LITTLER ON
DATA PROTECTION
& RELEASE OF
PERSONAL INFORMATION:
HIPAA & Related Laws

Authors:
Philip L. Gordon
Kwabena A. Appenteng
Morgan J. Matson
ABOUT THE AUTHORS

Philip L. Gordon is a shareholder in the Denver office of Littler Mendelson, P.C., the largest U.S.-based law firm exclusively devoted to representing management in labor and employment law. He is also co-chair of the Privacy and Background Checks Practice Group. Philip has years of experience litigating privacy-based claims and counseling clients on all aspects of workplace privacy and information security. He has provided advice to businesses of all sizes on: surveillance of employees’ electronic communications; the Federal Wiretap Act; the Federal Stored Communications Act; workplace searches; location tracking and use of GPS-enabled devices; background checks, the Fair Credit Reporting Act (FCRA); social media and other new technologies affecting the workplace; the Health Insurance Portability and Accountability Act (HIPAA); state data protection laws; responding to security breaches; the European Union Data Protection Directive; global data protection laws; cross-border transfers of human resources data; outsourcing; and the Genetic Information Nondiscrimination Act (GINA). Philip also has substantial experience representing employers in disputes involving misappropriation of trade secrets, claims of unfair competition and charges of wrongful termination. In addition, he regularly counsels businesses on compliance with the Americans with Disabilities Act’s Accessibility Guidelines and frequently defends businesses against claims of public accommodation discrimination. Philip writes extensively on workplace privacy issues and has given dozens of presentations on the topic.

Kwabena A. Appenteng is an associate in Littler’s Chicago office. He represents and counsels clients on a range of employment issues with a focus on workplace privacy issues, including responding to security breaches, state data protection laws, social media laws, workplace surveillance laws and issues stemming from the Health Insurance Portability and Accountability Act (HIPAA). Kwabena is a Certified Information Privacy Professional for the U.S. private sector and Europe (CIPP/US; CIPP/E). These credentials from the International Association of Privacy Professionals (IAPP) indicate his understanding of global concepts of privacy and data protection laws, and how these components apply in the workplace. Kwabena is a frequent writer on privacy topics, and has been published in a variety of publications. He also routinely speaks and gives presentations on privacy-related topics.

Morgan J. Matson, an associate in Littler’s Pittsburgh office, provides strategic advice and counsel to multinational employers on a wide range of employment and compliance matters. Morgan regularly advises employers on the intricacies associated with managing a global workforce, including such areas as data privacy, global codes of conduct and international policies and global mobility and expatriate programs. She frequently publishes and speaks on data privacy issues.
COVERAGE

Scope of Discussion. The unauthorized access to and improper disclosure of personal information has serious consequences to both organizations and the individuals involved. There are several federal and state laws that: govern the myriad types of personal information (Social Security numbers, health information, etc.); define “personal information;” determine whether, and to what extent, employees can access their own personnel files; govern the use, disclosure and destruction of various types of personal and health information; and dictate notification requirements when there is a data breach. This publication also looks at international laws in this area, including the European Union’s strict data protection laws. The publication is designed to provide an employer with an overview of potential areas of risk and offers compliance guidance on several topics.

Disclaimer. This publication is not a do-it-yourself guide to resolving employment disputes or handling employment litigation. Nonetheless, employers may find the information useful in understanding the issues raised and their legal context. This publication is not a substitute for experienced legal counsel and does not provide legal advice regarding any particular situation or employer or attempt to address the numerous factual issues that inevitably arise in any employment-related dispute.

Although the major recent developments in federal employment and labor law are generally covered, this publication is not all-inclusive and the current status of any decision or principle of law should be verified by counsel. The focus of this publication is federal law. Although some state law distinctions may be included, the coverage is not comprehensive.

To adhere to publication deadlines, developments and decisions subsequent to January 1, 2017 are not covered.

©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
All material contained within this publication is protected by copyright law and may not be reproduced without the express written consent of Littler Mendelson.
# TABLE OF CONTENTS

§ 1 CONFIDENTIALITY OF EMPLOYEE HEALTH & RELATED INFORMATION
   § 1.1 THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT PRIVACY RULE
      § 1.1(a) Brief History of the HIPAA Privacy Rule
      § 1.1(b) How the HIPAA Privacy Rule Regulates Employers Directly
         § 1.1(b)(i) Health Plans Subject to the HIPAA Privacy Rule
         § 1.1(b)(ii) On-Site Health Care Providers & the HIPAA Privacy Rule
         § 1.1(b)(iii) Health Care Providers Subject to the HIPAA Privacy Rule
      § 1.1(c) A Covered Entity’s Compliance Obligations
         § 1.1(c)(i) Employee Health Information Subject to the HIPAA Privacy Rule
         § 1.1(c)(ii) Requirements for Handling PHI Under the HIPAA Privacy Rule
      § 1.1(d) Obtaining & Disclosing PHI of Employees or Applicants
         § 1.1(d)(i) Obtaining Applicant/Employee PHI Through Preemployment Physicals &
           Fitness-For-Duty Examinations
         § 1.1(d)(ii) Obtaining Employee PHI for Workers’ Compensation Purposes
         § 1.1(d)(iii) Disclosing Employee PHI to Third-Party Service Providers
         § 1.1(d)(iv) Obtaining & Disclosing Employee PHI for Purposes of Supplementing or
           Replacing Group Health Insurance
         § 1.1(d)(v) Disclosing Employee PHI in Civil Litigation
      § 1.1(e) HIPAA Enforcement & Penalties
         § 1.1(e)(i) HIPAA Enforcement
         § 1.1(e)(ii) Civil & Criminal Penalties for HIPAA Privacy Rule Violations
      § 1.1(f) Special HIPAA Liabilities for Health Care Employers
         § 1.1(f)(i) Tort Liability
         § 1.1(f)(ii) Liability for Violation of Patient Confidentiality Under State Statutes
         § 1.1(f)(iii) Exposure to Governmental Investigations & Criminal Liability
         § 1.1(f)(iv) Liability for HIPAA Violations Occurring Off Site
         § 1.1(f)(v) Use of HIPAA as a Defense to Employee Claims
   § 1.2 THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT SECURITY RULE
      § 1.2(a) Security Protocol: Required v. Addressable Security Measures
      § 1.2(b) Security Breach Notification & HITECH Act
         § 1.2(b)(i) What Triggers an Obligation to Notify?
         § 1.2(b)(ii) Who Must Be Notified?
         § 1.2(b)(iii) What Must the Notice Say?
         § 1.2(b)(iv) How Must the Notice Be Delivered?
         § 1.2(b)(v) When Must the Notice Be Delivered?
         § 1.2(b)(vi) Interplay with State Security Breach Notification Laws
         § 1.2(b)(vii) HHS Guidance on Ransomware Breaches
   § 1.3 CONFIDENTIALITY & PRIVACY PROTECTIONS UNDER THE AMERICANS WITH DISABILITIES ACT
   § 1.4 CONFIDENTIALITY & PRIVACY PROTECTIONS UNDER THE GENETIC INFORMATION
     NONDISCRIMINATION ACT
      § 1.4(a) Title II of GINA
         § 1.4(a)(i) Exceptions to Prohibition on Requesting, Requiring or Purchasing Genetic
           Information
         § 1.4(a)(ii) Confidentiality of Genetic Information
      § 1.4(b) Title I of GINA: Health Plans & Health Insurance Issuers
   § 1.5 STATE LAWS CONCERNING MEDICAL RECORDS
§ 2 CONFIDENTIALITY OF OTHER PERSONNEL/EMPLOYEE RECORDS
   § 2.1 ACCESS TO PERSONNEL RECORDS
   § 2.2 LIABILITY FOR UNAUTHORIZED ACCESS TO & IMPROPER RELEASE OF PERSONAL INFORMATION
      § 2.2(a) Data Breaches Leave Employers at Risk
      § 2.2(b) Identity Theft in the Workplace
      § 2.2(c) Federal & State Developments
         § 2.2(c)(i) Laws Restricting Use of Social Security Numbers
         § 2.2(c)(ii) Laws Regulating Destruction of Certain Types of Personal Information
§ 2.2(c)(iii) Laws Requiring Security Breach Notification of Affected Individuals
§ 2.2(c)(iv) Other Legislative Efforts to Prevent Identity Theft

§ 2.3 Disclosing Information About Former Employees to Prospective Employers
§ 2.3(a) Liability for Defamation Arising from Release of Personal Information
§ 2.3(b) Interference with Prospective Economic Advantage

§ 3 Global Information Sharing: The Impact of International Data Protection Laws on Multinational Employers
§ 3.1 Distinctions in Global Approaches to Privacy
  § 3.1(a) The U.S. Approach
  § 3.1(b) The European Union Approach
    § 3.1(b)(i) Works Councils
  § 3.1(c) The Latin American Approach

§ 3.2 E.U. Data Protection Directive & the Upcoming General Data Protection Regulation
  § 3.2(a) E.U. Data Protection Directive’s Application to Employment Law
  § 3.2(b) E.U. General Data Protection Regulation’s Application to Employment Law
  § 3.2(c) Transfer of Data to the United States & Other Countries
    § 3.2(c)(i) Invalidation of U.S.-E.U. Safe Harbor Framework & Adoption of the Privacy Shield
    § 3.2(c)(ii) U.S.-E.U. Privacy Shield
    § 3.2(c)(iii) Continued Alternatives to the Privacy Shield Certification
  § 3.2(d) Role of Brexit

§ 3.3 Safeguarding Private Information in Countries with Less Established Privacy Protection Schemes

§ 4 Practical Guidelines for Employers
§ 4.1 Complying with the Health Insurance Portability and Accountability Act & the Americans with Disabilities Act
  § 4.1(a) Obtaining the Results of Work-Related Physical Examinations
  § 4.1(b) Disclosing PHI to Third-Party Service Providers/Business Associates
  § 4.1(c) Responding to Subpoenas & Civil Discovery Requests Seeking Employee Health Information
  § 4.1(d) Complying with the ADA’s Confidentiality Requirements

§ 4.2 Complying with the Genetic Information Nondisclosure Act
§ 4.3 Providing Access to Personnel Records
§ 4.4 Safeguarding Employee Personnel Data from Theft
§ 4.5 Third-Party Inquiries
§ 4.6 Transborder Data Transfers
  § 4.6(a) Implementing a Privacy Shield Compliance Program for Transfers of HR Data
§ 1 CONFIDENTIALITY OF EMPLOYEE HEALTH & RELATED INFORMATION

§ 1.1 THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT PRIVACY RULE

Many employers collect large quantities of health information concerning their employees. Employers create and receive health information for several different reasons and in various capacities. For example, employers that sponsor self-insured group health plans often receive detailed information about virtually all aspects of their employees’ health care. Even employers with fully insured health plans may receive detailed information about their employees’ health (e.g., through the workers’ compensation insurance process, through selecting a reasonable accommodation for an employee with a disability and when resolving large claims against a self-insured health plan). The privacy regulations implementing the Health Insurance Portability and Accountability Act of 1996 (HIPAA), known collectively as the HIPAA Privacy Rule, as amended by the regulations contained in the Omnibus Final Rule, are a detailed, lengthy and comprehensive body of federal regulations governing the use and disclosure of individually identifiable health information.1

All covered “health care providers” and virtually all HIPAA-covered “health plans” must comply with the HIPAA Privacy Rule, which poses a major interpretive challenge for employers. The U.S. Department of Health and Human Services (HHS), the administrative agency responsible for drafting and enforcing the HIPAA Privacy Rule, has emphasized that these regulations do not regulate employers per se.2 Despite this statement, HHS has emphasized that a central objective of the HIPAA Privacy Rule is to limit the use and disclosure of employee health information for employment-related purposes.3

§ 1.1(a) Brief History of the HIPAA Privacy Rule

The U.S. Congress enacted HIPAA with the overriding objective of making health insurance more affordable and accessible. At the time, hospitals, physicians, health insurance issuers and health maintenance organizations (HMOs) were using hundreds of different proprietary electronic codes, making communications between and among them time-consuming and expensive. HIPAA, and a body of related regulations known as the “HIPAA Transaction Rule,” leveled the field by requiring those that provide health care and those that pay for it to communicate in a uniform electronic language.4

Once sensitive medical information is translated into a single, widely used electronic language, the continued privacy and security of that information is at risk. Recognizing the potential for damage when, with the touch of a button, records of diagnosis and treatment could be published around the world, Congress also mandated in HIPAA, the development of strict procedures to safeguard the privacy and security of health information related to specific individuals. HHS responded to this congressional mandate by promulgating the HIPAA Privacy Rule.5

The HIPAA Privacy Rule, as initially promulgated in 2000, came under attack from the employer

---

1 See generally 45 C.F.R. §§ 160, 164.
2 See, e.g., 67 Fed. Reg. 53,192 (Aug. 14, 2002) (stating that HHS “must remain within the boundaries set by [HIPAA], which does not include employers per se as covered entities”).
©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
community. To address some of these criticisms, the Bush Administration, in 2002, materially modified the regulations as initially promulgated. Of most significance to employers, these revisions clarified that the HIPAA Privacy Rule does not apply to all health information about employees obtained by an employer. However, the limits on the use and disclosure of employee health information for employment-related purposes remained unchanged by the revisions.

In 2013, HHS issued sweeping regulations again significantly changing the HIPAA Privacy Rule. As explained by HHS’s Office for Civil Rights then-Director Leon Rodriguez:

This final omnibus rule marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented. … These changes not only greatly enhance a patient’s privacy rights and protections, but also strengthen the ability of [HHS] to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates.

§ 1.1(b) How the HIPAA Privacy Rule Regulates Employers Directly

§ 1.1(b)(i) Health Plans Subject to the HIPAA Privacy Rule

The HIPAA Privacy Rule’s definition of health plan includes a long list of private and government-sponsored health benefits programs and plans. The most significant definition on the list for employers encompasses any insured or self-insured employee welfare benefit plan, as defined by the Employee Retirement Income Security Act (ERISA), which provides health care. This definition encompasses:

- employer-provided group health insurance;
- dental and vision coverage;
- health care reimbursement flexible spending accounts;
- most employee assistance programs;
- long-term care coverage;
- some wellness programs;
- health reimbursement arrangements; and

---

6 See, e.g., Simon J. Nadel, Health Care: HHS Rule Protecting Health Care Privacy Irks Some Employers, Likely to Affect Many, 75 Daily Lab. Rep. (BNA), at C-1 (Apr. 18, 2000) (The U.S. Chamber of Commerce worried that the rule would limit the activities of employers that run health improvement and well-being programs for their employees, as well as stymie efforts to create integrated benefits programs); Cassie M. Chew, Health Care: Clinton, Shalala Release Privacy Standards; Final Rule Differs Significantly From Proposal, 246 Daily Lab. Rep. (BNA), at A-9 (Dec. 21, 2000) (“[The] new regulations [would] greatly complicate the administration of employees’ benefits, increase their cost for manufacturers and workers, encourage litigation and strangle the necessary flow of information through the health care system.”).


11 45 C.F.R. § 160.103 (definitions of group health plan and health plan).

©2017 LITTLE MENDELSON, P.C. ALL RIGHTS RESERVED.
• prescription drug plans.

The HIPAA Privacy Rule’s definition of health plan does not encompass any of these policies, plans or programs frequently offered by employers:

• short-or long-term disability income insurance;
• stop-loss insurance coverage;
• general liability insurance;
• workers’ compensation insurance;
• retirement plans;
• automobile liability and medical payment insurance; or
• coverage for on-site medical clinics.

For smaller employers, there are two important additional elements to the HIPAA Privacy Rule’s definition of health plan. An employee welfare benefit plan, as defined in ERISA, falls within the HIPAA Privacy Rule’s definition only if the plan has 50 or more participants or is administered by a third party.\(^\text{12}\) In light of these additional criteria, smaller businesses seeking to avoid the burdens of complying with the HIPAA Privacy Rule can do so by taking “in-house” the administration of any otherwise covered plan with fewer than 50 participants.

§ 1.1(b)(ii) On-Site Health Care Providers & the HIPAA Privacy Rule

Many employers offer some form of on-site health care provider, ranging from a nurse practitioner or mental health professional to a licensed physician. The services offered by these and by most other employer-provided, on-site health care providers fall within the HIPAA Privacy Rule’s definition of health care, i.e., any “[p]reventive, diagnostic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition or functional status of an individual or that affects the structure or function of the body.”\(^\text{13}\)

Significantly, for employers, a provider of services falling within the HIPAA Privacy Rule’s broad definition of health care is not a “covered entity” required to comply with the HIPAA Privacy Rule unless the provider also uses the special electronic codes specified in the HIPAA Transaction Rule (described above) for conducting “administrative activities” related to the provision of health care.\(^\text{14}\) These administrative activities include, for example, communicating with a health insurance issuer regarding payment, referring patients to a hospital or other practitioner, and first report of injury.\(^\text{15}\) However, health care providers do not have to use the electronic codes specified in the HIPAA Transaction Rule. Thus, the HIPAA Privacy Rule is inapplicable to an on-site health care provider who does not engage in electronic transmissions, such as seeking reimbursement from a health insurance issuer or making referrals to other providers.

\(^\text{12}\) 45 C.F.R. § 160.103 (definition of group health plan).
\(^\text{13}\) 45 C.F.R. § 160.103 (definitions of health care and health care provider).
\(^\text{14}\) See, e.g., Beard v. City of Chicago, 299 F. Supp. 2d 872 (N.D. Ill. 2005) (holding that city’s fire department could not withhold production of employee health records based upon the HIPAA Privacy Rule because even if the fire department could be deemed a “health care provider,” it did not engage in standard electronic transactions and, therefore, was not covered by the Privacy Rule).
\(^\text{15}\) 45 C.F.R. §§ 160.102(a)(3) (defining a covered health care provider), 160.103 (definition of transaction).
§ 1.1(b)(iii) Health Care Providers Subject to the HIPAA Privacy Rule
While most on-site health care providers are not subject to the HIPAA Privacy Rule, all health care providers that receive payment from health insurance companies or government programs, such as Medicare and Medicaid, are subject to the HIPAA Privacy Rule.

§ 1.1(c) A Covered Entity’s Compliance Obligations

§ 1.1(c)(i) Employee Health Information Subject to the HIPAA Privacy Rule
At first blush, the scope of health information protected by the HIPAA Privacy Rule appears to encompass all employee health information. The HIPAA Privacy Rule broadly defines protected health information (PHI) to include all information related to the past, present or future health status of an identified individual, to treatment received by an identified individual and to payment for treatment.16 Thus, PHI includes not only the records of diagnosis and treatment but also billing records, information about premium payments and even some enrollment and disenrollment information, which may include Social Security numbers.

For employers, there is an important caveat to this definition: health information is not PHI unless it was created or received by the employer in its capacity as a “health plan” or covered “health care provider.” The 2002 modifications to the HIPAA Privacy Rule codified this caveat. The Privacy Rule’s amended definition of PHI states: “Protected health information excludes … individually identifiable information in [e]mployment records held by a covered entity in its role as employer.”17 In interpretive notes accompanying the 2002 modifications, HHS gave this example of the exclusion’s application:

When the individual gives his or her medical information to the covered entity as the employer, such as when submitting a doctor’s statement to document sick leave, or when the covered entity as employer obtains the employee’s written authorization for disclosure of protected health information, such as an authorization to reveal the results of a fitness-for-duty examination, that medical information becomes part of the employment record, and as such is no longer protected health information.18

To further clarify the distinction, HHS’s interpretive notes provide several additional examples of the types of employment records falling outside the definition of PHI and, therefore, outside the scope of the HIPAA Privacy Rule. Employment records not covered by the HIPAA Privacy Rule include:

- medical information required by an employer to carry out its obligations under the Americans with Disabilities Act (ADA), the Family and Medical Leave Act (FMLA) and other laws;

- files containing information about occupational injuries, disability insurance eligibility, sick leave requests and justifications; and

---

16 45 C.F.R. § 164.501 (definition of protected health information); 45 C.F.R. § 160.103 (definition of individually identifiable health information). It is also important to note that the same information could be PHI in one context and not in another. See, e.g., State of Wis. v. Friedman, 735 N.W.2d 194 (Wis. Ct. App. 2007) (holding that results of blood alcohol test performed at a hospital were not PHI when used to determine sobriety for law enforcement purposes but indicating that the same test results, if obtained for other purposes such as patient care, would be considered PHI).


• drug screening results, workplace medical surveillance and fitness-for-duty tests for employees.\(^\text{19}\)

Thus, the key inquiry in determining whether health information is an employment record not subject to the HIPAA Privacy Rule is the role the employer played when it created or received the information. If the employer received the information in its capacity as the administrator of a health plan, i.e., as part of a coverage dispute resolution procedure, the information would be subject to the HIPAA Privacy Rule. If, however, the employer received the exact same health information, for example in a medical certification for FMLA leave prepared by the employee’s physician, that record would not be subject to the Rule.\(^\text{20}\)

Illustrating this distinction, the court in Cooney v. Chicago Public Schools held that a municipal school board had no duty under HIPAA to safeguard employees’ health insurance elections on open-enrollment forms because the board had received that information in its capacity as an employer and, therefore, the information was an employment record not subject to HIPAA.\(^\text{21}\)

\section*{§ 1.1(c)(ii) Requirements for Handling PHI Under the HIPAA Privacy Rule}

Health plans and covered health care providers have wide-ranging obligations with respect to plan participants’ and patients’ protected health information. The obligations of covered health care providers are materially the same, albeit employers with on-site medical clinics falling within the HIPAA Privacy Rule’s definition of health care provider should confer with counsel concerning the distinctions.

