index_en.htm</a>
<b>Federal Trade Commission</b>	FTC general privacy resources; U.S. Fair Information Practice Principles	<a href="http://www.ftc.gov/privacy">www.ftc.gov/privacy</a> ; <a href="http://www.ftc.gov/reports/privacy3/fairinfo.shtm">http://www.ftc.gov/reports/privacy3/fairinfo.shtm</a>
<b>International Association of Privacy Professionals</b>	Membership information, knowledge resources, news alerts, and other resources	<a href="http://www.iapp.com">www.iapp.com</a>
<b>National Conference of State Legislatures</b>	U.S. state privacy and identity theft protection law listings	<a href="http://www.ncsl.org/Default.aspx?TabID=756&amp;tabs=951,71,539#539">www.ncsl.org/Default.aspx?TabID=756&amp;tabs=951,71,539#539</a>
<b>Office of the Privacy Commissioner of Canada</b>	Canadian federal laws, regulations, and guidelines, including links for provincial and territorial privacy commissions	<a href="http://www.priv.gc.ca">www.priv.gc.ca</a>
<b>Organization for Economic Cooperation and Development</b>	Guidelines on the Protection of Privacy and Transborder Flows of Personal Data	<a href="http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html">www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html</a>

### Appendix

The appendix contains listings of the OECD Privacy Principles and a summary of the Generally Accepted Privacy Principles.

**OECD Privacy Principles.** The OECD privacy principles warrant special attention because of their historic nature and their influence over more than 30 years in privacy and data protection laws and regulations worldwide.

## Privacy for the Pharmaceutical and Medical Device Industry

### ❑ **Collection Limitation Principle**

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

### ❑ **Data Quality Principle**

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

### ❑ **Purpose Specification Principle**

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

### ❑ **Use Limitation Principle**

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- a) with the consent of the data subject; or
- b) by the authority of law.

### ❑ **Security Safeguards Principle**

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

### ❑ **Openness Principle**

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

### ❑ **Individual Participation Principle**

13. An individual should have the right:

- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
- c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
- d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

### ❑ **Accountability Principle**

14. A data controller should be accountable for complying with measures that give effect to the principles stated above.

As with the Fair Information Practice Principles, the fundamental elements of these principles can be seen in modern information privacy and data protection laws and regulations.

## Privacy for the Pharmaceutical and Medical Device Industry

**AICPA/CICA Generally Accepted Privacy Principles.** The Generally Accepted Privacy Principles will serve as the basis for the further discussion of common privacy principles in this chapter. The overall privacy objective served by the GAPP is that “Personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the entity’s privacy notice and with criteria set forth in Generally Accepted Privacy Principles issued by the AICPA and CICA.” The underlying principles are as follows:

- ❑ **Management.** The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
- ❑ **Notice.** The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
- ❑ **Choice and consent.** The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
- ❑ **Collection.** The entity collects personal information only for the purposes identified in the notice.
- ❑ **Use, retention, and disposal.** The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
- ❑ **Access.** The entity provides individuals with access to their personal information for review and update.
- ❑ **Disclosure to third parties.** The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
- ❑ **Security for privacy.** The entity protects personal information against unauthorized access (both physical and logical).
- ❑ **Quality.** The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
- ❑ **Monitoring and enforcement.** The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

Both the AICPA and CICA offer resources and references aligned to the GAPP to help organizations with privacy risk management and compliance functions, including privacy audit and controls.