For purposes of the present section, the following brief summary of the regulatory requirements applicable to employers, as modified by the HITECH Act and its implementing regulations (such as the Omnibus Final Rule), should help put into perspective the remaining discussion in this section:

- Covered entities may use or disclose PHI only with the participant’s or patient’s written authorization except when using PHI for purposes of treatment, payment for the treatment, specified operational activities of the covered entity and in other circumstances where one of several exceptions applies.\(^\text{22}\) A plan’s own “health care operations” includes underwriting and premium rating.\(^\text{23}\) However, pursuant to the Genetic Information Nondisclosure Act (GINA), group health plans (excluding issuers of long-term care policies) cannot request or require genetic information for underwriting purposes (see § 1.4).\(^\text{24}\)

- Covered entities must appoint a privacy official who is responsible for overseeing the implementation of policies and procedures to ensure that:
  
  1. PHI will be used and disclosed only in accordance with the HIPAA Privacy Rule; and
  2. plan participants and patients can exercise their rights under the HIPAA Privacy Rule with respect to their own PHI.\(^\text{25}\)

- Covered entities must provide the following rights:
  
  1. the right to receive a notice describing the covered entity’s privacy policies and practices;

\(^\text{22}\) 45 C.F.R. § 164.502(a)(1).
\(^\text{23}\) 45 C.F.R. § 164.506(c)(1).
\(^\text{24}\) 45 C.F.R. § 164.502(a)(5).
\(^\text{25}\) 45 C.F.R. § 164.530(a).
2. the right to review and photocopy PHI or the right to obtain a copy of the PHI in the electronic form and format requested by the individual if readily producible, or, if not in a readable electronic form, in a format agreed to between the covered entity and the individual;  

3. the right to amend PHI;

4. the right to an accounting of certain disclosures of PHI by the covered entity for up to six years (or three years in some cases) prior to the request;

5. the right to request additional restrictions on the use and disclosure of PHI;

6. the right to request alternate means of communicating PHI by the covered entity to the participant or patient;

7. the right to receive notice of a security breach;

8. the right to lodge complaints with the covered entity alleging a violation of the policies and procedures in the privacy notice or of the HIPAA Privacy Rule; and

9. the right to be free from retaliation for exercising any of these rights.

• Covered entities must enter into written contracts, known as “business associate contracts,” with third-party service providers (e.g., outside benefits administrators, accountants, attorneys and insurance brokers) that receive PHI for purposes of performing services on the covered entity’s behalf.

• Covered entities must ensure that they use only the “minimum necessary” PHI when they do use or disclose PHI in a manner permitted under the HIPAA Privacy Rule. The HITECH Act further qualified the “minimum necessary” standard by requiring that, pending additional guidance from the Secretary of HHS, covered entities and business associates limit their use and disclosure of, and request for, PHI to a “limited data set” unless a greater amount of data is the minimum necessary to accomplish the purpose of the use, disclosure or request. A limited data set is defined as PHI that excludes certain direct identifiers about the individual, his or her relatives, employers and household members.

• The Omnibus Final Rule fundamentally changed the Privacy Rule by establishing that business associates are subject to direct enforcement by HHS, including the possibility of penalties, for failing to comply with the HIPAA Security Rule or applicable provisions of the HIPAA Privacy Rule.

---

26 42 U.S.C. § 17935(e); 45 C.F.R. § 164.524. Notably, covered entities are not required to provide individuals with direct access to the entities’ systems. Instead, they must provide individuals only with an electronic copy (such as a PDF), if the PHI is maintained in electronic (and not hard copy) format.

27 42 U.S.C. § 17935(c).

28 42 U.S.C. § 17935 (a). The HITECH Act compelled the covered entity to comply with the requested restriction if: (1) the disclosure is to a health plan for the purpose of payment or health care operations; and (2) the PHI relates only to an item or service for which the provider has already been paid out of pocket in full.


30 45 C.F.R. § 164.504(e).

31 45 C.F.R. § 164.502(b).

32 42 U.S.C. § 17935 (b).

33 45 C.F.R. § 164.514(e)(2).
These detailed regulations have been codified in parts 160 and 164 of title 45 of the Code of Federal Regulations.

§ 1.1(d) Obtaining & Disclosing PHI of Employees or Applicants

§ 1.1(d)(i) Obtaining Applicant/Employee PHI Through Preemployment Physicals & Fitness-For-Duty Examinations

Test results revealing information about an employee’s health will be protected by the HIPAA Privacy Rule only if the person that conducts the test is a “covered health care provider.” If the employer uses a member of its own workforce to conduct the tests, then the employer can easily determine whether the “tester” is covered; specifically, the employer will know whether the on-site provider engages in the standard electronic transactions specified in the HIPAA Transaction Rule.

When using an off-site healthcare provider to test or examine an employee, the employer has no obligations under the HIPAA Privacy Rule because it is not acting in the capacity of a covered healthcare provider or as the administrator of the health plan. The off-site examiner, however, would be subject to the HIPAA Privacy Rule if it engaged in the standard electronic transactions specified in the HIPAA Transaction Rule.

When the examiner is a covered health care provider—whether on-site or off-site—it generally must obtain a valid “authorization” from the subject of the test before disclosing the test results to the subject’s employer.\footnote{45 C.F.R. § 164.502. There may be exceptions to this general requirement, for example, in highly regulated industries where drug and alcohol testing, and the disclosure of the test result to the employer, may be required by law.} Whether the authorization is prepared by the employer or by the off-site health care provider is immaterial; the authorization must contain the following required elements:\footnote{45 C.F.R. § 164.508(c).}

- a specific and meaningful description of the PHI to be disclosed;
- a specific identification of the person(s), or categories of persons, authorized to make the disclosure;
- a specific identification of the person(s), or categories of persons, to whom the PHI will be disclosed;
- a description of the disclosure’s purpose;
- an expiration date or an expiration event (such as the termination of the subject’s employment with the employer requesting the information);
- an explanation of the subject’s right to revoke the authorization;
- a statement that the health care provider may refuse to perform the test if the subject does not sign the authorization;
- a warning that the subject’s PHI may be re-disclosed without further protection after it is disclosed pursuant to the authorization; and
- the subject’s signature and the date of signing.
An authorization to obtain “psychotherapy therapy notes” cannot be combined with an authorization to release any other medical records. The Privacy Rule defines psychotherapy notes to include: “notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual’s medical record.” The term “excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.”

Significantly, for employers with operations in more than one state, the HIPAA Privacy Rule does not preempt state law imposing more stringent privacy requirements. In other words, if a state, by statute or regulation, imposes requirements for a written authorization to release health information that are stricter than, or in addition to, those identified above, then those requirements must be incorporated into the authorization to release medical information. Authorizations in California, for example, must be in a 14-point font because California law requires the larger font (even though the HIPAA Privacy Rule does not specify a font size).

If the off-site health care provider requires the use of its own authorization form, the employer should review the form carefully before the subject of the test executes the form. The purpose of the review is to ensure that the authorization properly identifies the information to be disclosed, the person to whom the disclosure will be made and the purposes for the disclosure. The HIPAA Privacy Rule prohibits the covered health care provider from disclosing PHI other than as permitted by the authorization, and the employer could face liability by using the information for a purpose that is not authorized.

Finally, employers should note that, in commenting upon this authorization requirement, HHS has emphasized that employers may condition employment, or continued employment, upon a job applicant’s or employee’s execution of an authorization. Employers also should understand that once they receive the test results in their capacity as employer, the results are an “employment record,” not PHI, and, therefore, the results no longer are protected by the HIPAA Privacy Rule.

### § 1.1(d)(ii) Obtaining Employee PHI for Workers’ Compensation Purposes

Employers generally do not need to obtain an employee’s authorization to permit a covered health care provider to disclose the employee’s PHI for workers’ compensation purposes. Under the HIPAA Privacy Rule, a covered health care provider may disclose PHI to an employer, to a workers’ compensation insurer or to a workers’ compensation administrative agency as long as state workers’ compensation laws authorize the disclosure. This exception also applies to analogous federal programs, such as the programs established by the Black Lung Benefits Act, the Federal Employees’ Compensation Act, the Longshoreman and Harbor Workers’ Compensation Act and the Energy Employees’ Occupational Illness Compensation Program Act.

While the HIPAA Privacy Rule does permit disclosures for workers’ compensation purposes without

36 45 C.F.R. § 164.508(b)(3)(ii).
37 45 C.F.R. § 164.501 (definition of psychotherapy notes).
38 45 C.F.R. § 160.203(b).
39 CAL. CIV. CODE § 56.11(a).
40 45 C.F.R. § 164.508(a)(1).
42 45 C.F.R. § 164.512(l).

©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
authorization, employers may find that physicians are increasingly skittish about doing so. The “workers’ compensation exception” does not open the door to the covered health care provider’s disclosures of any and all PHI related to the employee. The exception permits disclosure of an employee’s PHI only “to the extent necessary” to comply with workers’ compensation laws. Employers must communicate the nuances of the exception to the various keepers of workers’ compensation information in the organization, including accounting and risk management.

§ 1.1(d)(iii) Disclosing Employee PHI to Third-Party Service Providers

Employers, in their capacity as administrators of a group health plan, often will enlist the assistance of a third-party service provider. Self-insured plans, for example, may hire a third-party administrator. Self-administered plans may require legal counsel to help resolve disputes over coverage, and plan administrators hire consultants to perform antidiscrimination testing.

In each of these situations, the third-party service provider is acting as the covered health plan’s business associate, defined by the HIPAA Privacy Rule to encompass any person that provides services to, or on behalf of, a health plan and those services require the use, disclosure, creation or receiving of a plan participant’s PHI. The Omnibus Final Rule makes clear that the definition of business associate includes a subcontractor that creates, receives, maintains or transmits PHI on behalf of a business associate. Services provided by a business associate to a health plan might include claims processing, claims administration, data analysis, data aggregation, quality assurance, billing, benefits management and the provision of legal, financial, actuarial or accounting advice.

The term business associate typically will not encompass conduits of information, such as Internet service providers and courier services or financial institutions that facilitate payment for health care, because any access these entities have to PHI is only incidental to the service they provide. For the same reason, janitorial services, plumbers, electricians and photocopy repair technicians also would not be considered business associates.

A health insurance issuer or HMO that provides coverage to a group health plan also is not a business associate. The issuer or HMO, like the group health plan itself, is a health plan that uses PHI for its own treatment, payment and operational purposes. The health insurance issuer or HMO is a covered entity in this situation and, therefore, must comply, in its own right, with the HIPAA Privacy Rule. No business associate contract is necessary to ensure that PHI remains protected.

Notably, the HITECH Act fundamentally altered the legal liability of business associates for HIPAA privacy and security violations. Prior to the HITECH Act, business associates were not directly liable under HIPAA. However, the HITECH Act provided that business associates have a direct statutory obligation to comply with the administrative, physical and technical safeguards of the HIPAA Security Rule. Furthermore, business associates are statutorily required to comply with the privacy obligations in their business associate agreements. The HITECH Act also extended to business associates the Act’s additional requirements related to privacy applicable to covered entities, and mandated that such

44  45 C.F.R. § 164.512(l).
45  45 C.F.R. § 160.103 (definition of business associate).
46  45 C.F.R. § 160.103.
requirements be incorporated into the business associate agreement. Business associates are now subject to civil and criminal penalties for violating these requirements. The HITECH Act also requires that upon discovering a material breach of the business associate agreement by a covered entity, a business associate must take reasonable steps to cure the breach or terminate the contact if feasible.

**Business Associate Agreements**

An employer, in its capacity as plan administrator, may disclose PHI to a business associate only after executing a written agreement with the third-party service provider that contains the provisions required by the HIPAA Privacy Rule. These provisions are intended to limit the business associate’s use and disclosure of PHI. The provisions must accomplish the following:

- Establish the business associate’s permitted and required uses of PHI.
- Prohibit the business associate from using or further disclosing PHI other than as permitted or required by the agreement or as required by law.
- Require that the business associate report to the covered entity any use or disclosure of PHI of which the business associate becomes aware that violates the agreement, including breaches of unsecured PHI.
- Require the business associate to obtain from any agent or subcontractor its written agreement to comply with the same privacy protections applicable to the business associate. The covered entity is not obligated to enter into a business associate agreement with the subcontractors of the covered entity’s business associates.
- Require the business associate to provide the individual with access to his or her PHI as required by the HIPAA Privacy Rule.
- Require the business associate to provide the individual with the opportunity to amend the individual’s PHI as required by the HIPAA Privacy Rule.
- Require the business associate to maintain records of certain disclosures of PHI so that the covered entity can provide a complete accounting of disclosures as required by the HIPAA Privacy Rule.
- Require the business associate to make its books and records available for inspection by HHS for purposes of determining the covered entity’s compliance with the HIPAA Privacy Rule.
- To the extent feasible, require that, upon termination of the agreement, the business associate return or destroy all PHI received from, or created or obtained for the covered entity.
- Permit the covered entity to terminate the contract upon discovery of a material breach by the business associate.
- To the extent the business associate will be carrying out the covered entity’s duties under the HIPAA Privacy Rule, the business associate must comply with the Privacy Rule to the same extent the covered entity would.

HHS has published “sample” language, while emphasizing that the sample language is not required and

---

52 42 U.S.C. § 17934(b).

©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
carries no presumptive weight.53

Failure of the business associate to adequately safeguard PHI, as required by a business associate contract, generally will constitute a material breach of a business associate contract. For example, in Managed Care Solutions, Inc. v. Community Health Systems, the covered entity, a hospital, terminated the services agreement after it learned that a workforce member of the business associate had been arrested for identity theft after police found patient records at her home.54 The business associate sued for breach of the services agreement, which contained a business associate addendum. The district court granted summary judgment in favor of the hospital, reasoning that the business associate’s workforce member’s improper acquisition and use of PHI constituted a material breach sufficient to warrant termination of the agreement.

Though comprehensively addressing privacy, the required contractual provisions do not purport to address the elements required under state law for an enforceable contract, such as the exchange of consideration. Other contractual elements typically included in contracts with a third-party service provider—such as indemnification, choice of law, choice of venue, the availability of alternative dispute resolution, and whether the contract can be assigned—also are not mentioned in the HIPAA Privacy Rule. It is up to the covered entity and the business associate, or the business associate and subcontractor, to decide whether to include these provisions in their agreement. In Monarch Fire Protection District of St. Louis County, Missouri v. Freedom Consulting & Auditing Services, Inc, the court made clear that the relationship between a covered entity and a business associate is contractual in nature, and the court will look to contract law to interpret contract clauses in business associate agreements, especially indemnification and fee-shifting provisions, and, importantly, language determining the scope of permissible disclosures.55 Most full-time business associates (e.g., third-party administrators, insurance brokers and pharmacy benefits managers) have developed form business associate agreements that often are sent to employers already signed by the business associate and without any intention to negotiate revisions. As with any contract with a third party, employers should not execute these agreements without, at a minimum, reading and analyzing them carefully and, if necessary, obtaining legal counsel. The issues that should be considered when reviewing these proposed agreements include the following:

- Does the proposed agreement contain all the required language, including the requirements imposed by the HITECH Act and the Omnibus Final Rule?
- Does the proposed agreement permit the covered entity the ability, if desired, to control and/or participate in the business associate’s obligations, such as to provide an accounting at the request of an individual?
- Does the proposed agreement state the required language in a manner that is acceptable to the employer, including breach notification?
- Does the proposed agreement properly allocate compliance obligations between the business associate and the employer?
- Does the proposed agreement properly allocate liability for damages resulting from a breach of the agreement between the business associate and the employer?
- Does the proposed agreement contain all of the nonmandatory provisions that the employer desires; and, if so, are the provisions stated in a manner agreeable to the employer?

55 644 F.3d 633 (8th Cir. 2011).
©2017 LITTLES MENDELSON, P.C. ALL RIGHTS RESERVED.
To date, most business associates have not attempted to impose fees for the potential cost of complying with the HIPAA Privacy Rule. Employers should consider shopping for another business associate if the proposed agreement does contain a fee schedule and the business associate refuses to perform HIPAA compliance gratis.

§ 1.1(d)(iv) Obtaining & Disclosing Employee PHI for Purposes of Supplementing or Replacing Group Health Insurance

Employers seeking to supplement or replace group health insurance may need to obtain plan participants’ PHI from a health insurance issuer or HMO with respect to the plan, then disclose that PHI to an insurance broker that, in turn, may need to disclose the PHI to other health insurance issuers or HMOs so that they can underwrite and price the policy or supplemental benefits to be purchased. The HIPAA Privacy Rule has created an obstacle to these activities for employers with fully insured health plans who have opted out of HIPAA compliance.

The HIPAA Privacy Rule provides that fully insured plans can avoid the cost and administrative burden of complying with the HIPAA Privacy Rule provided that the health insurance issuer or HMO with respect to the plan discloses no PHI to the plan sponsor other than enrollment and disenrollment information and “summary health information.” Summary health information is defined to encompass information about claims experience with all direct identities removed. Many employers have complained that “summary health information” is insufficient for seeking premium bids because, for example, it does not permit the plan sponsor to determine whether a high-cost participant during a prior plan year will not participate in the plan in the future because of death or termination of employment.

The HIPAA Privacy Rule does provide two methods for avoiding the need to rely exclusively upon summary health information. In theory, the employer could obtain the authorization of each plan participant. This route most likely will be impractical for fully insured plans with large numbers of participants.

The second method does not require the authorization of any plan participant, but does require that the fully insured plan comply with the full panoply of HIPAA privacy requirements. Under the HIPAA Privacy Rule, the relationship between a group health plan and its health insurance issuer or HMO with respect to PHI created or received by the issuer or HMO relating to a person that is or was a participant in the group health plan is known as an “organized health care arrangement” (OHCA), a term coined wholly for purposes of the HIPAA Privacy Rule. 56

The HIPAA Privacy Rule permits the participants in an OHCA to share PHI for the “health care operations” of any member of the OHCA without the prior authorization of the person to whom the PHI relates. 57 The HIPAA Privacy Rule defines health care operations to include the following activities:

Underwriting, premium rating and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance) … 58

In other words, an issuer or HMO can disclose to a group health plan, without prior authorization, the PHI of current and former plan participants so the plan can perform all the activities necessary to shop for replacement insurance or supplemental benefits. However, the employer that receives PHI without authorization is no longer eligible for the exemption from HIPAA compliance for fully insured plans. 59

56 45 C.F.R. § 164.501 (definition of organized health care arrangement).
57 45 C.F.R. § 164.506(c)(5).
58 45 C.F.R. § 164.501 (definition of health care operations).
59 See 45 C.F.R. § 164.530(k).

©2017 LITTLE MENDELSON, P.C. ALL RIGHTS RESERVED.
If the employer, in its capacity as plan administrator, were to retain an insurance broker to assist in the plan’s solicitation process, the plan would be required to enter into a “business associate agreement” with the insurance broker, as described in § 1.1(d)(iii), before disclosing plan participants’ PHI to the broker. However, once such a contract is in place, the issuer or HMO with respect to the plan may disclose plan participants’ PHI directly to the broker.60

Finally, the employer, in its capacity as plan administrator, or its insurance broker in its capacity as the plan’s business associate, may disclose plan participants’ PHI to issuers or HMOs to permit them to engage in underwriting and premium rating. Under the HIPAA Privacy Rule, a “health plan” may disclose PHI, without the participant’s prior authorization, for the plan’s own “health care operations,” which, as noted in § 1.1(e), include underwriting and premium rating.61 However, pursuant to GINA, group health plans (excluding issuers of long-term care policies) cannot request or require genetic information for underwriting purposes (see § 1.4).62

Employers should bear in mind that the HIPAA Privacy Rule’s “minimum necessary” requirement, as modified by the HITECH Act and discussed in § 1.1(c)(ii), applies to most uses and disclosures of PHI including those for “health care operations.” Under this requirement, a covered entity or business associate must make “reasonable efforts” to use and disclose, and request from another covered entity, the “minimum necessary [PHI] to accomplish the intended purposes of the use, disclosure or request.”63 Thus, the request for PHI made to the issuer or HMO with respect to the plan should be limited to the limited data set of PHI if practicable, or, if needed, PHI necessary to solicit and evaluate bids for replacement insurance or supplemental benefits. Similarly, the employer’s or the employer’s broker’s disclosure of PHI to issuers and HMOs from whom bids are being solicited should be the minimum necessary to permit the bidder, or potential bidder, to complete its underwriting and premium rating. When evaluating whether a request, or a disclosure, for “health care operations,” or for any other reason, is the “minimum necessary,” the employer, in its capacity as administrator of a health plan or covered health care provider, should consider not only which specific PHI is needed to accomplish the task but also who needs access to that PHI to get the job done.64 HHS has emphasized that the “minimum necessary” requirement is not an “absolute standard” but rather “a reasonableness standard that calls for an approach consistent with the best practices and guidelines already used by many providers and plans today to limit the unnecessary sharing of medical information.”65

§ 1.1(d)(v) Disclosing Employee PHI in Civil Litigation

Employee health information often is central to disputes subject to civil litigation. Employers defending Title VII claims routinely subpoena personnel files from the plaintiff’s former employers seeking, among other things, evidence undercutting the plaintiff’s claim for emotional distress damages or evidence of the employee’s prior misconduct. In a lawsuit charging that an employer negligently exposed employees to toxic materials, the plaintiff most likely would seek health information concerning similarly situated employees that are not parties to the lawsuit. Similarly, an ERISA lawsuit charging that a self-insured and

60 45 C.F.R. § 164.504.
61 45 C.F.R. § 164.506(c)(1).
62 45 C.F.R. § 164.502(a)(5).
63 45 C.F.R. § 164.502(b)(1); see also Miguel M. v. Barron, 17 N.Y. 3d 37 (N.Y. 2011) (holding that the HIPAA Privacy Rule prohibits the disclosure of a patient’s medical records to a state agency that requests them for use in a proceeding to compel the patient to accept mental health treatment where the patient has not authorized the disclosure nor received notice of a request of his medical records).
65 U.S. Dep’t of Health & Human Servs., How are covered entities expected to determine what is the minimum necessary information that can be used, disclosed, or requested for a particular purpose?, available at http://www.hhs.gov/ocr/privacy/hipaa/faq/minimum_necessary/207.html.

©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
self-administered group health plan improperly denied benefits could implicate the health information of nonparty plan participants. The PHI of patients can become important in employment litigation as well—for example, when a health care institution defends against discrimination claims on grounds that an employee was terminated because of poor patient care.

When responding to a civil discovery request or to a subpoena seeking employee health information, an employer should first determine its role when it created or received the responsive documents. The HIPAA Privacy Rule applies only to those responsive documents that the employer created or received in its capacity as a “health plan” or a covered “health care provider.” In the Title VII action described above, for example, an FMLA certification from the plaintiff’s treating psychiatrist stating that the employee required a leave of absence for treatment at a mental health clinic would not be subject to the HIPAA Privacy Rule when located in the personnel file of the plaintiff’s former employer. By contrast, the Privacy Rule would apply to the notes of a mental health counselor in the former employer’s employee assistance program that provided services to the same employee. In the ERISA action described above, the HIPAA Privacy Rule would apply to all of the records of the self-insured and self-administered health plan as long as the plan had 50 or more participants because the employer then would have created and received responsive documents in its capacity as the administrator of a covered “health plan.”

When responsive documents contain PHI, the employer’s responsibilities under the HIPAA Privacy Rule will depend upon the requesting party’s relationship to the PHI. If the requesting party seeks production of his or her own PHI, then the employer may simply produce it. The HIPAA Privacy Rule requires the disclosure of PHI to the individual who is the subject of the PHI. Someone acting as an executor, administrator or other person having authority under applicable state law to act on behalf of a decedent or his or her estate may seek the decedent’s PHI. Similarly, a family member involved in the individual’s care or payment for health care may seek PHI related to that family member’s involvement. A surviving spouse may also be able to obtain the records in some circumstances.

If the requesting party serves a document request or a subpoena seeking production of PHI related to a third party, then the employer may not disclose responsive documents containing PHI, unless the requesting party provides “adequate assurance” that the PHI will be protected. The requesting party may satisfy this requirement in one of two ways:

1. The requesting party may provide a written statement and documentation demonstrating that:
   a. it has made a good faith effort to provide the subject of the PHI with notice of the request;
   b. the notice included sufficient information about the litigation (or proceeding) and an opportunity to object; and
   c. the time for objecting has expired, and there has been no objection or an objection has

67 45 C.F.R. § 164.502(g)(4).
68 45 C.F.R. § 164.510(b)(5).
69 Alvista Healthcare Ctr. v. Miller, 686 S.E.2d 96 (Ga. 2009) (permitting surviving spouse access to deceased husband’s PHI under 45 C.F.R. § 164.502(g)(4)); Opis Mgmt. Res. L.L.C. v. Secretary’ Fla. Agency for Health Care Admin., 713 F.3d 1291, 1296 (11th Cir. Fla. 2013) (45 C.F.R. § 164.510(b)(5) permits covered entities to release a deceased individual’s PHI in narrowly delineated circumstances. First, the regulation applies only to two groups of people: (1) those who were involved in the deceased individual’s health care, and (2) those who paid for the deceased individual’s health care. Second, covered entities may release only protected health information that is relevant to such person’s involvement, i.e., information that is relevant to the care of the deceased individual or to the payment of the deceased individual’s health care.).

©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
been overruled by the court.

2. The requesting party may provide a written statement and documentation that:

   a. the parties to the litigation in which the document request was made have agreed to a “qualified protective order” and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

   b. the requesting party has filed a “qualified protective order” for approval by the court.  

If the requesting party does provide “adequate assurance,” the employer should be careful to produce only PHI falling within the scope of the document request or subpoena. An overbroad production could expose the employer to liability for a disclosure of PHI in violation of the HIPAA Privacy Rule.

Whether an employer can use an employee’s PHI in litigation without the employee’s authorization is a complex question. The HIPAA Privacy Rule permits disclosures of PHI without authorization for “health care operations” purposes, and “conducting and arranging for … legal services” falls within the scope of that exception. However, for this exception to apply, the litigation must be directly related to the operations of the covered entity. Thus, while a covered health plan could use a plan participant’s PHI, without authorization, to defend against a denial of benefits claim by the plan participant, the plan could not use the PHI of nonparty participants, without their authorization, to disprove a claim of pregnancy discrimination by the employer. Employers also should note that in those circumstances where the employer discloses PHI (but not medical records that are not subject to HIPAA) to outside counsel, without the employee’s authorization, the employer is required to enter into a business associate agreement with outside counsel before disclosing the PHI.

Employers also should note that state laws or rules imposing tighter restrictions on the disclosure of patient records trump HIPAA’s exception permitting disclosure of PHI in response to a subpoena or civil discovery request. In *Turk v. Oiler*, for example, the court found that a hospital could not rely upon HIPAA to defeat a common law claim based upon the hospital’s violation of the physician-patient privilege. The hospital contended that the HIPAA Privacy Rule specifically authorizes a covered entity to disclose a patient’s medical records in response to a grand jury subpoena. Rejecting this argument, the court stated that Ohio’s physician-patient privilege “permits disclosure only in certain limited circumstances,” which do not include a response to a subpoena. Because HIPAA does not preempt more stringent state laws, rules or regulations, the Privacy Rule’s exception permitting disclosure of patient

---

70 45 C.F.R. § 164.512(e)(1)(ii)-(v). For purposes of 45 C.F.R. § 164.512(e)(1)(ii), a qualified protective order is one that permits use of the third-party’s PHI only in connection with the litigation and requires the PHI’s return or destruction at the end of the litigation. See also *Good v. Maxim Healthcare Servs.*, 2009 U.S. Dist. LEXIS 50725 (S.D. Ill. June 17, 2009) (granting defendant’s motion to enter a protective order that permitted disclosure to plaintiff of certain information about the provision of health care to defendant’s nonparty clients).

71 45 C.F.R. § 164.502(a).

72 45 C.F.R. § 164.501.

73 45 C.F.R. § 164.501.

74 45 C.F.R. § 164.502(e).

75 732 F. Supp. 2d 758 (N.D. Ohio 2010). *But see Marcum v. Scioto Cnty.*, 2012 U.S. Dist. LEXIS 77927, at **14–15 (S.D. Ohio June 4, 2012) (noting that discovery requested pursuant to plaintiff’s 42 U.S.C. § 1983 claim is “governed by the provisions of federal law, not state law, pursuant to the Supremacy Clause of the United States Constitution” and because “the standards applicable to discovery requests under the Federal Rules of Civil Procedure do not provide a physician-patient (or hospital-patient) privilege, the [requested materials] are not protected from disclosure … [and the defendants] would violate no patients’ rights in complying with [this Court’s order].”).

76 732 F. Supp. 2d 758, 771.
records in response to a subpoena did not apply. However, a federal district court distinguished Turk in Cleveland Clinic Found. v. U.S. because the disclosure in Turk was in response to a state court grand jury subpoena pursuant to state law, while the demand to the company was governed by federal law and, therefore, the Ohio privilege statute did not apply.\textsuperscript{77} Given these complexities, before the employer discloses PHI to outside counsel for litigation purposes, outside counsel should discuss with the employer whether the disclosure can be made without the employee’s authorization, as well as the terms of a business associate agreement.

\textbf{§ 1.1(e) HIPAA Enforcement & Penalties}

\textbf{§ 1.1(e)(i) HIPAA Enforcement}

The HHS Office of Civil Rights, which is responsible for enforcing the HIPAA Privacy Rule, focused its initial enforcement efforts on responding to complaints (as opposed to conducting unannounced audits) and on encouraging voluntary compliance. However, with the passage of the HITECH Act, HHS was required to initiate HIPAA compliance audits for both covered entities and business associates. HHS’s Office of Civil Rights also has authority for the administration and enforcement of the HIPAA Security Rule in addition to the Privacy Rule. (See discussion at § 1.2 regarding the HIPAA Security Rule.)

The most common problems include: the impermissible uses and disclosures of PHI; lack of safeguards of PHI, lack of patient access to their PHI; uses or disclosures of more than the minimum necessary PHI; and lack of administrative safeguards for PHI.\textsuperscript{78} The most common types of covered entities that have been required to take corrective action to achieve compliance are: private practices, general hospitals, outpatient facilities, health plans (group health plans and insurance issuers) and pharmacies.\textsuperscript{79}

In particularly egregious cases, such as the knowing disclosure or obtaining of PHI, HHS can request criminal prosecution by the Department of Justice (DOJ). The more common practice upon receiving a complaint is for HHS to work with the covered entity to establish compliance, although the Omnibus Final Rule makes informal resolution discretionary\textsuperscript{80} and HHS can move directly to a penalty proceeding without attempting resolution with an employer first.

The Omnibus Final Rule also permits HHS to impose a penalty on a covered entity for a violation by its business associate when the business associate is the covered entity’s agent as determined by the federal common law of agency.\textsuperscript{81} To complicate matters for employers, it can be difficult to determine whether a business associate is acting as an agent or an independent contractor, and a business associate could act as both in the same business associate relationship. To distinguish between the two roles, HHS explains in the regulatory commentary to the Omnibus Final Rule that “[t]he right or authority to control the business associate’s conduct … is the essential factor in determining whether an agency relationship exists … .”\textsuperscript{82} The regulatory commentary then provides the following additional guidance:

\begin{quote}
If the only avenue of control is for a covered entity to amend the terms of the agreement or sue for breach of contract, this generally indicates that a business associate is not acting as an agent. In contrast, a business associate generally would be an agent if it enters into a business associate agreement with a covered entity that granted the covered entity the authority to direct the performance of the service provided by its business associate after the relationship was established. For example, if the terms of a business
\end{quote}

\textsuperscript{77} 2011 U.S. Dist. LEXIS 31963 (N.D. Ohio Mar. 9, 2011).

\textsuperscript{78} See www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html.

\textsuperscript{79} See www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html.

\textsuperscript{80} 45 C.F.R. § 160.312(a).

\textsuperscript{81} 45 C.F.R. § 160.402(c).

associate agreement between a covered entity and its business associate stated that “a business associate must make available protected health information in accordance with § 164.524 based on the instructions to be provided by or under the direction of a covered entity,” then this would create an agency relationship between the covered entity and business associate for this activity because the covered entity has a right to give interim instructions and direction during the course of the relationship.  

While HHS’s discretion to forego informal complaint resolution and its ability to hold a covered entity responsible for its business associates’ HIPAA violations are certainly newsworthy, the absence from the Omnibus Final Rule of any restriction on how HHS counts HIPAA violations for purposes of calculating a penalty may pose the greatest risk for employers in light of the stringent penalty structure detailed below. For example, in the regulatory commentary to the Omnibus Final Rule, HHS takes the position that, in calculating a penalty based on the lack of a required safeguard, the agency can count each day the safeguard is absent as a separate violation. As another example, in calculating a penalty based on a security breach, HHS will count each person affected by the breach as a separate violation. In addition, although the total penalty for identical violations is capped at $1.5 million in a calendar year, HHS takes the position that it can seek up to $1.5 million per calendar year for different types of violations. The treatment of what constitutes a violation could therefore result in significant penalties for unsuspecting employers.

§ 1.1(e)(ii) Civil & Criminal Penalties for HIPAA Privacy Rule Violations

Reflecting the shift to more aggressive enforcement of HIPAA violations, the HITECH Act and the Omnibus Final Rule significantly strengthened HIPAA’s enforcement provisions. Before the HITECH Act, HHS was authorized to impose civil money penalties of not more than $100 for each violation, up to a cap of $25,000 annually for all violations of the same requirement or prohibition. The HITECH Act increased the penalty amounts as well as expanded circumstances in which a penalty can be accessed.

There are four tiers of penalties based on the severity of the violation. In all four tiers, the civil money penalties are capped at no more than $1.5 million for identical violations during a calendar year. The penalties otherwise vary by requiring that a penalty may not be less than:

1. $100 or more than $50,000 for each violation unknown to the covered entity and would not have been known through the exercise of reasonable diligence;
2. $1,000 or more than $50,000 for each violation due to reasonable cause and not willful neglect;
3. $10,000 or more than $50,000 for each violation due to willful neglect that was corrected during the 30-day period beginning on the first date the covered entity knew or should have known through the exercise of reasonable diligence that the violation occurred; and
4. $50,000 for each violation due to willful neglect that was not corrected during the 30-day period.

---

85 45 C.F.R. § 160.404(b)(2).
86 45 C.F.R. § 160.404(b)(2)(i).
87 45 C.F.R. § 160.404(b)(2)(ii).
88 45 C.F.R. § 160.404(b)(2)(iii).
89 45 C.F.R. § 160.404(b)(2)(iv).

©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
Criminal penalties include: (1) a fine of not more than $100,000, imprisonment of not more than one year, or both for knowing violations; (2) if the offense is committed under false pretenses, a fine not to exceed $100,000, imprisonment of not more than five years or both; and (3) if the offense is with intent to sell, transfer, or use PHI for commercial advantage, personal gain or malicious harm, a fine of up to $250,000, imprisonment of up to ten years, or both. In *U.S. v. Michel*, the defendant was convicted after a jury trial and faced a maximum sentence of 30 years’ imprisonment and fines of up to $750,000 for stealing patient information from various nursing homes and submitting thousands of fraudulent claims to Medicare. 90

Private litigation also poses a serious risk of liability for employers. Although courts have unanimously held that the HIPAA Privacy Rule does not itself create a private right of action, the regulations establish a “duty of care” with respect to PHI. Violators of that duty may be sued under state, common law tort theories or even for violations of the Employee Retirement Income Security Act (ERISA). Moreover, given the large number of plan participants or patients potentially affected by a single violation—for example, a health plan’s unauthorized disclosure of participants’ PHI for marketing purposes—there is great potential that violators will be confronted with costly class action litigation that generates bad publicity for the organization and exposes the employer to a potentially large damages award.

§ 1.1(f) Special HIPAA Liabilities for Health Care Employers

§ 1.1(f)(i) Tort Liability

When an employee of a health care provider violates the HIPAA Privacy Rule while handling patients or patient information, the employee exposes the provider to tort liability. In *Bigelow v. Sherlock*, for example, a hospital employee alleged that while he was a patient of the hospital and under anesthesia, coworkers applied women’s cosmetics to him, wrote vulgarities on his body and posted photographs of him in that state on the hospital bulletin board. The court held that the plaintiff could proceed with a state law negligence claim against the hospital based upon his coworkers’ alleged conduct in violation of the HIPAA privacy regulations. Similarly, the court ruled in *I.S. v. Washington University* that a patient may cite HIPAA as the “standard of care” in a state-law-based negligence lawsuit against a university hospital that disclosed excessive PHI about the patient to her employer and exceeded her authorization.

§ 1.1(f)(ii) Liability for Violation of Patient Confidentiality Under State Statutes

Although there is no private right of action for violations of HIPAA, conduct constituting a HIPAA violation may nevertheless support a state statutory claim for violation of patient confidentiality. For example, in *Yath v. Fairview Clinics, N.P.*, a Minnesota appellate court revived a claim by a patient

93 There are exceptions to this prohibition against disclosure. One such example is the disclosure of PHI to law enforcement when required for their investigation of a crime on the premises. See, e.g., *Parker v. Quinn*, 2006 U.S. Dist. LEXIS 24239 (N.D. Miss. Apr. 10, 2006) (holding that a pharmacist’s release of information to a law enforcement officer, even in the absence of a warrant, was a “valid reason for disclosure” and that it was in the “good faith belief that a crime had occurred on the premises”).
against a medical clinic under a state statute prohibiting negligent or intentional release of a health record. In that case, an employee of the medical clinic accessed plaintiff’s medical records out of curiosity after seeing plaintiff at the clinic and then disclosed that the plaintiff had a sexually transmitted disease. After that information was posted on a MySpace page, the patient sued the clinic for, among other claims, violation of Minnesota’s health record confidentiality statute. The trial court held that the statute was contrary to HIPAA because it provided for a private right of action and that, therefore, HIPAA preempted it. The appellate court reversed, holding that the private right of action provided by state statute was not contrary to HIPAA because it was possible for a health care provider to comply with both laws, that the goals of both laws were similar, the state statute actually complemented HIPAA and, therefore, HIPAA did not preempt the state statutory action.

§ 1.1(f)(iii) Exposure to Governmental Investigations & Criminal Liability
Beyond the possibility of a lawsuit, violations of the HIPAA Privacy Rule can expose a health care provider to time consuming and costly governmental investigations and its employees to criminal liability. For example, in 2014, HHS secured a $4.8 million settlement against a New York hospital and affiliated university regarding the disclosure of electronic PHI (“ePHI”) of 6,800 patients. Due to a lack of technical safeguards, when a physician attempted to deactivate a personally-owned computer server on the network containing the hospital’s patient information, the ePHI of the patients was accessible on Internet search engines, including patient status, vital signs, medications and laboratory results. The entities only discovered the breach after receiving a complaint by an individual who found the ePHI of the individual’s deceased partner on the Internet. In addition to the monetary settlement, the entities agreed to substantive corrective action plans for the violations of the HIPAA Privacy and Security Rules.

§ 1.1(f)(iv) Liability for HIPAA Violations Occurring Off Site
Even HIPAA violations occurring off site may be sufficient to expose a provider to liability. For example, the Illinois Supreme Court held that a hospital phlebotomist’s disclosure of protected health information at a bar, after hours, and in violation of the hospital’s privacy policies violated the HIPAA Privacy Rule. In that case, the phlebotomist learned through her review of a friend’s blood test results that her friend was pregnant and, without authorization, disclosed that fact to the friend’s sister. The friend found out about the unauthorized disclosure and sued the hospital. The hospital admitted that the disclosure had occurred but contended that the phlebotomist had acted outside the scope of her employment with the hospital. The appeals court rejected this argument, reasoning that “that duty [of confidentiality] imposed by the hospital in its execution of its duties, was, according to its own training, to extend to all times and to all places. In effect, for purposes of patient confidentiality, [the phlebotomist] was on duty 24 hours a day, seven days a week.” Consequently, the hospital could be held responsible for the phlebotomist’s after-hours indiscretion. Although the Illinois Supreme Court ultimately disagreed and affirmed the trial court’s entry of summary judgment for the hospital, the court was cautious to remind employers that simply forbidding employees to disclose patient information and having a policy prohibiting unauthorized disclosure will not necessarily be enough to defeat liability when a health care provider’s employee violates HIPAA. The court’s principal basis for finding in favor of the employer was that the disclosure was in no way undertaken to benefit the hospital.

90 767 N.W.2d 34 (Minn. App. Ct. 2009).
91 767 N.W.2d at 49–50.
93 Bagent v. Blessing Care Corp., 862 N.E.2d 985 (Ill. 2007).
94 862 N.E. 2d at 989.
96 Bagent, 862 N.E.2d at 994.
97 862 N.E.2d at 994.
©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
§ 1.1(f)(v) Use of HIPAA as a Defense to Employee Claims

While patients have used the HIPAA Privacy Rule as a sword, providers have invoked it as a shield from liability for discrimination or retaliation asserted by their employees with varying degrees of success.

For example, in *Pacosa v. Kaiser Foundation Health Plan of the Northwest*, the court granted summary judgment in the provider’s favor on the employee’s FMLA claim where the employee had violated the provider’s privacy policies and access management policies by gaining unauthorized access to family members’ medical information.\(^{104}\) In a similar vein, in *Bingham v. Allina Health System*, the court ruled that an employee’s single violation of the employer’s HIPAA privacy policy specifying no tolerance for inappropriate access or sharing of patient information constituted “misconduct” that disqualified the employee from unemployment benefits after termination of employment.\(^{105}\)

In *Vaughn v. Epworth Villa*, a retirement community employer successfully relied upon HIPAA in defending against its former employee’s retaliation claim.\(^{106}\) The plaintiff, a nurse’s aide, filed a charge of discrimination with the EEOC while she was still an employee. In support of her charge, she submitted to the EEOC several pages of unredacted medical records concerning a patient of the employer. When the retirement community found out about this unauthorized disclosure, it fired the employee for a HIPAA privacy violation.\(^{107}\) The appellate court found that the employee had engaged in a protected activity by giving the papers to the EEOC, but that the employee’s HIPAA violation was a legitimate and nonretaliatory reason for terminating her employment and that the reason was not a pretext. To prove pretext, the employee needed to show that other retirement-community employees were not terminated for engaging in the same or similar conduct. The employee could not identify any other employee that had committed a similar, intentional HIPAA violation. That the employer’s policies did not require termination under the circumstances did not establish pretext.\(^{108}\)

However, health care employers do not always prevail in using HIPAA as a shield in cases by former employees, such as in whistleblower cases.\(^{109}\) For example, in *Westlake Surgical, L.P. v. Turner*, a registered nurse brought suit against the hospital that terminated her employment, allegedly in retaliation for her reporting alleged unlawful conduct related to the delivery of health care.\(^{110}\) Shortly after being notified of her termination, she copied her hard drive and provided it to her attorney. She subsequently sued the hospital, which counterclaimed for conversion and civil theft, alleging that the nurse copied or took 3,000 pages of confidential patient records and information. The Texas Court of Appeals affirmed the trial court’s denial of the hospital’s motion for temporary injunction to force the plaintiff to return the medical records. The court relied on a provision of the HIPAA Privacy Rule that provides a covered entity does not violate HIPAA when an employee in good faith discloses PHI (protected health information) for purposes of reporting allegedly unlawful conduct in connection with the delivery of health care.\(^{111}\)

§ 1.2 THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT SECURITY RULE

Employers that are required to comply with the HIPAA Privacy Rule also must comply with information

---


\(^{106}\) 537 F.3d 1147 (10th Cir. 2008).

\(^{107}\) 537 F.3d at 1149.

\(^{108}\) 537 F.3d at 1153–54.

\(^{109}\) 45 C.F.R. § 164.502(j)(1).


\(^{111}\) *Westlake Surgical*, 2009 Tex. App. LEXIS 6132, at *14 (citing 45 C.F.R. § 164.502(j)(1)).
security regulations known collectively as the HIPAA Security Rule. The HITECH Act included an amended security breach notification requirement. Also of significant note, the Omnibus Final Rule makes business associates directly liable for any failures to comply with the HIPAA Security Rule.

On its face, the Security Rule has a significant limitation. It applies only to PHI stored or transmitted in electronic format. Covered transmission includes the physical movement of electronic storage media as well as intranet and Internet communications. The Security Rule does not apply to PHI stored on paper, voice transmissions of PHI, video conferencing and paper-to-paper fax transmissions containing PHI. Nonetheless, covered entities and business associates should consider safeguards for nonelectronic PHI similar to those required by the Security Rule, to the extent applicable, as a means of complying with their obligation under the HIPAA Privacy Rule to provide “appropriate technical, administrative, and physical safeguards” for all PHI.

The Security Rule’s primary objective is to ensure that each covered entity safeguards the confidentiality, integrity and availability of electronic PHI. Those key terms are defined as follows:

- Confidentiality means that data are not made available or disclosed to unauthorized persons or processes.
- Integrity means that data have not been altered or destroyed in an unauthorized manner.
- Availability means that data are accessible and usable upon demand by an authorized person.

In addition, covered entities and business associates must protect electronic PHI against reasonably anticipated threats or hazards and against reasonably anticipated uses or disclosures that would violate the HIPAA Privacy Rule.

There is no silver bullet for satisfying these general requirements. HHS has emphasized that the regulations are “technology neutral.” However, while encryption is not mandated by the security rule, it

---

112 Employers that sponsor fully insured group health plans are not exempt from the HIPAA Security Rule, although they are exempt from most of the requirements of the HIPAA Privacy Rule. 45 C.F.R. § 164.530(k). However, the HIPAA Security Rule applies only to the extent that the fully insured group health plan creates or maintains electronic PHI (other than summary health information and enrollment information). If benefits are provided through an insurer or HMO and the only electronic PHI received or maintained by the employer on behalf of the plan is enrollment information or pursuant to an individual authorization, the plan would need to adopt only very basic security policies and procedures. The plan would be required to designate a security official, perform and document a risk analysis (to determine if any of its computer systems contain electronic PHI), develop and document risk management procedures (which would also be limited if the plan did not hold or transmit any electronic PHI) and comply with the breach notification requirements. American Bar Ass’n, Technical Session Between the Centers for Medicare and Medicaid Services and the Joint Committee on Employee Benefits (May 16, 2005), available at http://www.americanbar.org/groups/committees/employee_benefits/events_cle/practitioner_q_as1/cms_qa.html (select “2005”).


114 45 C.F.R. § 164.302.


116 45 C.F.R. § 164.530(e)(1).

117 45 C.F.R. § 164.304 (definition of confidentiality).

118 45 C.F.R. § 164.304 (definition of integrity).

119 45 C.F.R. § 164.304 (definition of availability).


does create a safe harbor from the new breach notification requirement.\textsuperscript{122} In addition, the Security Rule’s requirements are “scalable,” \textit{i.e.}, appropriate security measures will depend on: (1) the covered entity’s or the business associate’s size, complexity and capabilities; (2) the covered entity’s or the business associate’s technical infrastructure, hardware and software security capabilities; (3) cost; and (4) the probability and significance of a risk to electronic PHI if the security measure is not implemented.\textsuperscript{123}

\textbf{§ 1.2(a) Security Protocol: Required v. Addressable Security Measures}

The Security Rule’s security measures are either required or “addressable.”\textsuperscript{124} Just as the name suggests, covered entities and business associates must implement required security measures. For each addressable security measure, the covered entity or the business associate must evaluate and document whether the measure is reasonable and appropriate when considering:

1. the entity’s risk analysis;
2. the entity’s risk management strategy;
3. the security measures already in place; and
4. the cost of implementation.\textsuperscript{125}

If an addressable security measure is not reasonable or appropriate, the covered entity is required to identify an alternative, document the rationale behind selecting the alternative, and then implement the alternative—if implementation would be reasonable and appropriate.\textsuperscript{126}

Covered entities and business associates are required to designate a single person that is ultimately responsible for the security of electronic PHI. This person also is responsible for ensuring that the covered entity engages in the mandatory security management process.\textsuperscript{127}

The security management process has four principal pillars.

1. The covered entity or the business associate must conduct a risk analysis, \textit{i.e.}, an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI.\textsuperscript{128}

2. Using the results of the risk analysis, the covered entity or the business associate must then engage in “risk management,” by implementing security measures sufficient to reduce the risks and vulnerabilities identified in the risk analysis to a reasonable and appropriate level.\textsuperscript{129} These security measures should be periodically reevaluated, from a technical and nontechnical perspective, and modified as necessary to address environmental and technological change.\textsuperscript{130}

3. Once the security measures have been implemented or after they are modified, the covered

\textsuperscript{123} 45 C.F.R. § 164.306(b)(2).
\textsuperscript{124} 45 C.F.R. § 164.306(d).
\textsuperscript{125} 68 Fed. Reg. 8334, 8336.
\textsuperscript{126} 45 C.F.R. § 164.306(d).
\textsuperscript{127} 45 C.F.R. § 164.308(a)(2).
\textsuperscript{128} 45 C.F.R. § 164.308(a)(1)(ii)(A).
\textsuperscript{129} 45 C.F.R. § 164.308(a)(1)(ii)(A).
\textsuperscript{130} 45 C.F.R. § 164.308(a)(1)(ii)(10).

©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
entity or the business associate must monitor system activity, for example, by reviewing audit logs and access reports and tracking security incidents, to ensure that security measures are being followed and are effective.131

4. The covered entity must implement and enforce a sanctions policy against workforce members when security measures are breached.132

Within this general framework, the Security Rule identifies specific security measures that must be implemented and others that must be evaluated as part of the risk management process and implemented if reasonable and appropriate. These measures include, for example, the following (with the required measures indicated):

- **Controlling Authorized Access to PHI.** Establish policies and procedures: (1) to limit access to PHI to those with a need to know, i.e., by limiting access to workstations, programs and applications; (2) to restrict those with authorized access to the minimum PHI necessary to perform their jobs; (3) to document, review and, when necessary, modify access rights; and (4) to terminate access upon termination of employment.133 Unique identifiers must be assigned to permit tracking of access by system users.134

- **Ensuring Emergency Access to PHI [required].** Procedures must be implemented to ensure that electronic PHI can be accessed during emergencies.135

- **Protections Against Unauthorized Access to PHI.** Passwords should be issued, safeguarded and changed periodically. Anti-virus software should be installed and regularly updated. Login attempts should be monitored.136

- **Business Associate Agreement [required].** A covered entity may permit a business associate to create, receive, maintain or transmit PHI on the covered entity’s behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information. Covered entities are not required to obtain a business associate contractor from a subcontractor of the business associate. Instead, business associates are required to enter into business associate contracts with their subcontractors.137

- **Audit Controls [required].** Hardware and software should record, and permit examination of, activity on information systems containing electronic PHI.138

- **Authentication.** Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner and to verify the identity of persons seeking access to PHI. (The latter form of authentication is a required measure). Error-correcting

---

131 45 C.F.R. § 164.308(a)(1)(ii)(D).
132 45 C.F.R. § 164.308(a)(1)(ii), (a)(8). The type and severity of sanctions to be imposed, and for what causes, must be determined by each covered entity based upon its security policy and the relative severity of the violation. 68 Fed. Reg. 8334, 8347.
133 45 C.F.R. § 164.308(a)(3)–(4).
134 45 C.F.R. § 164.312(a)(2). Note that the assignment of unique identifiers is required.
135 45 C.F.R. § 164.312(a)(2).
136 45 C.F.R. § 164.312(a)(2).
137 45 C.F.R. § 164.308(b)(1).
138 45 C.F.R. § 164.312(b).
memory and magnetic disk storage are examples of built-in data authentication mechanisms that are ubiquitous in hardware and operating systems.\(^{139}\)

- **Security Awareness & Training.** Each member of the covered entity’s workforce that accesses electronic PHI should receive training commensurate with the level of access. The training should explain security measures and how to reduce the risk of unauthorized access to, and use or disclosure of, PHI. Those with access to PHI also should receive periodic security reminders.\(^{140}\)

- **Security Incident Reporting [required].** Establish a system for identifying and responding to unauthorized access to, or use or disclosure of, PHI. Mitigate the harm from known security incidents to the extent practicable, and document each incident and its outcome.\(^{141}\)

- **Controlling Access to Physical Facilities.** The physical spaces where information systems equipment, such as servers and back-up tapes, are stored should be secure. Access should be restricted and controlled, and access in the case of an emergency should be planned.\(^{142}\)

- **Workstation Use & Security [required].** Ensure that workstations that can access electronic PHI are used properly and are safeguarded to prevent access by unauthorized users.\(^{143}\) Workstations should lock down automatically after a specified period of inactivity.\(^{144}\)

- **Data Destruction Policies [required].** Implement appropriate data destruction policies and ensure that electronic PHI is removed from all storage media before re-use.\(^{145}\)

- **Monitoring Storage Media.** Track the movement of all hardware and storage media containing electronic PHI and create an exact copy of electronic PHI, when necessary, before moving hardware.\(^{146}\)

- **Encryption & Transmission Security.** While the feasibility of encrypting electronic PHI in storage and in transmission must be considered, its use should be based upon an entity’s risk analysis.\(^{147}\) Encryption typically will not need to be considered for switched, point-to-point connections and dial-up lines. Covered entities that transmit electronic PHI over the Internet are encouraged to consider encryption although the financial and technical burden may render encryption inappropriate depending upon the results of the entity’s risk analysis.\(^{148}\)

In addition to these security measures, the Security Rule requires planning for contingencies that might affect the integrity or availability of data, such as fire, flood, vandalism or a system crash. To that end, each covered entity must:

1. create and maintain data backups;

---

\(^{139}\) 45 C.F.R. § 164.312(c), (d); 68 Fed. Reg. 8334, 8356.

\(^{140}\) 45 C.F.R. § 164.308(a)(5).

\(^{141}\) 45 C.F.R. § 164.308(a)(6).

\(^{142}\) 45 C.F.R. § 164.310(a).

\(^{143}\) 45 C.F.R. § 164.310(b), (c).

\(^{144}\) 45 C.F.R. § 164.312(a)(2)(iii). This security measure is “addressable.”

\(^{145}\) 45 C.F.R. § 164.310.

\(^{146}\) 45 C.F.R. § 164.310(d).


2. be capable of restoring lost data; and

3. establish policies and procedures to safeguard electronic PHI when operating in emergency mode.

When “addressable,” the covered entity should test these contingency plans and revise them as appropriate.\(^{149}\)

The HITECH Act requires HHS to conduct periodic audits to ensure that covered entities and business associates are complying with the HIPAA Privacy and Security Rules and breach notification standards.\(^{150}\)

\section*{§ 1.2(b) Security Breach Notification & HITECH Act}

One of the most significant obligations created by the HITECH Act is the security breach notification requirement, which mandates employers that sponsor HIPAA-covered plans to provide notice of a breach of unsecured PHI to affected individuals and, in certain cases, to HHS and media outlets.\(^{151}\) The Omnibus Final Rule provides further guidance on when security breach notification is required.\(^{152}\)

The regulations suggest a series of questions covered entities can ask to determine whether a breach-triggering event has occurred.

\section*{§ 1.2(b)(i) What Triggers an Obligation to Notify?}

1. \textbf{Did the incident involve PHI?} Covered entities need to determine whether PHI is involved. In the employment context, only individually identifiable health information created, or received by, or on behalf of an employer in its capacity as the administrator of a HIPAA-covered plan or covered health provider is considered PHI.

2. \textbf{Was the PHI “unsecured”?} If the information is PHI, then covered entities need to evaluate whether the PHI is “unsecured.” The breach notification requirement applies only to unsecured PHI, which the HITECH Act defines as not having been rendered unusable, unreadable or indecipherable to unauthorized persons through technology or methodology specified by HHS.\(^{153}\) Unsecured is defined by HHS to mean PHI that has not been either: (1) encrypted consistent with standards set by the National Institute for Standards and Technology; or (2) the media on which the PHI is stored or recorded have been destroyed in a manner that renders the information irrecoverable.\(^{154}\) While the use of encryption is not required, it does create a “safe harbor” from the requirement to provide security breach notification.

3. \textbf{Did the incident involve a use or disclosure of unsecured PHI that violated the HIPAA Privacy Rule?} Additionally, there must be a “breach” of unsecured PHI to trigger the notice. HHS defines breach as the acquisition, access, use or disclosure of unsecured PHI in

\(^{149}\) 45 C.F.R. § 164.308(a)(7).
\(^{150}\) 42 U.S.C. § 17940.
\(^{151}\) 42 U.S.C. § 17932.
\(^{152}\) 45 C.F.R. pts. 160, 164.
\(^{153}\) 42 U.S.C. § 17932(h) (HHS is required to annually update the technologies and methodologies that it deems will render PHI secure.).
violation of the HIPAA Privacy Rule. Therefore, covered entities must carefully evaluate whether the use or disclosure violated the Privacy Rule.

4. **Does the HIPAA Privacy Rule violation fall within one of the exceptions to the notification requirements?** Even if there has been a violation of the Privacy Rule, HHS has identified the following narrow exceptions to the notice obligation:

- when a workforce member authorized to access PHI inadvertently accesses PHI that is not within the scope of the authorization and does not misuse the information;
- when a workforce member authorized to access PHI inadvertently discloses PHI to another worker that is authorized to access PHI at the same facility; or
- when the covered entity has a good faith belief that the unauthorized person that received the PHI could not have retained it.156

5. **Does the Privacy Rule violation pose a “low probability that the PHI has been compromised” based on a risk assessment?** Factors to be considered include:

- the nature and extent of the PHI involved, including the types of identifiers and the likelihood of reidentification;
- the unauthorized person who used the PHI or to whom the disclosure was made;
- whether the PHI was actually acquired or viewed; and
- the extent to which the risk to the PHI has been mitigated.157

The covered entity may consider other factors but must consider these four factors at a minimum. If based on this analysis, the covered entity determines that notice is not required, the covered entity must document the basis for that decision.158

§ 1.2(b)(ii) **Who Must Be Notified?**

If a breach of unsecured PHI does not fit within one of the four exceptions outlined above, the covered entity must notify all affected individuals. If the breach involved 500 or more individuals, the covered entity must contemporaneously notify HHS, which will post a notice of the breach on its website.159 If the breach involves fewer than 500 individuals, the covered entity must notify HHS by March 1 of the following calendar year. The covered entity can provide notice to HHS by completing and electronically submitting a breach report form on the HHS website.160

---

155 45 C.F.R. § 164.402. In the preamble to the Interim Final Rule, HHS states that a violation of the Security Rule “does not itself constitute a potential breach under this subpart, although such a violation may lead to a use or disclosure of protected health information that is not permitted under the Privacy Rule, and thus, may potentially be a breach under this subpart.” 74 Fed. Reg. 42,740, 42,744 (Aug. 24, 2009).
156 45 C.F.R. § 164.402.
157 45 C.F.R. § 164.402.
159 HHS lists the name of the covered entity, the number of individuals affected by the breach, the date of the breach, the type of breach (e.g., unauthorized access/disclosure or theft) and a brief summary of the cases that the HHS’s Office of Civil Rights has investigated and closed.
If the breach involved 500 or more individuals from a state or other jurisdiction, the covered entity must also notify “prominent media outlets serving the state or jurisdiction.” Both the posting on the HHS website and notification of the security breach to media outlets are likely to draw unfavorable publicity and increase the prospects for litigation.161

The regulations do not define the phrase prominent media outlets, but HHS commented that the appropriate media outlet could be a citywide newspaper if all affected individuals reside within city limits but would be a statewide newspaper or television news program if affected individuals are more dispersed.162 The notice can take the form of a press release. As noted above (see § 1.1(e)(ii)), the HITECH Act authorizes state attorneys general to enforce HIPAA. Consequently, to the extent the media outlet publicizes the breach, this notice may raise the risk of an enforcement action by the attorney general’s office.

§ 1.2(b)(iii) What Must the Notice Say?
The regulations identify five subject matters that must be addressed in the notice:

1. a brief description of what happened, including the date of the breach and the date that the breach was discovered, if known;

2. the types of unsecured PHI involved in the breach, e.g., Social Security number, date of birth, diagnosis;

3. steps affected individuals can take to reduce the risk of harm from the breach;

4. a brief description of the covered entity’s investigation, efforts to mitigate harm to affected individuals and steps taken to prevent a recurrence; and

5. contact information for obtaining additional information.163

The regulations do not require that a covered entity offer any particular service to assist affected individuals, such as credit monitoring or fraud resolution services. The HIPAA Privacy Rule does, however, require that each covered entity take reasonable steps to mitigate the harmful effects of an unauthorized use or disclosure of PHI. In some circumstances, the covered entity may need to offer services to affected individuals to comply with this mitigation requirement.

§ 1.2(b)(iv) How Must the Notice Be Delivered?
The notice to individuals generally must be delivered by first class mail to the last known address.164 If ten or more notices are returned as undeliverable, the covered entity must prominently post the notice, or a hyperlink to the notice, on its website. The notice must remain posted for at least 90 days and include a toll-free number where callers can learn whether the breach compromised their PHI.

161 In addition, each year, HHS must submit an annual report containing the number and nature of breaches reported to HHS, as well as the actions taken in response to certain Congressional committees. HHS must also make these reports available to the public on its website. 42 U.S.C. § 17932 (i). The annual reports are available at http://www.hhs.gov/ocr/privacy/hitechrepts.html.


163 45 C.F.R. § 164.404(c)(1)(A)–(E).

164 42 U.S.C. 17932(e)(1)(A); 45 C.F.R. § 164.404(d)(1)(i). Written notice may be in the form of electronic mail if the individual agrees to receive an electronic notice and such agreement has not been withdrawn. If the covered entity deems a situation urgent, because of possible imminent misuse of PHI, the covered entity may provide information to affected individuals by telephone or other appropriate means, in addition to (but not in lieu of) written notice. 45 C.F.R. § 164.404(d)(3).
§ 1.2(b)(v) When Must the Notice Be Delivered?

The notice must be provided without unreasonable delay, but in no event more than 60 days after discovery of the incident. The time spent investigating an incident to determine whether a breach, in fact, has occurred counts against the 60-day time limit.

Discovery occurs when any person that is a “workforce member” or agent of the covered entity (other than the responsible person) knows of the incident. The Privacy Rule broadly defines workforce member to include “employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.” As a result, the 60-day period for delivering notice could start to run before anyone in management is aware of the incident.

To address this issue, covered entities should consider implementing reasonable systems for discovering a breach and train workforce members on how to identify and report a possible security breach. HIPAA uses the term business associate to describe third-party agents that create or receive PHI on the covered entity’s behalf. The regulations also impose a notice requirement on business associates. More specifically, a business associate must notify the covered entity of a breach and of the identity of the individuals. However, there is no time frame specified for doing so. Therefore, the covered entity should include in the business associate agreement a requirement that the business associate immediately notify the covered entity of the breach and provide the covered entity with such information as it will be required to provide to the individual.

Covered entities also should consider including an indemnification agreement in the business associate agreement requiring indemnification for all expenses incurred by the covered entity in connection with a security breach caused by the business associate’s action or inaction.

Discovery of a breach can occur even when no one knows of the incident if the incident would have been known to the covered entity through the exercise of reasonable diligence. HHS interprets the term reasonable diligence to mean “business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.” Under this definition, the 60-day notice period would run if, for example an employee failed to report a lost or stolen laptop containing unsecured PHI.

A statement by law enforcement that complying with any of the notice requirements would impede a criminal investigation or undermine national security tolls the 60-day notice period. A written request tolls the notice period for the duration of the requested delay. An oral request tolls the notice period for no more than 30 days unless followed by a written request for a longer delay. The covered entity must document the oral request.

Minimizing the Risk

165 45 C.F.R. § 164.404(b).
166 45 C.F.R. § 164.404(a)(2). HHS defines discovery as actual knowledge of the breach by a workforce member or agent of the covered entity and/or business associate or when, by exercising reasonable diligence, the breach would have been known.
167 If a business associate experiences the security breach, the 60-day clock begins during the business associate’s investigation when the business associate is acting as the covered entity’s agent as determined by federal common law. Because there is virtually no guidance on when a business associate is an agent under federal common law, covered entities should assume that the time for providing notice to affected individuals begins to run when the business associate discovers the breach.
168 A business associate must notify the covered entity of the breach so that the covered entity can notify affected individuals. A business associate is not required to notify affected individuals of a breach.
170 45 C.F.R. § 164.412.

©2017 LITTLES MENDELSON, P.C. ALL RIGHTS RESERVED.
Faced with the possibility of unfavorable publicity and potentially costly litigation in response to a breach of unsecured PHI as well as penalties for the privacy violation that resulted in the breach, covered entities should consider taking the following steps to minimize the risk:

- create or update a security incident response plan;
- implement systems for detecting a security breach;
- train workforce members on their role in responding to a security breach;
- revise HIPAA policies and procedures as necessary to address the security breach notification requirements;
- include provisions in new business associate agreements that require business associates to promptly notify the covered entity of a security breach and to obtain the agreement of any subcontractor to promptly notify the business associate; and
- discuss with legal counsel how business associate agreements need to be modified to address security breach notification requirements (as well as other amendments needed to comply with other provisions of the Omnibus Final Rule).

§ 1.2(b)(vi) Interplay with State Security Breach Notification Laws

Covered entities and business associates still may be required to comply with state breach notification laws in addition to the federal breach notification rule. HHS has opined that, while state laws contrary to, and less stringent than, the federal breach notification rule are preempted by the federal rule, covered entities subject to state laws imposing additional but nonconflicting breach notification requirements must comply with those state law requirements as well. Nearly every state as well as the District of Columbia, Puerto Rico and the U.S. Virgin Islands have enacted security breach notification laws that are similar to, but can vary materially from, HIPAA’s security breach notification requirements. For further discussion of state laws, see the discussions at § 1.5 and § 2.2(c).

§ 1.2(b)(vii) HHS Guidance on Ransomware Breaches

In July 2016, HHS issued guidance on ransomware attacks, clarifying that a ransomware attack involving ePHI will be presumed to be a HIPAA breach unless the covered entity or business associate demonstrates on the basis of several factors that a “low probability that the PHI has been compromised.” Ransomware is a form of malicious software that denies the user access to his or her data by encrypting the data with a key known only to the hacker, who generally contacts the user demanding a ransom payment to receive the decryption key. The HHS fact sheet, issued in the form of questions-and-answers, notes that the security measures taken to conform to the HIPAA Security Rule may help covered entities and business associates prevent and recover from malware infections, including ransomware. The guidance also provides information on how to detect ransomware and the steps a covered entity or business associate should take if their computer systems are infected with ransomware.

---

171 According to a study of 65 healthcare organizations by the Ponemon Institute, the economic impact of data breach incidents over a two-year period was approximately $2 million per organization. *Benchmark Study on Patient Privacy and Data Security*, 9 PRIV. & SEC. L. REP. (BNA) 1608, Nov. 22, 2010.


©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
§ 1.3 CONFIDENTIALITY & PRIVACY PROTECTIONS UNDER THE AMERICANS WITH DISABILITIES ACT

The Americans with Disabilities Act (ADA) prohibits discrimination based on a real or a perceived disability. The ADA creates important privacy protections for the health information of job applicants and employees generated by job-related medical examinations or received by the employer as part of the process of finding a reasonable accommodation for an employee. These protections complement the HIPAA Privacy Rule’s limitations on the use and disclosure of employee health information because, unlike the HIPAA Privacy Rule, the ADA’s privacy protections apply to certain categories of health information in the employer’s employment records. Put another way, the ADA imposes privacy obligations on the employer in its role as employer, whereas the HIPAA Privacy Rule imposes privacy obligations on the employer in its capacity as the administrator of a group health plan and, in some cases, as the provider of on-site health care.

In 2012, the Seventh Circuit Court of Appeals held that an employer did not violate the ADA’s confidentiality provision by allegedly disclosing medical information about a former employee to a prospective employer.174 In that case, the employer was asked for references regarding the plaintiff/ex-employee. The ex-employee’s former supervisor told several prospective employers of the ex-employee that he “has medical conditions where he gets migraines. I had no issue with that. But he would not call us. It was the letting us know.”175 The EEOC took the position that the supervisor’s response violated the ADA’s confidentiality requirement because the ADA protects medical information learned by an employer through any job-related inquiry. The court disagreed with the EEOC. The court held that the ADA’s confidentiality provisions apply only to employee health information obtained by the employer through a medical inquiry or medical exam. By contrast, the supervisor had learned about the migraines through a general inquiry, i.e., “what’s going on?” The employee had voluntarily offered the medical information even though the supervisor had not asked for it. This case is especially helpful to employers that are the recipients of unsolicited medical information.

Employers that collect health information about job applicants or employees as permitted by the ADA176 must maintain that information on separate forms, kept in a file separate from general personnel information and treated as confidential.177 In addition, such information may be disclosed only in three situations:

1. when supervisors and managers need to be informed regarding necessary restrictions on work or duties of the employee and necessary accommodations;

2. when first-aid and safety personnel need to be informed about a disability that might require emergency treatment; and

3. when government officials investigating compliance with the ADA request access to such records or information.178

Putting aside restrictions two and three above regarding external disclosures, employers need to be cautious about internal disclosures of employee medical information falling within the scope of the ADA’s confidentiality provision. In a 2011 federal case, the court narrowed the scope of intra-corporate

174 EEOC v. Thrivent Fin. for Lutherans, 700 F.3d 1044 (7th Cir. 2012).
175 700 F.3d at 1047.
176 Medical examinations of current employees are generally prohibited unless the exam is “job-related and consistent with business necessity.” 42 U.S.C. § 12112(d)(4).

©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
disclosures to those managers needing to be informed as to the restrictions or reasonable accommodations being made for the employee.\footnote{179} In this case, the court ruled that the disclosure of information from the plaintiffs’ pre-employment medical screening constituted a breach of the ADA’s confidentiality requirement because it was disclosed for the purpose of trying to show that the plaintiff had lied on his questionnaire by not sharing a diagnosis of attention deficit disorder, rather than to advise the managers of necessary restrictions or accommodations. By contrast, the confidentiality requirement does not apply to “voluntary disclosures initiated by the employee,” such as when an employee volunteers information about his or her health condition to a supervisor or to coworkers.\footnote{180}

Typically, a plaintiff bringing a disclosure of confidential information claim under the ADA must exhaust all administrative remedies. However, a 2005 court decision found an employee’s mention in an EEOC charge that her employer created and publicized an incident report, which contained information regarding her medical condition, was sufficient to satisfy the prerequisite. In\footnote{181} Khalil v. Rohm & Haas Co., the plaintiff complained that repainting her office caused her to suffer breathing problems. Upon investigating the incident, the employer created an incident report, which included information regarding the plaintiff’s asthmatic condition. The employer then distributed the report to several of plaintiff’s coworkers without plaintiff’s authorization. The court found that even though the plaintiff did not specifically allege violations of the ADA for disclosure of confidential medical information, because the plaintiff’s complaints to the EEOC included a reference to the incident report, she sufficiently exhausted her administrative remedies.\footnote{182}

\section{1.4 Confidentiality & Privacy Protections Under the Genetic Information Nondiscrimination Act}

Scientific advances in genetics have improved the understanding of links between genes and diseases, and the potential for earlier detection and better treatment of these diseases. However, these scientific advances raised concerns about the potential for the misuse of genetic information in employment and insurance. In response, federal and state legislation have created significant limitations on employers’ ability to conduct genetic testing or screening, and use/disclosure of related information.\footnote{183}

The federal Genetic Information Nondiscrimination Act (GINA) prohibits health insurers and employers from discriminating against individuals based on their genetic information,\footnote{184} and imposes broad restrictions on the use of genetic information, as well as the collection and disclosure of genetic information.\footnote{185} It applies to all employers with 15 or more employees, as well as to employment agencies and labor unions and joint labor-management training programs as those terms are defined in Title VII. There is no individual liability under GINA.\footnote{186}

\begin{footnotes}
\item[180] See Cash v. Smith, 231 F.3d 1301, 1307 (11th Cir. 2000).
\item[182] 2005 U.S. Dist. LEXIS 29125.
\item[183] For example, California’s Fair Employment and Housing Act generally prohibits employers from subjecting applicants and employees to genetic testing. See CAL. GOV’T CODE § 12940(o).
\item[184] 42 U.S.C. §§ 2000ff et seq.
\item[185] Pub. L. No. 110-233, § 2. “Congress has collected substantial evidence that the American public and the medical community find the existing patchwork of State and Federal Laws to be confusing and inadequate to protect them from discrimination. Therefore Federal legislation establishing a national and uniform basic standard is necessary to fully protect the public from discrimination and allay their concerns about the potential for discrimination, thereby allowing individuals to take advantage of genetic testing, technologies, research, and new therapies.”
\end{footnotes}
§ 1.4(a) **Title II of GINA**

The following is a brief overview of Title II of GINA, its applications and limitation. GINA prohibits employers from:

- using an individual’s genetic information when making employment decisions or otherwise discriminating against employees or applicants because of genetic information;\(^{187}\)
- retaliating against employees that complain of discrimination based on genetic information;
- requesting, requiring, or purchasing genetic information (with a few exceptions as discussed in more detail below);\(^{188}\) and
- disclosing genetic information to others (except in some limited situations as discussed below).\(^{189}\)

GINA defines *genetic information* as information about:

1. an individual’s genetic tests;
2. the genetic tests of the individual’s family members;
3. the manifestation of a disease or disorder in the individual’s family member;
4. an individual’s request for, or receipt of, genetic services; and
5. the genetic information of a fetus or any embryo legally held by an individual or family members using reproductive technology.\(^{190}\)

In part, the definition is intended to prevent an employer from inferring that an employee is predisposed to the same disease or disorder as a family member. Significantly, GINA defines *family member* expansively to include not only the employee’s dependents, but also relatives of the employee or of the employee’s dependents from the first to the fourth degree.\(^{191}\)

The EEOC is empowered to enforce the provisions of Title II of GINA and issue regulations. For more information regarding discrimination and retaliation under GINA, see LITTLER ON DISCRIMINATION IN THE WORKPLACE: RACE, NATIONAL ORIGIN, SEX, AGE & GENETIC INFORMATION.

§ 1.4(a)(i) **Exceptions to Prohibition on Requesting, Requiring or Purchasing Genetic Information**

As noted above, GINA prohibits employers from requesting, requiring or purchasing genetic information except in limited circumstances.\(^{192}\) These exceptions include:

---


\(^{188}\) 42 U.S.C. § 2000ff-1(b); 29 C.F.R. § 1635.8.


\(^{190}\) 42 U.S.C. § 2000ff(4); 29 C.F.R. § 1635.3(c).

\(^{191}\) 42 U.S.C. § 2000ff(3); 29 C.F.R. § 1635.3(a).

\(^{192}\) 42 U.S.C. § 2000ff-1(b); 29 C.F.R. § 1635.8(a).
• **Genetic Monitoring Programs.** Employers do not violate GINA where the information involved is to be used for *genetic monitoring*¹⁹³ of the biological effects of toxic substances in the workplace if all of the following conditions are met:

- the employer provides written notice of the genetic monitoring to the employee;
- the employee provides prior, knowing, voluntary and written authorization, or the genetic monitoring is required by federal or state law;
- the employee is informed of individual monitoring results;
- the monitoring is in compliance with any federal or state genetic monitoring regulations; and
- the employer, excluding any licensed health care professional or board certified genetic counselor that is involved in the genetic monitoring program, receives the results of the monitoring only in aggregate terms that do not disclose the identity of specific employees.¹⁹⁴

(Further, employees that refuse to participate in voluntary genetic monitoring programs may not be discriminated against on that basis.¹⁹⁵)

• **Inadvertent Acquisition of Genetic Information.** Employers do not violate GINA by “inadvertently” requesting or requiring family medical history, which highlights the need for employers to eliminate intentional requests for family medical histories.¹⁹⁶ In describing the “inadvertent” or “water cooler” exception in the regulations, the EEOC applies the exception to any genetic information that the employer inadvertently acquires, despite the fact that the statute refers only to family medical history. As examples of situations covered by the exception, the EEOC explains that a supervisor’s questions to an employee, such as “How are you?” or “How’s your son feeling today?” do not violate GINA even if such questions inadvertently elicit genetic information.¹⁹⁷ However, employers may not ask follow-up questions such as whether other family members also have the condition, or whether the individual has been tested.¹⁹⁸

The regulations provide a safe harbor provision for employers that inadvertently acquire genetic information in response to a lawful request for medical information.¹⁹⁹ The EEOC states that the acquisition of genetic information will not be considered *inadvertent* unless the employer directs the individual and/or health care provider supplying the information not to provide genetic information. Importantly, in the context of employment-related medical examinations, a warning to health care providers instructing them *not to ask for genetic

---

¹⁹³ *Genetic monitoring* means the periodic examination of employees to evaluate acquired modifications to their genetic material, such as chromosomal damage or evidence of increased occurrence of mutations, that may have developed in the course of employment due to exposure to toxic substances in the workplace, in order to identify, evaluate, and respond to the effects of or control adverse environmental exposures in the workplace. 42 U.S.C. §§ 2000ff(5).


¹⁹⁵ 29 C.F.R. § 1635.8(b)(5).


¹⁹⁷ 29 C.F.R. § 1635.8(b)(1)(ii)(B).

¹⁹⁸ 29 C.F.R. § 1635.8(b)(1)(ii)(B).

¹⁹⁹ 29 C.F.R. § 1635.8(b)(1)(i)(A).

©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
information is mandatory. Employers must also take additional reasonable measures within their control if they learn that medical providers conducting such examinations are requesting or requiring genetic information.

- **Genetic Information Obtained as Part of Health or Genetic Services (e.g., Wellness Programs).** Recognizing that employers may offer genetic services as an employee benefit, such as genetic counseling as part of a wellness program, GINA carves out an exception for requests for genetic information in connection with such services. To qualify, three requirements must be satisfied:

  1. the employer must obtain prior, voluntary, and written authorization for disclosure of genetic information to the service provider;
  2. only the employee and the licensed health care professional or board certified genetic counselor involved in providing the services may receive individually identifiable information related to the service; and
  3. no individually identifiable information related to the service may be disclosed to the employer.

Thus, an employer’s involvement in an offering of genetic services effectively must be limited to structuring and paying for the service. The EEOC’s regulations explicitly state that for this exception to apply, the wellness program must be “voluntary,” meaning the employer neither requires the individual to provide genetic information nor penalizes those that choose not to provide it.

Consistent with the voluntary requirement, an employer may not offer a financial inducement for individuals to provide genetic information. However, an employer may provide a financial inducement for employees to complete a health risk assessment that includes questions about family medical history and other genetic information, provided that the employer clearly explains to the participants that the financial inducement is available regardless of whether the individual answers the questions about genetic information.

- **Request for Family Medical History as Part of FMLA Leave Certification Process.** One of the most significant exceptions allows employers to request or require the disclosure of a family member’s genetic information, including manifested diseases or disorders, to comply with the federal Family and Medical Leave Act and state family and medical leave laws.

- **Publicly-Available Documents.** Employers do not violate GINA if they purchase commercially and publicly available documents (excluding medical databases and court records) that contain genetic information about an employee or an employee’s family member. The “publicly available” exception does not include documents obtained from sources that require permission of an individual to access or where access is limited to

---

200 29 C.F.R. § 1635.8(d).
201 29 C.F.R. § 1635.8(d).
203 29 C.F.R. § 1635.8(b)(2)(i)(A).
204 29 C.F.R. § 1635.8(b)(2)(i).

©2017 LITTLEG MENDELSON, P.C. ALL RIGHTS RESERVED.
individuals in a particular group. Similarly, the exception does not apply where an employer obtains information from a media source, whether or not it is commercially and publicly available, if the employer is likely to obtain genetic information from that source.

§ 1.4(a)(ii) Confidentiality of Genetic Information

Genetic information must be treated as confidential, maintained on separate forms and in separate medical files, and internal access must be strictly limited to those with a need to know. Thus, GINA generally prohibits employers from disclosing genetic information to third parties. However, it allows disclosure of genetic information under limited circumstances:

1. to the employee or member of a labor organization at the written request of the employee or member of such organization;

2. to an occupational or other health researcher if the research is conducted in compliance with federal regulations;

3. in response to a court order that expressly authorizes the disclosure of specific genetic information, provided that the employer notifies the employee of the disclosure if the court order was issued without the employee’s knowledge;

4. to government officials investigating compliance with GINA; or

5. when necessary for the employer to comply with federal or state medical leave laws.

While the rule allows for disclosure in response to a court order, the rule does not allow disclosure in other circumstances during litigation, such as in response to discovery requests or subpoenas that are not governed by an order specifying that genetic information must be disclosed.

§ 1.4(b) Title I of GINA: Health Plans & Health Insurance Issuers

Title I of GINA amends ERISA to prohibit group health plans and health insurance issuers from adjusting contribution amounts or premiums for the group based on the genetic information of a plan participant. It prohibits plans and issuers from requesting or requiring a genetic test, except in three circumstances:

1. A health care professional that is providing health care services to the individual is permitted to request that the individual undergo a genetic test.

2. A plan or issuer is permitted to obtain and use the results of a genetic test for determinations regarding payment.

3. A plan or issuer is permitted to request, but not require, genetic testing for research if stringent requirements are met.

Group health plans and issuers are prohibited from requesting, requiring or purchasing genetic

---

207  29 C.F.R. § 1635.8(b)(4)(ii).
208  29 C.F.R. § 1635.8(b)(4)(iv).
210  42 U.S.C. § 2000ff-5(b); 29 C.F.R. § 1635.9(b).
211  29 C.F.R. § 1635.9(b).
212  29 C.F.R. § 2590.702-1(b).
213  29 C.F.R. § 2590.702-1(b), (c).

©2017 LITTLE MENDELSON, P.C. ALL RIGHTS RESERVED.
The regulations define the term *underwriting purposes* very broadly to include providing an incentive (“discounts, rebates, payments in kind, or other premium differential mechanisms”) in return for activities such as completing a health risk assessment or participating in a wellness program. Such an interpretation of the term “underwriting purposes” prohibits health risk assessments for which an incentive is offered for participation from collecting genetic information, including family medical history. Even if an employer offers no incentive at all, Title I of GINA and its implementing regulations prohibit group health plans from using a health risk assessment prior to, or in connection with, enrollment in the plan if the assessment requests family medical history. Because of the complexity of these rules, employers should consult counsel before implementing a health risk assessment that requests family medical history.

§ 1.5 State Laws Concerning Medical Records

Some states have special provisions governing employer access to medical records and the protection of the confidentiality of those records. Only a few states, however, have comprehensive protection for medical records that mirror the intent of the HIPAA Privacy Rule. For example, California has one of the most comprehensive statutes in the country and thus serves as an instructive example of the types of limitations that states may place on an employer’s ability to use and disclose medical information about its employees.

In California, employers are required to establish appropriate procedures to ensure that employees’ medical information will remain confidential and will be protected from unauthorized use and disclosure. Appropriate procedures may include giving instructions regarding confidentiality to individuals handling files containing medical information and/or instituting security systems restricting access to such files. Finally, employers are prohibited from using or disclosing medical or psychiatric information they possess about an employee without a signed authorization from the employee permitting such use or disclosure.

As previously noted, the HIPAA Privacy Rules does not necessarily preempt any of these requirements. To the extent the California statute imposes obligations that are directly contrary to the HIPAA Privacy Rule’s requirements and more protective of privacy, or that supplement the federal regulations, those obligations will control.

The California statute may be particularly troublesome for employers that are monitoring an employee’s disability or workers’ compensation leave. For example, in *Pettus v. Cole*, the court found that the employer violated the Confidentiality of Medical Records Act, as well as the employee’s right to privacy, when it terminated an employee on disability leave for failing to enroll in an alcohol-treatment program. The court examined the employee’s reasonable expectation of privacy under the test outlined by the California Supreme Court in *Hill v. National Collegiate Athletic Association*, and found that the employee had also stated a *prima facie* case for invasion of privacy against the company-paid physicians. Both the employer and the physicians argued that the company had a need for the

---

214 29 C.F.R. § 2590.702-1(d).
216 29 C.F.R. § 2590.702-1(d)(2).
217 CAL. CIV. CODE § 56.20(a).
218 CAL. CIV. CODE § 56.20(a).
219 CAL. CIV. CODE § 56.20(a).
221 7 Cal. 4th 1 (1994).
employee’s medical records to evaluate his request for disability leave, but the court disagreed. The court held that without prior written authorization from the employee, employers are entitled only to notice as to whether an employee can perform essential job functions.

Because states other than California may place similar restrictions on the use of employee medical information, employers that seek to collect such information should consult the applicable state statutes.

§ 2 CONFIDENTIALITY OF OTHER PERSONNEL/EMPLOYEE RECORDS

§ 2.1 ACCESS TO PERSONNEL RECORDS

There are a number of state statutes, and some federal laws, that govern whether and to what extent employees can access their own personnel files. Under federal law, for example, employers must permit employees to inspect their own medical records under regulations issued pursuant to the Occupational Safety and Health Act. Moreover, federal agencies are required to allow individuals to examine, copy and request the correction of information in the agency’s records, pursuant to the Federal Privacy Act.

Nearly all states have statutes, regulations or case law covering an employee’s access to his or her own personnel file. Similarly, many collective bargaining agreements contain provisions granting personnel file access to employees and, in some instances, to the union representatives.

However, most personnel-file access laws contain exceptions and limitations, for example:

- Some states limit their applicability to state employees, while others extend coverage to private-and public-sector employees, and still others give the right of access only to private-sector employees.

- In general, personnel-file access laws cover topics such as the time and place of access; right to make copies; right to correct; right to protest and seek removal; and right to insert explanations.

- Many states award damages and/or attorneys’ fees for failure to timely provide access.

Some examples of the provisions and limitations provided by individual states are as follows:

- **Connecticut**: The law applies to both private-and public-sector employers; defines what records are included and/or excluded from a personnel file and medical record; establishes access rights of employees (reasonable time, during business hours, at a location near the employee’s place of employment); states the procedure for correcting information; defines the requirements for disclosure to third persons; outlines the employee’s right to make copies (an employer may charge a fee); and limits an employee’s access to the records to no more than two occasions per calendar year. At the employee’s request, the employee’s physician may also receive a copy of the employee’s medical records.

---

222 CONN. GEN. STAT. §§ 31-128a et seq.
223 CONN. GEN. STAT. § 31-128g.

©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
• **Massachusetts:** An employee or former employee may request to view or copy his or her personnel record. “Personnel record” does not include personal information about another person if disclosure would constitute a clearly unwarranted invasion of privacy.\(^{224}\)

• **Oregon:** An employee, upon request, must be given a reasonable opportunity to inspect, at his or her place of work, all personnel records used to determine his or her qualifications for employment, promotion and pay raises, or used in termination or other disciplinary action against him or her.\(^{225}\) An employee must also be given a certified copy of these records upon request.

Employers should consult whichever access laws apply to their organizations. Multistate employers may want to adopt a policy for each state or attempt to adopt a uniform policy that complies with all applicable laws.

§ 2.2 LIABILITY FOR UNAUTHORIZED ACCESS TO & IMPROPER RELEASE OF PERSONAL INFORMATION

§ 2.2(a) *Data Breaches Leave Employers at Risk*

Wherever protected data is collected and processed, the risk of a data breach exists. When a breach occurs, the central questions are: (1) Who must be notified? and (2) When? An amalgamation of laws in 47 U.S. states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands protects consumers, employees and others by mandating that citizens be notified when the security of their personal information has been compromised.\(^{226}\) The rationale underlying compulsory breach notification laws is that a business forced to inform its consumers or employees that their personal data has been compromised will improve information security measures to avoid having to provide such a notification in the future.

Security breaches have serious consequences to both the organizations and the individuals involved. Figures provided by the Privacy Rights Clearinghouse, which tracks security breaches in publicly available sources, demonstrate the prevalence of data breaches:

<table>
<thead>
<tr>
<th>Year</th>
<th>No. of Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>over 27.9 million</td>
</tr>
<tr>
<td>2013</td>
<td>over 60.9 million</td>
</tr>
<tr>
<td>2014</td>
<td>over 67.9 million</td>
</tr>
<tr>
<td>2015</td>
<td>over 160.0 million</td>
</tr>
<tr>
<td>2016</td>
<td>over 11.0 million</td>
</tr>
</tbody>
</table>

The entities involved in such breaches include financial and insurance services companies, retailers, educational institutions, government and military, health care providers and nonprofit organizations. The reported causes of these security breaches were manifold, including: dishonest insiders; lost or stolen

---

\(^{224}\) *Mass. Gen. Laws* ch. 149, § 52C.

\(^{225}\) *Or. Rev. Stat.* § 652.750.


\(^{227}\) Information from the Privacy Rights Clearinghouse can be found at https://www.privacyrights.org/data-breach.

©2017 LITTLE MENDELSON, P.C. ALL RIGHTS RESERVED.
Additionally, data/security breaches continue to be costly in terms of out-of-pocket costs and loss of business reputation for businesses:

<table>
<thead>
<tr>
<th>Year</th>
<th>Average Cost per Lost or Stolen Record</th>
<th>Average Total Cost of Data Breach</th>
<th>Average Lost Business Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>$194/record</td>
<td>$5.5 million</td>
<td>$3.0 million</td>
</tr>
<tr>
<td>2013</td>
<td>$188/record</td>
<td>$5.4 million</td>
<td>$3.0 million</td>
</tr>
<tr>
<td>2014</td>
<td>$201/record</td>
<td>$5.9 million</td>
<td>$3.3 million</td>
</tr>
<tr>
<td>2015</td>
<td>$217/record</td>
<td>$6.5 million</td>
<td>$3.7 million</td>
</tr>
</tbody>
</table>

There is also the risk of class-action litigation arising out of a security breach involving the loss or theft of personal information. Notably, there is a growing number of cases allowing individuals whose identity is actually compromised as a result of a data breach to sue the companies responsible. The Eleventh Circuit Court of Appeals in Resnick v. AvMed held that plaintiffs claiming actual identity theft resulting from a data breach had standing to sue the company that suffered the compromise. The Eleventh Circuit reversed the dismissal of plaintiffs' negligence, breach of contract, breach of fiduciary duty and unjust enrichment claims. In Resnick, two laptops containing sensitive customer information were stolen from the corporation’s office. Ten and 14 months after the theft, two customers whose information was on the stolen computers allegedly became the victims of identity theft and suffered monetary losses. The court held that the plaintiffs had standing to sue because they suffered an injury that was fairly traceable to the corporation’s alleged failure to secure the data on the laptops. The plaintiffs also sufficiently pled causation of damages for all of their claims because there was a nexus between the data breach and the identity theft that relied on more than just coincidence in time and sequence of events. Thus, securing sensitive information of customers and employees, as well as corporate technology and mobile devices, is more important than ever.

The Seventh Circuit Court of Appeals has gone further by ruling that plaintiffs have standing to sue simply for the time and expense of preventing fraud on their accounts by taking such preventive measures as monitoring their credit score and securing replacement cards.

Thus, it is critical that employers take steps to safeguard not only the information it has about its own employees, but any personal information it may have about clients, customers, etc.

§ 2.2(b) Identity Theft in the Workplace

The U.S. Federal Trade Commission (FTC) issued a guide to businesses in 2013 for complying with the

---

230 693 F.3d 1317 (11th Cir. 2012).
231 693 F.3d at 1321.
232 693 F.3d at 1323–24.
233 693 F.3d at 1327–28.
234 Lewert v. P.F. Chang’s China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016); Remijas v. The Neiman Marcus Grp. L.L.C., 794 F.3d 688 (7th Cir. 2015).

©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
FTC’s 2007 red flags rule, which “requires many businesses and organizations to implement a written identity theft prevention program designed to detect the ‘red flags’ of identity theft in their day-to-day operations, take steps to prevent the crime and mitigate its damage.” The 14-page guide, “Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business,” includes a description of which businesses must comply with the rule, frequently asked questions and a four-step process for complying with the rule’s requirements.  

As a result of this guidance, businesses should determine whether they are required to have a written identity theft prevention program.

§ 2.2(c) Federal & State Developments

Federal Developments

For private sector employers, the FTC has been particularly active in filing enforcement actions against companies that suffer data breaches, including cyber-attacks. In 2015, the Third Circuit Court of Appeals issued its decision in Federal Trade Commission v. Wyndham Worldwide Corp. After the company suffered three cybersecurity attacks between 2008 and 2009, the FTC filed suit, alleging the company engaged in unfair cybersecurity practices that “taken together, unreasonably and unnecessarily exposed consumers’ personal data to unauthorized access and theft.” In affirming the district court’s decision to deny the company’s motion to dismiss, the Third Circuit rejected the company’s argument that it did not engage in an unfair practice because it was victimized by criminals and held that a cybersecurity attack could still be deemed to be an unfair practice if the harm suffered was foreseeable. The Third Circuit’s ruling provides private sector employers with an additional reason to ensure that they are taking appropriate measures to protect against data breaches. The Eleventh Circuit Court of Appeal’s 2016 decision in LabMD, Inc. v. Federal Trade Commission, however, made clear that the FTC’s ability to bring an enforcement action against a company that suffers a data breach is limited to cases in which consumers have suffered an actual harm, and not a mere intangible harm.

In 2015, the FTC issued a guide for companies, Start with Security, on ensuring that consumer data is securely stored and disposed. In 2016, the FTC issued a second guide, Data Breach Response, which provides businesses with tips on the steps to take once a data breach has occurred. Also in 2016, the FTC issued guidance explaining the Commission’s view on compliance with the Department of Commerce’s National Institute of Standards and Technology’s (NIST) Cybersecurity Framework. According to the FTC, while the framework was intended to provide organizations with a compilation of industry-leading cybersecurity practices that organizations should consider in building their cybersecurity programs, applying the framework is also one way for a company to ensure it has implemented reasonable data security processes.

Finally, on January 9, 2017, as this title went to publication, lawmakers reintroduced the Email Privacy Act (H.R. 387), a bill intended to amend the Electronic Communications Privacy Act of 1986 (ECPA). The bill is designed to update the privacy protections for electronic communications information that is stored by third-party service providers by prohibiting the government from obtaining e-mail

---

236 799 F.3d 236 (3d Cir. 2015).
237 799 F.3d at 240.
238 Case No. 16-16270 (11th Cir. Nov. 10, 2016).

©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
communications from a provider of an electronic communication service (such as an employer’s e-mail network) without a warrant, regardless of how long the communication has been held in electronic storage. Currently under the ECPA, the government does not need to obtain a warrant for e-mails that have been stored for longer than 180 days.242

State Developments

At the state level, the growing threat of identity theft has prompted virtually every state to enact laws limiting the use and disclosure of personal information. These laws generally fall into four categories:

1. laws that restrict the use of Social Security numbers;
2. laws that regulate the destruction of certain types of personal information;
3. laws that require businesses to notify individuals whose personal information, maintained by the business, has been compromised through acquisition by an unauthorized person; and
4. laws that require business to implement safeguards for personal information, including detailed requirements in some states, such as Massachusetts243 and Oregon.

§ 2.2(c)(i) Laws Restricting Use of Social Security Numbers

Social Security numbers are of special interest to persons who commit identity theft because they are a broadly used unique identifier and, therefore, particularly useful in perpetrating such fraud. As a result, several states have enacted legislation aimed at protecting the privacy and security of Social Security numbers. These statutes generally prohibit businesses, including employers, from:

- posting or publicly displaying an individual’s Social Security number;
- using such numbers on identification cards;
- requiring the transmittal of employee Social Security numbers over the Internet, except via a secure (i.e., encrypted) connection; and
- mailing any document containing a Social Security number (unless the Social Security number is required by law to be placed on the document).244

An increasing number of states, such as California, New York and Texas, broadly require businesses that collect Social Security numbers and other sensitive personal information, such as driver’s license numbers, to implement reasonable safeguards for that information.245 Massachusetts and Oregon go a step further and require such businesses to implement comprehensive security programs and provide detailed

243 Notably, Massachusetts now has an online data breach notification archive that tracks the number of data breach notifications received by the Massachusetts Office of Consumer Affairs and Business Regulation since the Commonwealth’s notification law took effect. See http://www.mass.gov/ocabr/data-privacy-and-security/data/data-breach-notification-archive.html.
244 Idaho and Maine have taken very limited approaches to their respective restrictive use statutes. Idaho only prohibits a person from intentionally communicating an individual’s Social Security number. IDAHO CODE ANN. 28-52-108. Maine only prohibits persons from using a Social Security number on a credit card, customer service card or debit card. ME. REV. STAT. ANN. tit. 10, § 1272.
245 CAL. CIV. CODE § 1798.85; CAL. LAB. CODE § 226; N.Y. GEN. BUS. LAW § 399-ddd; TEX. BUS. & COM. CODE §§ 501.001 et seq.

©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
requirements for such programs. Finally, a small minority of jurisdictions, such as Connecticut and Michigan, require that employers implement and post a privacy policy that addresses their use of Social Security numbers.

The federal judiciary also requires attorneys to redact certain personal identifying information of individuals involved in litigation when filing documents in federal court—either electronically or in traditional paper format. Rule 5.2(a) of the Federal Rules of Civil Procedure reads:

Unless the court orders otherwise, in an electronic or paper filing with the court that contains an individual’s social-security number, taxpayer-identification number, or birth date, the name of an individual known to be a minor, or a financial-account number, a party or nonparty making the filing may include only:

1. the last four digits of the social-security number and taxpayer identification number;
2. the year of the individual’s birth;
3. the minor’s initials; and
4. last four digits of the financial-account number.

§ 2.2(c)(ii) Laws Regulating Destruction of Certain Types of Personal Information

More than half of the states have enacted legislation requiring businesses to take reasonable steps when destroying records that contain personal information to ensure that the personal information cannot be retrieved by, for example, “dumpster divers.” Although the laws in some of these jurisdictions apply only to customer records, employers should, nonetheless, consider developing policies and practices for properly destroying records containing personal information of employees because these records also can be used to commit identity theft.

For purposes of the document destruction statutes, personal information generally means an individual’s name accompanied by other information such as the individual’s Social Security number, credit or debit card number, savings or checking account number or driver’s license number. Reasonable measures to destroy records include:

1. burning, pulverizing, recycling or shredding of papers containing personal information so that the information cannot practicably be read or reconstructed; and
2. the destruction or erasure of electronic media and other nonpaper media containing personal information so that the information cannot be retrieved.

A business may hire a third party to help destroy personal information in a manner consistent with the document destruction statutes so long as the business takes steps to ensure the competence and reliability of the party hired for this purpose.

Relatedly, as part of its efforts to combat identity theft, the FTC promulgated regulations requiring the proper destruction of consumer information. Consumer information is defined to include credit reports, or information derived from such reports, used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer’s eligibility for employment. The federal regulations do not

249 16 C.F.R. § 682.1(b).
mandate any specific methods or equipment for disposing of such information, but instead require businesses to take “reasonable measures” to safeguard consumer credit information.\textsuperscript{250}

Under the regulations, \textit{reasonableness} may be determined by considering: (1) the sensitivity of the consumer information; (2) the nature and size of the business’s operations; (3) the costs and benefits of different disposal methods; and (4) relevant technological changes.

The regulations list as illustrative examples:

- burning, pulverizing or shredding of paper documentation;
- destruction or erasure of electronic media; and
- contracting with a third party that engages in the business of destroying such information, so long as such contract is entered into after due diligence, and the third party’s compliance with this rule is monitored and audited by the contracting business.

\textbf{§ 2.2(c)(iii) Laws Requiring Security Breach Notification of Affected Individuals}

Currently 47 states, as well as the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands, have responded to the increased threat of identity theft by enacting statutes requiring businesses to notify individuals whose personal information has been stolen.\textsuperscript{251} Virtually all of these statutes have an impact on employers because they impose a duty to provide notice regardless of whether the personal information involved belongs to an employee or to a consumer. Only Alabama, New Mexico and South Dakota do not have a security breach notification law.

The notice of security breach statutes vary in detail from state to state but have substantial similarity in their broad outlines.

- **Definition of Personal Information:** Various jurisdictions define \textit{personal information} differently. For example:
  
  - **Most jurisdictions:** define \textit{personal information} to mean:
    
    1. an individual’s name;

\textsuperscript{250} 16 C.F.R. § 682.3(a).


©2017 LITTLET MENDELSON, P.C. ALL RIGHTS RESERVED.
2. accompanied by: (a) Social Security number, driver’s license or state identification number, or (b) a financial account, credit or debit card number in combination with any security code or password that would permit access to the individual’s financial account.

- **Illinois, Iowa, Nebraska, North Carolina, Texas and Wisconsin**: define personal information to include the above information as well as an individual’s name accompanied by “unique biometric data such as a fingerprint, voice print, or retina or iris image, or other unique physical representation.”

- **Arkansas, California, Florida, Illinois, Missouri, Montana, Nevada, North Dakota, Oregon, Rhode Island, Texas and Virginia**: define personal information to include one or more of the following: an individual’s medical history, mental or physical condition, medical treatment or diagnosis and/or an individual’s health insurance policy number.

**What Triggers the Notice Requirement?:** The obligation to notify affected individuals is triggered when the owner of unencrypted computerized data discovers, or is notified of, a security breach. The laws include some limitations on the notice obligation. For example, in most states, notice is required only if the unauthorized acquisition causes, or is reasonably believed will cause, a material risk of identity theft or other fraud. Moreover, the theft or loss of personal information that is encrypted generally will not trigger the notice obligation. In many states, an employer may avoid the notice requirements by redacting the personal information or taking other steps to make the information unreadable and unusable. Federally-regulated financial institutions and health care-related entities subject to regulation under HIPAA are usually exempt from the states’ notice of security breach statutes, although such entities are required to provide notice under other federal laws.

**Content of Notice:** Notably, a significant minority of these statutes mandates the content of the notice that must be provided to affected individuals. These content requirements can add significant variations to the notice requirements from state to state. In most circumstances, however, a notice of security breach may include the following:

1. a brief explanation of the cause of the security breach;
2. a description of the categories of information that were compromised;
3. additional steps taken to safeguard the information;
4. steps that the recipient of the notice can take to reduce the risk of identity theft; and
5. a contact at the company who can provide assistance.

A notice that addresses all of these points likely will satisfy most state notice laws. Massachusetts, for example, additionally requires that the notice inform recipients of their right to obtain a police report and of the procedures for placing a security freeze on their credit reports.

---

252 See, e.g., IOWA CODE § 715C.1(11)(e); WIS. STAT. § 134.98(1)(b).
253 In some states the notice obligation may be triggered even when data is not stored electronically. See, e.g., ALASKA STAT. § 45.48.400; HAW. REV. STAT. ANN. § 487N-2(a); IND. CODE § 24-4.9-2-2 (breach of security includes “the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in computerized format”).
254 In Massachusetts, businesses need not provide notice unless the security breach “creates a substantial risk of identity theft or fraud against a resident of the commonwealth.” MASS. GEN. LAW ch. 93H, § 1.
255 MASS. GEN. LAW ch. 93H, § 3(b).
• **Procedural Requirements:** The notice in security breach statutes requires several procedural requirements.

- Notice must be provided without unreasonable delay after the discovery of the security breach unless a law enforcement agency determines that notice would impede a criminal investigation or jeopardize national security—for example, because the notice would tip off a hacker under criminal investigation. The notice laws in Tennessee, Ohio and Wisconsin are unique in that they set a specific outside time limit—45 days from the date of discovery—for providing notice to individuals.\(^{256}\)

- In all states that have enacted security breach statutes, notice may be provided in writing or electronically under certain circumstances. Notice by telephone is permitted in approximately half of the states that have enacted notice of security breach statutes.\(^{257}\)

- The laws in several states require that the entity must also notify the three nationwide credit reporting agencies—the number of affected individuals that trigger this requirement varies by state.\(^{258}\) Several states require that businesses provide notice of the breach to a state agency, typically the Attorney General’s office. The number of affected state residents needed to trigger this requirement again varies.\(^{259}\)

• **Multistate Employers:** State notice laws pose a particular challenge for multistate employers. Security breaches involving employee information typically do not affect just employees who reside in one state. The theft or loss of a backup tape containing payroll information, for example, generally will result in the unauthorized acquisition of personal information concerning employees in all of the employer’s locations. In these circumstances, a multistate employer will be required to comply with the notice laws of every state in which affected employees reside. Given the variations of these laws in their details, multistate employers typically will need to confer with in-house or outside counsel who can ensure that the employer’s response to the incident satisfies the varying requirements of each state that has enacted a notice law in which employees reside.

§ 2.2(c)(iv) **Other Legislative Efforts to Prevent Identity Theft**

• **Encryption of Transmitted Records:** Some states mandate encryption of transmitted records and stored data containing personal information.\(^{260}\)

---

\(^{256}\)See, e.g., OHIO REV. CODE ANN. § 1349.19(B)(2); WIS. STAT. § 134.98(3).

\(^{257}\)See, e.g., ARIZ. REV. STAT. § 44-7501; COLO. REV. STAT. § 6-1-716(1)(c); CONN. GEN. STAT. § 36a-701b(e); DEL. CODE ANN. tit. 6, § 12B-101(3)(b); GA. CODE ANN. § 10-1-393.8; HAW. REV. STAT. ANN. § 487N-2(e); IDAHO CODE § 28-51-104(4); IND. CODE § 24-4.9-3-4; MD. CODE ANN. COM. LAW § 14-3504(e); MICH. COMP. LAWS § 445.72(5)(c) (if certain conditions are met); MISS. CODE ANN. § 75-24-29; MO. REV. STAT. §§ 407.1500.1 et seq. (if certain conditions are met); MONT. CODE ANN. § 2302; S.C. CODE ANN. § 39-1-90; UTAH CODE § 13-44-202(5); VA. CODE ANN. §§ 18.2-186.6; VT. STAT. ANN. tit. 9, § 2435(b); W. VA. CODE § 46A-2A-102(d); WIS. STAT. § 895.507(3).

\(^{258}\)See, e.g., FLA. STAT. § 501.171(5); GA. CODE ANN. § 10-1-912(d) (if more than 10,000 residents are affected); MINN. STAT. § 325E.61(2) (if more than 500 residents are affected); N.Y. GEN. BUS. LAW § 899-aa(8) (if more than 5,000 residents are affected).

\(^{259}\)See, e.g., HAW. REV. STAT. § 487N-2(f); KY. REV. STAT. ANN. § 365.732; LA. ADMIN. CODE 16:III:701; N.Y. GEN. BUS. LAW § 899-aa(8); N.C. GENET. STAT. § 75-65(f). Under certain circumstances, notice also must be provided to consumer reporting agencies in Massachusetts and Montana. MASS. GEN. LAW ch. 93h, § 1; MONT. CODE § 30-14-704(7).

\(^{260}\)See, e.g., Frequently Asked Question Regarding 201 CMR 17.00, MASSACHUTES OFFICE OF CONSUMER ©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
• **Security Freeze Laws:** All states and the District of Columbia have enacted “security freeze” laws to battle identity theft.\(^{261}\) These laws permit an individual affected by a security breach to place a “freeze” on their personal credit records. The security freeze typically prohibits a consumer reporting agency from releasing all or part of the consumer’s credit report or any information derived from it without the individual’s express authorization. In any notice of security breach, employers should consider providing information on how affected employees can place a security freeze on their credit reports.

## § 2.3 Disclosing Information About Former Employees to Prospective Employers

Generally, with the exercise of caution, an employer may furnish a truthful statement concerning the reason for a former employee’s discharge or voluntary termination. In many states, such a statement is subject to a common-law privilege.\(^{262}\) If such a statement is not in response to a request, however, or is accompanied by marks or symbols that convey information contrary to the statement, it is *prima facie* evidence of a misrepresentation. Further, even when an employer responds truthfully to a prospective employer’s appropriate request, the employer may be liable if its response is unfavorable and in retaliation against an employee for having filed a claim under certain employee-protection laws.\(^{263}\)

It should be noted that certain federal laws require private employers to disclose specific information to prospective employers. For example, Federal Motor Carrier Safety Administration regulations require current or former employers to accurately respond to an inquiry from a truck driver’s prospective employer regarding whether the applicant driver has refused to take a drug test, or has tested positive for drugs, while employed as a truck driver with the former employer.\(^{264}\) Under the regulations, applicants are required to sign releases for the provision of such information prior to being allowed to perform safety-sensitive functions.\(^{265}\) To protect a former employer against the risk of being sued by a former employee for providing such information, the regulations have a safe-harbor provision that states that no action or proceeding for defamation, invasion of privacy or interference with a contract that is based on the furnishing or use of information in accordance with the regulations may be brought against the disclosing party.\(^{266}\)

Further, regarding current employees, Department of Transportation (DOT) regulations require medical certification for drivers of commercial motor vehicles. A federal court in Texas found that obtaining medical records for purposes of DOT certification did not invade a current employee’s right to privacy, even after the employee expressly refused to consent to the release of her medical records.\(^{267}\) In this case,

---


\(^{263}\) See, e.g., *Hillig v. Rumsfeld*, 381 F.3d 1028 (10th Cir. 2004) (employer violated Title VII by informing plaintiff’s prospective employer that plaintiff was a “sh---y employee,” in retaliation for plaintiff’s filing of previous discrimination complaints); *Smith v. BellSouth Telecomms., Inc.* 273 F.3d 1303, 1313 (11th Cir. 2001) (employer violated the Fair Labor Standards Act by informing a prospective employer that a former employee had filed a complaint seeking unpaid overtime).

\(^{264}\) 49 C.F.R. §§ 40.25, 382.413.

\(^{265}\) 49 C.F.R. § 40.25(a).


the court found that requesting the medical records was reasonable and justified because the leave administrator had obtained the records, for the purpose of determining whether the employee met DOT standards.\footnote{268}

Under the Health Care Quality Improvement Act,\footnote{269} a health care entity is required to report to the National Practitioner Data Bank certain disciplinary actions taken with respect to physicians. The statute includes immunity for health care entities who report such information.\footnote{270} At least one court, however, has recognized the limitations of this immunity. In \textit{Brown v. Presbyterian Healthcare Services}, the court held that, where the hospital’s reasons for disciplining a physician as stated in internal reports differed from the reasons reported to the National Practitioner Data Bank, the immunity provided by the statute did not shield the hospital from liability for defamation.\footnote{271}

The type of information that may be released to prospective employers is the subject of state law as well. Minnesota law, for example, delimits the various categories of information that may be released (with the consent of the former employee) by a private employer.\footnote{272}

\section*{§ 2.3(a) Liability for Defamation Arising from Release of Personnel Information}
For a discussion on defamation arising from the release of personnel information, see \textsc{Litl}ler On Employment Torts.

\section*{§ 2.3(b) Interference with Prospective Economic Advantage}
For a discussion on the tort of interference with prospective economic advantage, see \textsc{Litl}ler On Employment Torts.

\section*{§ 3 Global Information Sharing: The Impact of International Data Protection Laws on Multinational Employers}

\section*{§ 3.1 Distinctions in Global Approaches to Privacy}
Multinational employers may centralize all personnel data in one location from locations around the world for record-keeping, benefits and payroll purposes, and this centralization raises issues regarding the affected nations’ data protection laws. There are important distinctions between the privacy laws of the United States and other countries that must be taken into account whenever transferring employee data across national borders.\footnote{273}

A comparison of the United States’s privacy framework with the European Union’s comprehensive privacy regime highlights the significant differences between two global privacy models. Under the United States’s sectorial approach, certain sectors of the economy are protected by privacy laws. For

\footnote{268} 2007 U.S. Dist. LEXIS 85833, at *12.  
\footnote{269} 42 U.S.C. § 11133(a).  
\footnote{270} 42 U.S.C. § 11137(c).  
\footnote{271} 101 F.3d 1324, 1334 (10th Cir. 1996); \textit{see also} \textit{Odom v. Fairbanks Mem’l Hosp.}, 999 P.2d 123, 131 (Alaska 2000) (plaintiff’s complaint was sufficient to survive a motion to dismiss because it included allegations that hospital made knowingly false statements to National Practitioner Data Bank).  
\footnote{272} \textsc{Minn. Stat.} § 181.967.  
\footnote{273} \textit{See also} \textsc{The Litl\-ler Men\-delson Guide to International Employment and Labor Law} (5th ed. 2017). This publication includes information on data protection laws of 60 countries and the European Union. \textit{See} § 11.3 of each country-chapter for a discussion of data transfer restrictions.  

\textcopyright 2017 \textsc{Litl\-ler Men\-delson, P.C. All Rights Reserved}.  

\textcopyright 2017 \textsc{Litl\-ler Men\-delson, P.C. All Rights Reserved}.  

\textcopyright 2017 \textsc{Litl\-ler Men\-delson, P.C. All Rights Reserved}.
example, the medical industry is protected by the Health Information Portability and Accountability Act (HIPAA), and the banking and securities industry is protected by the Gramm-Leach Bliley Act (GLBA). Under this sectorial approach, no single authority is charged with enforcing and overseeing compliance with all privacy laws; instead, this responsibility is shared among a range of government agencies. For example, the U.S. Department of Health and Human Services enforces HIPAA, while the U.S. Consumer Financial Protection Bureau enforces GLBA. The European Union’s comprehensive data protection regime, on the other hand, protects all forms of personal data, defined as any information relating to an identified or identifiable natural person. Under the E.U. model, before personal data can be processed, which is defined to include collection, recording, storing, using or transferring the data outside of the European Union, the processing must comply with specific criteria. These criteria limit the situations in which an individual’s personal data can be collected, used, or disclosed. For more information on the approach taken by the European Union, see § 3.2.

The varying approaches to data protections globally adds complexity and uncertainty to a corporation’s best intentions to comply with applicable protections for employee information. Before undertaking a cross-border transfer of data, an employer must proactively ensure compliance with any pertinent data protection regime(s). The issues corresponding to any particular transfer will vary based on whether the transfer is to or from a country with strong privacy protections, such as those within the E.U. on the one hand, or to or from a country with little to no privacy protections in place.

To illustrate the challenges facing employers as a result of jurisdictional disparities, this section first discusses the general employment privacy regime and the obstacles confronted by companies and the approaches they utilize when transferring information or outsourcing administrative functions to countries with more established privacy regulatory schemes (e.g., countries within the E.U.) and with limited protections (e.g., China and India).

§ 3.1(a) The U.S. Approach
The United States uses a sectored approach to data protection, which relies on a combination of legislation and regulation at the federal, state and local levels, in addition to self-regulation. Employers in the United States should expect restrictions on data transfers imposed based on ad hoc factors. For example, in some instances, federal or state constitutions or statutes confer privacy protections based on location, such as in one’s home. In other instances, the United States’ sectored approach provides protections based on the type of information. For example, the ADA and GINA impose strict limitations on the disclosure of employee health information, even within the corporate entity or to related entities. The United States’ approach may also vary based on the reason for the collection.

§ 3.1(b) The European Union Approach
If a business’s transborder data flow emanates from one of the Member States of the E.U., the organization will confront a markedly different approach to privacy and data protection than experienced in the United States. In Europe, privacy is viewed as a fundamental human right. European countries have enacted comprehensive lawmaking to protect the privacy of individual citizens both at work and at

275 The 28 Member States of the European Union are Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and (until “Brexit” is implemented) the United Kingdom. Under the European Economic Area (EEA) agreement, Iceland, Lichtenstein and Norway have implemented data protection laws similar to those in place in the Member States, although these countries are not members of the E.U.
276 Many countries outside the E.U., including Argentina, Australia, Canada and the territory of Hong Kong, have enacted data protection laws based upon the European model. A discussion of the specific differences between the data protection laws of these countries and those applicable to the E.U. Member States is beyond the scope of this publication.
home. European privacy laws generally apply to all forms of individually identifiable information and generally do not distinguish among various categories of information (e.g., financial records, video rental information, model and color of a person’s car, home address and telephone records), as is the case in the United States. While E.U. laws have enacted a baseline level of protection to all forms of individual information, the E.U. provides additional protections for certain categories of sensitive information, including medical records or information concerning one’s sex life.

As applied to the employment context, multinational employers may not be able to apply standard U.S. business procedures to subsidiaries or related entities in the E.U. without due consideration. Where U.S.-based companies may ordinarily seek to obtain certain types of personal information from applicants or employees—such as national origin or even smoking status—obtaining certain categories of “sensitive personal data,” such as race or ethnic origin, may be prohibited in the E.U. in certain circumstances. For example, a U.S. company motivated to increase diversity may ask for information related to one’s age, race, national origin or other protected category; however, E.U. data protection laws impose strict limits on employers’ collection of information concerning an employee’s race or ethnic origin.

Monitoring e-mails presents a further example of enhanced privacy rights confronting employers in the E.U. While generally speaking, a U.S.-based multinational can transfer, without restriction, an employee’s e-mail on the company’s U.S. server to an E.U. subsidiary, the E.U. regulates a broader spectrum of information than the United States so that the disclosure of certain types of information permitted under U.S. law may not be permitted under the laws of other countries. To illustrate this point, in the E.U., the European Court of Human Rights awarded monetary damages to an employee when her employer, a college in Wales, monitored her e-mail account without her knowledge. The court ruled that the college’s surreptitious monitoring of the employee’s e-mail activities “amounted to an interference with her right to respect for her private life and correspondence,” despite the fact that the college owned the computers and e-mail accounts through which the communications had been transmitted. Furthermore, in a 2013 decision, the Brussels Labour Court of Appeal refused to admit a former employee’s e-mails into evidence to establish the employer’s justification for the employee’s termination because the employer’s actions in reviewing the employee’s e-mails violated E.U. and Belgian privacy rules.

§ 3.1(b)(i) Works Councils

One selective area of added privacy protections in the E.U. may apply to employers. Specifically, the E.U. Works Council Directive imposes a duty upon certain large employers with 1,000 or more E.U. employees and at least 150 employees in two or more Member States to inform and/or consult with a works council—that is, an organized panel of plant-level employees—before making decisions that touch upon the privacy rights of its workers. Another directive aimed at employers with only 20 or 50 employees in the E.U., depending upon the choice made by a Member State, discusses national works councils and the adoption of certain minimum standards on consultation and the sharing of information between management and workers. Although the subjects upon which the company must confer with a works council vary with each Member State, these subjects often include collection of employee data,


©2017 LITTLED MENDELSON, P.C. ALL RIGHTS RESERVED.
data protection policies, employee monitoring policies, implementation of new technologies in the workplace and transfers of employee information to foreign affiliates.

Consultation with a works council may be a lengthy and arduous process and require formalized documentation in certain circumstances. However, in most E.U. Member States—Germany excluded—the positions taken by works councils are nonbinding and do not limit the actions that the company ultimately may take. Nevertheless, consultation with works councils is not a voluntary exercise, and failure to do so may result in negative publicity and damage to a company’s goodwill with its employees.

§ 3.1(c) The Latin American Approach
Eleven countries throughout Central and South America have adopted data privacy regulations: Argentina, the Bahamas, Chile, Colombia, Costa Rica, Mexico, Nicaragua, Peru, Saint Lucia, Trinidad and Tobago and Uruguay. Several of these regulations involve similar requirements as E.U. and U.S. data protection regulations. For example, Colombia, Costa Rica, Nicaragua, Peru, and Trinidad and Tobago have established data protection authorities responsible for overseeing compliance with the data protection laws. Several other laws regulate the appropriate manner for transferring documents and providing notice to individuals of that transfer. Unlike the E.U., however, there is no common directive for the data protection laws in Central and South America. Because of this, employers must interpret each country’s data protection laws individually.

§ 3.2 E.U. Data Protection Directive & the Upcoming General Data Protection Regulation
Following the formal adoption of the Data Protection Directive 95/46/EC (“Directive”) on October 24, 1995, each E.U. member state was responsible for enacting its own laws that implemented the fundamental principles of the Directive. This resulted in considerable differences in the data protections laws of each member state, causing legal uncertainty and significant administrative costs and burdens for companies. To address those issues, on December 15, 2015, the European Parliament, Council and Commission agreed to new data protection rules introduced as the General Data Protection Regulation (GDPR) that will repeal and replace the Directive. The GDPR passed its final legislative hurdle when it was adopted by the European Parliament on April 14, 2016. The GDPR went into effect on May 24, 2016 with its publication in the Official Journal of the European Union, and all E.U. Member States will have to be in compliance with the GDPR by May 25, 2018.

The GDPR establishes a harmonized data protection framework across the E.U. that is intended to make the rules for companies more uniform and to strengthen citizens’ fundamental rights. Once fully implemented, the GDPR should eliminate country-specific differences in data protection requirements that increase compliance burdens, although local labor laws still could result in country-specific requirements for the processing of employees’ personal data.

§ 3.2(a) E.U. Data Protection Directive’s Application to Employment Law
Until the GDPR takes effect in May 2018, the 1995 Directive sets the minimum standards for the applicable law in the European Union. The Directive’s objectives are twofold:

---

©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
1. to protect individuals with respect to the processing of personal information; and

2. to ensure the free movement of personal information within the E.U. through the coordination of national laws.

The Directive is broad in scope. It encompasses all categories of individually identifiable personal information, not just discrete categories of personal data, such as health or financial information. Employee personnel information is covered, including names, addresses, phone numbers, gender type, employee identification numbers, resumés, educational histories, e-mail addresses, pay rates, benefits, performance reviews and training records. The Directive applies to all forms of data processing—which is defined to include all functions with respect to personal data, such as collection, use, disclosure, storage and destruction—whether online or offline, manual or automated. This term excludes only processing “in the course of purely personal or household activity.” In its first decision addressing application of the Directive, the Court of Justice of the European Communities construed this exemption narrowly, holding that the posting by a church volunteer of a web page containing personal information about other church members fell outside the exemption because this activity “clearly extended beyond [the volunteer’s] personal and domestic circle.”

The fundamental principles of the Directive, as applied to the employment context, include the following:

- **Legitimacy**: The employer (the “data controller”) may process an employee’s (the “data subject’s”) personal data only: (1) with the employee’s prior consent; (2) as necessary to perform the employment contract; (3) to the extent necessary to comply with legal obligations; or (4) for other legitimate interests of the employer.

- **Notice or Transparency**: Before processing personal data, the employer must inform the employee of the personal data being collected, how and why the personal data has been or will be processed, to whom the data has been or will be disclosed and whether the data will be exported outside the E.U.

- **Proportionality**: The employer may process data for the purposes disclosed in the notice to employees, or for compatible purposes. The personal data which is processed under the Directive must be the minimum necessary to carry out that purpose. It would violate this “minimum necessary” requirement, for example, to require that a job applicant furnish his or her prospective employer with the European equivalent of a Social Security number, if that number would not be used in the hiring process.

- **Access**: The employer must: (1) grant each employee’s reasonable request for access to the personal data it maintains; (2) provide each employee with the opportunity to correct, erase or block further processing or transfers of inaccurate, outdated or incomplete data; and (3) notify any third party to whom inaccurate, outdated or incomplete data has been disclosed of any additions or corrections made in response. While some ad hoc U.S. federal or state authority provides employee access to some employee documents (such as personnel files), the scope does not approach the access requirements in the Directive.

---

288 See e.g., cal. lab. code § 1198.5.

©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
• **Security:** The employer must implement technical and organizational safeguards to protect the data from unauthorized access and disclosure. These types of security are often imposed in the U.S. based on the type of information, if, for example, it is medical information.

• **Accuracy:** The employer must take steps to ensure that personal data is accurate and up-to-date.\(^ {289}\)

The Directive requires each E.U. Member State to enact implementing legislation that incorporates the Directive’s guiding principles into the Member State’s own national laws. The Directive further requires that each Member State establish a “data protection authority,” an administrative agency responsible for enforcing the laws implemented in the Member State to effectuate the Directive’s guiding principles.\(^ {290}\) Before processing any personal data, the national data controller generally is required to notify the local data protection authority of that processing through a public filing.\(^ {291}\)

§ 3.2(b) E.U. General Data Protection Regulation’s Application to Employment Law

Only one of the GDPR’s 91 articles specifically addresses the personal data of prospective, current or former employees (collectively, “employee data”). Article 81 of the version published by E.U. authorities in December 2015 provides that E.U. Member States may enact laws specific to the processing of employee data to implement the GDPR. For multinational employers, this provision could defeat one of the principal putative benefits of the GDPR—to establish a single set of data protection rules applicable in all E.U. Member States to eliminate complexity, ensure consistency and reduce administrative costs. In respect of employee data, the GDPR should therefore be read in conjunction with any applicable laws of relevant E.U. Member States that regulate the handling of employee data.

Even though the GDPR specifically addresses employee data in only one article, the GDPR applies broadly to the processing of all “personal data,” which is defined to mean “any information related to an identified or identifiable natural person.” Consequently, U.S. multinationals need to determine how to apply, in the employment context (together with the applicable local employee data protection laws), regulatory requirements designed to protect online consumers and numerous other categories of data subjects.

The GDPR’s scope is broad in another way that impacts U.S.-based multinationals. The GDPR applies to all E.U. residents, regardless of citizenship. For U.S.-based multinationals, this means that expatriates working at an E.U. subsidiary are entitled to all of the GDPR’s protections when their data is collected while they reside in the European Union.

Additional highlights from the GDPR that multinational employers should consider include:

- Employers can only “process” employee data if the GDPR specifically permits the processing.

- The GDPR requires that data controllers distribute a notice of data processing to each individual when personal data is first collected. As applied in the employment context, this means that employers will be required to provide a notice to job applicants concerning the processing of their data during the application process as well as a notice to new hires, typically during the

---


©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
onboarding process, explaining how their personal data will be processed during the employment relationship.

While the basic notification requirement is unchanged from the Data Protection Directive, the GDPR requires a far more robust notice. The notice must include the following information: (1) the identity and contact details of the employer; (2) the purposes for the processing and when the processing is based on legitimate interests, a description of those interests; (3) the categories of recipients of disclosures of personal data; (4) that the controller intends to transfer personal data to a third country and the legal basis for the transfer; (5) the period for which the personal data will be stored or the criteria for determining the period; (6) how employees can exercise the rights of access, correction, erasure and objection; (7) where processing is based on consent, the right to withdraw consent; (8) the right to file a complaint with a data protection authority (DPA); (9) whether the employee is obliged to provide the data by statute, contract or for another reason, and the possible consequences of failing to provide the data; and (10) whether the personal data will be subject to automated processing and, if so, the logic and consequences of the processing for the data subject.

- The GDPR places substantial emphasis on individuals’ rights of access, correction, erasure and objection as a means of achieving the new law’s broader objective of protecting individuals’ fundamental right of privacy. To that end, the GDPR requires that employers provide employees with a mechanism to exercise these rights and to respond, in writing, to any request without undue delay and, at the latest, within one month. The response period may be extended for up to two additional months in light of the complexity and number of requests. Any denial of a request must include the reasons for the denial and the right to file a complaint with the DPA or to seek judicial relief. All responses to requests must be free of charge unless the request is manifestly excessive (generally because it is repetitious). If the employer has doubts regarding the identity of a person making a request, it may ask for verification of the person’s identity.

While prior law provided a right of access and correction, the right of erasure (also known as the “right to be forgotten”) is new. Employees generally have the right to require the employer to delete their personal data when, for example: (1) the data no longer is necessary for the purposes for which it was collected; (2) the employee has withdrawn consent to processing, and no other ground for processing is available; and (3) the employee objects to processing, and there is no compelling ground that overrides the employee’s interests. However, employers are not required to erase any employee data that they are required to retain under E.U. or Member State law that is necessary to establish, pursue or defend legal claims.

- The GDPR requires employers to implement administrative and technical safeguards for employee data to reduce identified risks and to prevent a “personal data breach.” The GDPR defines a breach to mean a “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.” The GDPR does not specify safeguards that must be implemented, but it identifies the following steps and objectives as potentially appropriate: (1) pseudonymization and encryption; (2) the ability to ensure the confidentiality, integrity and availability of personal data; (3) disaster recovery capabilities; and (4) a process for regularly testing, assessing and evaluating the safeguards.

- When a personal data breach occurs, the GDPR requires prompt action. The employer must notify the DPA within 72 hours, and if that notification is delayed, explain the reason for the delay. Notification is not required if the breach “is unlikely to result in a risk for the rights and freedoms of individuals.” The employer must document its breach response sufficiently to permit the DPA to verify compliance with the GDPR.

Employers must notify affected employees of a personal data breach “without undue delay,” if the breach is “likely to result in a high risk to the rights and freedoms of individuals,” or if
ordered to do so by the DPA. As with U.S. breach notification laws, the GDPR establishes an “encryption safe harbor,” meaning that the employer is not required to notify affected individuals if their personal data is subject to encryption that renders the information unreadable. Notification to individuals also is not required if: (1) the employer took steps to ensure that the high risk to employees does not materialize; or (2) notification would involve disproportionate effort, but in this case, the employer must provide notice by public communication, such as by posting notice on a website or by publication in the media.

- The GDPR specifies a long list of matters that must be addressed in the service agreements with vendors that access personal data from Europe. The service agreement must address, for example: (1) the subject matter and duration of the processing; (2) the nature and purpose of the processing; and (3) the types of personal data and categories of data subjects. The service agreement also must impose numerous obligations on the service provider, including, for example, that the service provider: (1) process personal data only subject to the employer’s instructions; (2) require its employees to execute a confidentiality agreement; (3) implement required security measures; (4) assist the employer fulfill its obligations to respond to requests by employees to exercise their rights; and (5) cooperate with the employer in fulfilling its breach notification obligations.

- The GDPR provides that the processing of “special categories of personal data,” also known as “sensitive personal data,” is prohibited unless an exception applies. Sensitive personal data includes race or ethnic origin, data concerning health or sex life and sexual orientation, trade-union membership, genetic data, biometric data, political opinions, and religious or philosophical beliefs. An employer can process sensitive personal data only in the following limited circumstances: (1) the employee gives explicit consent (except where the law does not permit the employee to consent); (2) processing is necessary for the employer to fulfill obligations and exercise specific rights established by E.U. or Member State law; or (3) processing is necessary to establish, pursue or defend against legal claims. In addition, a health care professional can process personal data concerning an employee’s health when necessary for preventive or occupational medicine, to assess the working capacity of the employee or to provide care. Given the GDPR’s emphasis on protecting sensitive personal data, regulators likely will narrowly construe these exceptions. The GDPR also establishes a special rule for the processing of criminal history information, albeit that category is not specifically identified as sensitive personal data. Under that special rule, an employer can process criminal history information—even with an applicant’s or employee’s consent—only if specifically authorized by E.U. or Member State law to perform a criminal history check.

- The GDPR requires that employers maintain detailed records concerning their data processing. These records must be provided to the DPA upon request. The information to be recorded includes the following: (1) contact information for the employer; (2) the purposes of the processing; (3) the categories of data subjects and of personal data processed; (4) the categories of recipients, including those in third countries; (5) the third countries to which personal data will be transferred and the instrument, e.g., Standard Contractual Clauses (SCCs) approved by the European Commission or binding corporate rules (BCRs) used to provide an adequate level of protection; (6) where possible, the envisaged retention periods for different categories of employee data; and (7) a general description of the security measures for employee data.

Overall, the GDPR will not demand dramatic changes in the policies and procedures previously implemented to comply with the Directive. While the compliance requirements have not changed significantly, the enforcement risk has increased dramatically. The GDPR empowers data protection regulators to impose administrative fines of 20 million Euro, or up to 4% of a corporate group’s worldwide gross annual revenue, for most violations and up to 2% of that amount, or 10 million Euro, for less serious violations. Regulators also can ban data processing at the E.U. subsidiary and suspend data transfers to the parent corporation. Consequently, U.S.-based multinationals should take advantage of the two-year grace period to come into compliance.

©2017 LITTLEG MENDELSON, P.C. ALL RIGHTS RESERVED.
§ 3.2(c) Transfer of Data to the United States & Other Countries

Of particular significance for U.S. employers with employees in the E.U., personal data generally cannot be transferred from an E.U. Member State to a country outside the E.U. unless the “data exporter” first obtains the approval of the national data protection authority. Approval may be denied if the recipient of the personal data resides in a country that does not provide “an adequate level of protection,” meaning privacy protections similar to, or more stringent than, those required by the Directive.292

The “adequacy” standard creates a potential barrier to data exports from the E.U. to the United States. The European Commission, the E.U.’s executive body, has determined that United States privacy law does not provide “an adequate level of protection.” National data protection authorities can rely upon that determination to block data exports to the United States and to seek administrative penalties from, and criminal prosecution of, those who intentionally circumvent this restriction.

§ 3.2(c)(i) Invalidation of U.S. – E.U. Safe Harbor Framework & Adoption of the Privacy Shield

Until October 2015, multinational employers could rely on a Safe Harbor Framework, an agreement forged years ago between the U.S. Department of Commerce and the European Commission to permit the transfer of personal data. In 2000, the Commission ruled that the Safe Harbor Framework would meet the “adequate level of protection” standard.293 Under the Framework, U.S. businesses wishing to receive personal data from the E.U. were required to: (1) post a Safe Harbor Privacy Policy in which they represented their intention to adhere to seven Safe Harbor Principles designed to protect the data;294 (2) submit a self-certification form through the Commerce Department’s Safe Harbor website; and (3) pay a required fee.295 The FTC had responsibility for enforcing the Safe Harbor Framework.296

In October 2015, the E.U. Court of Justice (ECJ) invalidated the Safe Harbor Framework. The ECJ held that the Safe Harbor Framework did not ensure an “adequate level of protection” for personal data because of lack of meaningful enforcement by the FTC, access to personal data by intelligence agencies (highlighted by Edward Snowden’s leaks demonstrating that U.S. intelligence agencies are permitted to collect substantial quantities of personal data) and the inability of E.U. citizens to seek administrative or judicial redress for the collection of their personal data under U.S. surveillance programs.297

The invalidation of the Safe Harbor Framework caused a radical structural change in the relationship between the European Union and the United States as it pertains to cross-border data transfers. Before the ECJ’s ruling, more than 4,000 U.S. businesses had relied on the Safe Harbor to legitimize cross-border

---

294 The seven principles addressed: (1) notice; (2) choice (i.e., affirmative consent or opportunity to “opt out” of information’s disclosure); (3) transfer rules related to a third-party nonagent; (4) security; (5) data integrity; (6) access; and (7) enforcement.
295 Information on the Safe Harbor Framework can be found at the Commerce Department’s website (http://export.gov/safeharbor/).
297 Other countries, both inside and outside the European Union acted to revoke their safe harbors after the European Union acted, including Switzerland, Israel, Dubai, Portugal and Spain.
data transfers. As a result, the group of European data protection regulators from each of the 28 E.U. Member States, known as the Article 29 Working Party, were under pressure to issue guidance on the implications of the ECJ’s decision. On February 2, 2016, E.U. and U.S. negotiators announced the outline of the “Privacy Shield” as the new framework for trans-Atlantic data transfers. The European Commission issued its determination that the Privacy Shield provides an “adequate level of protection” on July 12, 2016, and the Privacy Shield went into effect on August 1, 2016. The Privacy Shield is in many ways similar to the invalidated Safe Harbor.

Because of continued uncertainty over the Privacy Shield, however, U.S.-based multinationals should remain vigilant in monitoring developments. Notably, when the European Union’s top data protection regulatory body, the Article 29 Working Party (the “Working Party”), completed its initial review of the proposed Privacy Shield, it expressed “strong concerns” with the new framework. The European Data Protection Supervisor followed with a lengthy critique of the Privacy Shield in June 2016. These critiques, therefore, provide a playbook for a legal challenge to the Privacy Shield. The Privacy Shield may also be materially revised in the future based on these critiques. For example, the Article 29 Working Party raised concerns that the Privacy Shield does not provide an adequate level of protection as required by the GDPR, discussed at § 3.2(b). Furthermore, there is currently more than one pending lawsuit challenging the Privacy Shield. It is unclear at this time whether the European Commission is planning to address concerns by revising the Privacy Shield.

Consequently, employers need to decide whether to adopt the Privacy Shield (see § 3.2(c)(ii)) or turn to one of two long-standing alternatives to the Privacy Shield and Safe Harbor certifications (see § 3.2(c)(iii)). To make this decision, employers should consider undertaking a thorough (and privileged) review of their current data protection practices for E.U. employees’ personal data and evaluate the available options for such data transfers moving forward. A description of the Privacy Shield, as well as long-standing alternatives to the Privacy Shield and Safe Harbor certifications, are discussed immediately below. Additional recommendations to employers in implementing the Privacy Shield are included at § 4.6.

§ 3.2(c)(ii) U.S. – E.U. Privacy Shield

As with the Safe Harbor, the basic steps necessary to enjoy the Privacy Shield’s benefits are straightforward. An eligible U.S. organization must self-certify on the Commerce Department’s Privacy Shield website and publish a Privacy Shield Privacy Policy that embodies the Privacy Shield Privacy Principles. U.S. organizations were able to self-certify beginning August 1, 2016.

Self-certifying for transfers of human resources (HR) data in the context of the employment relationship is substantially the same as self-certifying for transfers of other types of personal data. The organization will be required to provide basic information, including, for example, the organization’s contact information, information about the data transfer and information about the organization’s privacy policy. A corporate officer must sign the self-certification form.


301 The certifying entity must be subject to the jurisdiction in the United States of either the FTC or the Department of Transportation.
Self-certification for transfers of HR data entails one critical distinction from other types of data transfers. The organization is required to choose E.U. data protection authorities (DPAs) from among the several available independent dispute resolution mechanisms. In addition, organizations must pay a fee that will not exceed $500 dollars, and will be less for smaller companies, to subsidize this dispute resolution mechanism.

The “human resources privacy policy” submitted with the self-certification must contain the same mandatory elements as other Privacy Shield privacy policies. The policy must address the organization’s commitment to all seven of the “Privacy Shield Privacy Principles” (the “Principles”). These Principles include Notice, Choice, Accountability for Onward Transfers, Security, Data Integrity and Purpose Limitation, Access, and Recourse/Enforcement and Liability. To satisfy the Commerce Department that the HR privacy policy fully addresses the Principles, the policy submitted by the certifying organization must contain a long list of required elements including, among others:

1. an identification of all U.S. affiliates that will access transferred personal data and their commitment to adhere to the Principles;
2. the categories of personal data collected;
3. the purposes for the collection;
4. the third parties to which data may be transferred;
5. a description of data subjects’ access rights; and
6. a contact for requests to exercise individual rights and submit complaints.

There is one significant distinction between an HR privacy policy and privacy policies addressing other types of personal data under the Privacy Shield. The HR privacy policy does not have to be posted on a publicly available website. Instead, the policy must be posted where it will be available to all E.U.-based employees whose personal data will be transferred to the U.S. subject to the Privacy Shield. This typically means that the policy will be posted on the corporate intranet. Organizations that choose not to publicly post their HR privacy policy will be required to submit the policy with the self-certification form rather than just providing a link.

Once the certifying organization completes these basic steps, the Commerce Department will review the self-certification form, to confirm that required information has been provided, and the HR privacy policy, to confirm that it addresses all required elements. If so, the Commerce Department will list the U.S. parent corporation and any certifying affiliates on its Privacy Shield List. Immediately after the listing, the E.U. subsidiaries can begin transferring their employees’ personal data to the U.S. Because the European Commission has determined that the Privacy Shield “ensures an adequate level of protection for personal data,” the E.U. subsidiaries will not need to obtain additional approvals from local DPAs, albeit in some countries, such as France, the DPA must be notified of the data transfer.

The Privacy Shield can be used to transfer personal data of both current and former E.U. employees. The U.S. parent corporation must apply the Principles to all transferred data for as long as that information is retained, even if the parent corporation subsequently decides to withdraw from the Privacy Shield. An organization that withdraws from the Privacy Shield will be required to satisfy the annual verification and recertification requirements for as long as the organization retains personal data transferred pursuant to the Privacy Shield.

Additional information on the Privacy Shield and the steps that an employer should consider taking to implement a Privacy Shield compliance program are discussed at § 4.6.
§ 3.2(c)(iii) Continued Alternatives to the Privacy Shield Certification

Two principal alternatives are available to the Safe Harbor and Privacy Shield certifications, each of which presents its own challenges. Employers can consider using the “Standard Contractual Clauses” (SCCs) approved by the European Commission or relying on binding corporate rules (BCRs). There are also certain exceptions to the Data Protection Directive, referred to in E.U. parlance as “derogations,” that may apply in the employment context.

Standard Contractual Clauses

SCCs (also referred to as “Model Clauses”) remain a valid mechanism for transferring personal data outside the E.U. The SCCs are sets of model contract clauses embedded in a data transfer contract that the Commission has determined ensure an adequate level of protection for transferred personal data. Two sets of the clauses relate to the transfers between controllers, such as transfers between E.U. subsidiaries and their U.S. parent corporation, while another clause addresses transfers between a controller and a processor, such as transfers between an employer and a service provider.

In an implicit rebuke to some national data protection authorities who have questioned the continued viability of the SCCs after the ECJ’s decision, the Communication states that national data protection authorities “may not refuse the transfer of [personal] data to a third country on the sole basis that these SCCs do not offer sufficient safeguards.” However, the Commission acknowledges that national data protection authorities may continue to require submission of the SCCs for review to confirm that none of the standard clauses have been modified. The E.U. countries where Model Contracts must be submitted for review include, for example, Austria, France, Portugal, Romania and Spain.

In addition to the potential delay caused by this review, SCCs can also be unwieldy, administratively burdensome and slow to implement. The parties to these agreements cannot modify the SCCs, in any respect, to address any factual circumstances specific to their relationship. In addition, the parties are required to complete a form appendix to the SCCs that describes the data transfer in substantial detail, including the categories of data to be transferred and the purposes for which the transferred data will be processed. When the data importer needs to import additional categories of personal data or use the personal data transferred for new purposes, the appendices to the data transfer agreements must be amended. When a U.S. multinational has a large number of EU subsidiaries, managing these agreements and the amendments to them can be administratively burdensome.

Binding Corporate Rules

BCRs provide another alternative mechanism to the Safe Harbor for transfers of personal data within a corporate group. BCRs involve the development and implementation of a uniform set of rules that provide the high level of protection for personal data required by the Directive and are binding on all members of the corporate group, regardless of location.

While BCRs may initially appear to be a ready-made solution for U.S. multinationals that previously relied on Safe Harbor certification, they likely will not provide the answer for most companies. Notably, since the Commission first approved BCRs in the early 2000s, fewer than 100 companies globally and fewer than 30 in the U.S. have implemented them. Those organizations that have implemented BCRs are among the largest, richest and most sophisticated U.S. corporations. BCRs likely have been selected by so few organizations (as compared to the more than 4,000 organizations certified to the Safe Harbor)

302 Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems) (Nov. 6, 2015).


©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
because of the onerous approval process. The data protection authority of each country where the U.S.
organization has a subsidiary with employees is entitled to an opportunity to review and comment on the
BCRs. Additionally, the Conference of German Data Protection Authorities issued guidance that, for
now, German data protection authorities will not approve BCRs.304

This review and approval process can require substantial resources to navigate and routinely takes more
than one year to complete. Moreover, with the invalidation of the Safe Harbor, many data protection
authorities likely will see a spike in requests for approval of BCRs, resulting in additional delay. With the
low cost and ease of trans-Atlantic telecommunications, many smaller U.S. companies are now
multinational employers. These companies typically will not have the internal resources, financial capital
or time to complete the BCR review and approval process.

Derogations

As with most legal rules, the Directive sets out several exceptions (or “derogations”) to the general rule
that personal data cannot be transferred to a third country unless that country “ensures an adequate level
of protection” for personal data. The November 2015 Communication from the European Commission
highlights the relatively limited value for employers of the derogations as an alternative to the Safe
Harbor. The only two derogations potentially applicable in the employment context are: (1) transfers with
the unambiguous consent of the data subject (i.e., the employee); and (2) transfers that are necessary for
the performance of a contract between the data subject (i.e., employee) and the controller (i.e., the E.U.-
based employer). On the first, the Communication echoes the commonly held view that employers
generally cannot rely on employees’ consent to transfer personal data outside the EU because of “the
relationship of subordination and inherent dependence of employees.”305 As a result, employees’ consent
generally cannot be “freely given,” which is required for consent to be valid.

For the second, “performance-of-contract” derogation to apply, the Commission explains that “there has
to be a ‘close and substantial connection,’ a ‘direct and objective link’ between the data subject and the
purpose of the contract.”306 In other words, a multinational employer might be able to rely on this
derogation to justify transfers of personal data if needed to administer payroll. However, the E.U.
subsidiary/employer likely would not be able to rely on this derogation to justify the parent corporation’s
use of E.U. employees’ personal data for purposes less tightly tied to performance of the employment
agreement between the E.U. employee and the E.U. subsidiary, such as global diversity initiatives, global
training programs or global succession planning.

§ 3.2(d) Role of Brexit

It remains to be seen how the United Kingdom’s decision to exit the European Union will influence the
transfer of personal data and requirements for multinational employers. Once the United Kingdom leaves
the European Union, it will no longer be required to align its data protection laws with the
GDPR. However, it may be within its interest to do so to facilitate transfers of personal data from the
European Union to the United Kingdom. For example, if the United Kingdom were to join the European
Economic Area (such as Norway, Lichtenstein and Iceland), it would be required to continue to comply
with the GDPR, and there would be no restrictions on cross-border data transfers. Alternatively, the
United Kingdom may seek an adequacy determination from the European Commission, similar to the
arrangement entered into with Switzerland. This would require a finding that the United Kingdom’s data

305  Communication from the Commission to the European Parliament and the Council on the Transfer of Personal
Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of
Justice in Case C-362/14 (Schrems) (Nov. 6, 2015).
306  Communication from the Commission to the European Parliament and the Council on the Transfer of Personal
Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of
Justice in Case C-362/14 (Schrems) (Nov. 6, 2015).
©2017 LITTLE MENDELSON, P.C. ALL RIGHTS RESERVED.
protection laws provide an adequate level of protection. If the Commission were to issue such a determination, it would allow the free transfer of personal data between the United Kingdom and the European Union.

The United Kingdom has been following E.U. data protection regulations for 15 years, so it is likely that the European Commission would make a determination that the United Kingdom’s data protection laws (unless drastically modified post-Brexit) provide an adequate level of protection. That said, U.S.-based companies with operations in the United Kingdom should assess whether there are significant transfers of personal data from Member States to the United Kingdom. Companies should also watch for guidance from E.U. regulators regarding compliance with the GDPR and examine any existing model contracts and binding corporate rules addressing data transfers to assure compliance and accuracy.

§ 3.3 SAFEGUARDING PRIVATE INFORMATION IN COUNTRIES WITH LESS ESTABLISHED PRIVACY PROTECTION SCHEMES

Operating between or among jurisdictions with well-established privacy regimes such as the European Union and United States can cause multinational companies to grapple with harmonizing and interpreting privacy laws. In the alternative, companies may choose to expand into countries with lesser workforce protections than the United States and the European Union. Avoiding conflicts between the existing privacy laws of more developed jurisdictions is one reason to outsource administrative functions and/or expand business into areas with less developed privacy laws. Outsourcing into these areas may also be induced by rapid expansion, the desire for cost savings, staffing shortages or any number of other reasons.

Regardless of the reason, such an expansion will in some instances lead to the international transfer of private employee data from a more-regulated area to a less-regulated area. In the absence of applicable laws in jurisdictions with undeveloped privacy protections, the preservation of employee privacy likely will result principally from the measures a company takes to safeguard the security of personal data.

In jurisdictions with less-developed privacy regulations, there may be little or no recourse for the disclosure of information. However, even if a foreign host does not provide an adequate remedy, the disclosure of private employee information by employees in other countries has the potential to create liability in the United States under the theories of agency and/or vicarious liability, among others. Thus, companies cannot consider outsourcing a “race to the bottom” in terms of seeking the lowest required privacy protections. To the contrary, as between two jurisdictions, a company often will be required to contractually ensure that personal data transferred to the jurisdiction with the less stringent requirements continues to receive the safeguards mandated by the jurisdiction with the more stringent requirements.

While not an exhaustive list of actions to be taken, the following are some proactive steps that a company can take to heighten safeguards for the personal data that is transferred to an offshore outsourcer:

- **Contractual Arrangements.** Contractual arrangements with any third-party provider, contractor, or employee can put in place the needed confidentiality conditions to comply with applicable regulations. Contracts between a foreign contractor or other third-party provider can specify a contractual remedy that requires the posting of a bond, for example, to secure recovery in the event information is compromised. By listing specific laws or regulations and requiring acknowledgement, companies can require foreign employees, contractors, or other third-party providers to expressly acknowledge the existence and applicability of laws or regulations, and can require their agreement to abide by the laws or regulations. Other contractual arrangements can include choice-of-law and choice-of-forum provisions specifying that any matter shall be tried in the United States and subject to U.S. law.

307 See RESTATEMENT (SECOND) OF AGENCY § 405 (for discussion of liability between agent and principal).

©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
Alternatively, the arrangement can require adjudication outside of the United States, provided that laws of another jurisdiction, such as the United States, will be applied. Finally, a contract can also require a private form of dispute resolution, such as binding arbitration that can be adjudicated under specified privacy laws. In this way a company can individually agree to privacy protections in order to fill the regulatory vacuum of less-regulated jurisdictions and comply with the data protection requirements of the jurisdiction from which the information originates.

- **Policies & Procedures.** A company’s policies and procedures can establish the framework necessary to protect sensitive employee information. Employers may also require proper usage of company resources and should include such requirements in their employment handbooks or labor manuals as internal policy. Policies can specify retention periods, proper methods for destruction of personal data, and redaction and copying policies. In appropriate circumstances, a company’s handbook and policy statements can also serve to notify employees of how their information will be handled, where it may be transmitted, and may provide a mechanism to address any employee concerns.

- **Physical & Technological Safeguards.** Outsourcing contracts and employment policies can specify appropriate physical technological safeguards for personal data to ensure that the information is transmitted, retained and destroyed in a manner that prevents unauthorized use or disclosure. These safeguards can include a prohibition on bringing any items that could be used to store personal data in or out of a restricted area. Employers also can limit access to those individuals with a “need to know.” Tracking numbers, encryption and other technologies that prevent copying also may be employed.

- **Investigate Third Party Providers, Employees & Individuals Who Will Have Access to Personal Information.** To the extent a company intends to use a third-party provider to house information off-shore, an employer should scrupulously investigate the foreign company it selects to handle the personal information of employees, both in terms of its professional integrity and competence. The thoroughness of the investigation should correspond to the sensitivity and the volume of the information, and may in certain circumstances require the assistance of an investigator or other professional. An investigation may include conducting a background check of the company, obtaining and contacting references, verifying the company’s past performance and reputation in the industry, requiring the company to complete an information security questionnaire, and evaluating any claims leveled against the company. An investigation may also include interviewing, choosing, and investigating the individuals who are charged with performing the work. It may require that the company or employee is professionally credentialed. A company should confirm that the foreign company or individual is familiar with privacy requirements of the jurisdiction from which the information originates.

- **Monitor & Audit.** Periodic audits will help verify that the policies, procedures, and safeguards initially put into place are actually followed and accomplish their intended purposes. The audits also will provide a mechanism to reassess and modify policies in light of developing practices, law, and technology.

- **Obtain Advice on Rights & Remedies Available in the Jurisdiction.** An informed legal opinion in the applicable jurisdiction is important to determine the remedies that are available for a security breach involving confidential information. When crafting appropriate safeguards, a legal opinion also will be important to determine the enforceability of the desired safeguards. A company should consider not only the substantive laws of the jurisdiction concerning confidentiality and privacy, but also other procedural and substantive rules that can impact the ability to maintain privacy. For example, a company that enters a contract with a third-party provider, employee, or contractor in another country will have to
obtain an opinion on the enforceability of the agreement and its provisions. If a choice-of-
law provision is not effective in a particular jurisdiction, then its inclusion in a contract will
be useless. An opinion also will be needed regarding the likely interpretation of any
agreement. Advice on contending with the practical problems of a country’s particular legal
system also will be of great benefit. Once information is transferred to a jurisdiction, an
opinion on the ability to gain access to that information in that jurisdiction likely will be
necessary to determine the effectiveness of attempted safeguards. As merely one example,
certain assessments or reviews of employees may be considered libel or slander in certain
countries and could prompt attempts to gain information through the legal process.

Although the transfer of private information between jurisdictions likely will cause some uncertainty in
terms of conflicting laws, a company can and should consider a wide range of innovative options to meet
the privacy challenges facing an increasingly multinational workforce.

§ 4 PRACTICAL GUIDELINES FOR EMPLOYERS

§ 4.1 COMPLYING WITH THE HEALTH INSURANCE PORTABILITY AND
ACCOUNTABILITY ACT & THE AMERICANS WITH DISABILITIES ACT

Described below are best practices under the HIPAA Privacy Rule for using, disclosing and obtaining the
protected health information (PHI) of employees and job applicants other than in the context of
administering an employee welfare benefit plan.

§ 4.1(a) Obtaining the Results of Work-Related Physical Examinations

- Determine whether the health care provider who will conduct the examination or perform the
test is a “covered” health care provider. If not, the HIPAA Privacy Rule imposes no special
requirements on the release of the examination or test results. Entities in the business of
providing drug and/or alcohol testing generally are not covered entities under HIPAA.

- If the examiner is covered under the HIPAA Privacy Rule, then obtain the employee’s
authorization for release of the examination or test results. Determine whether the examiner
will require use of its own form or will accept an authorization that you have prepared.

- If the examiner requires use of its own form, check that the form’s description of the
information to be disclosed and the specified purpose of the disclosure are accurate.

- If the examiner requires the employer to prepare the authorization, ensure that the form
contains the elements listed in the section discussing the HIPAA Privacy Rule. The form also
should contain the “safe harbor” language required by GINA. Consult with legal counsel to

---

308 For a discussion on how choice of laws issues in contracts are being handled in China, see Mo Zhang, Choice of
Economic Contract Law, Article 5 (permitting choice of law specification in a contract to settle the an issue in the
contract)); see also, e.g., Black Sea Steamship UL Lastochkina Odessa, USSR v. Union of India (AIR 1976 AP 103)
(finding it “perfectly open to the court to consider the balance of convenience, and interests of justice and like
circumstances when it decides the question of jurisdiction of a court in the light of a clause in the agreement
between parties choosing one of several courts or forums which were available to them”); INDIA CIV. PROC. CODE
§ 13 (foreign judgments are conclusive absent certain exceptions), 15 & 44A (decrees from reciprocating territories
are enforceable).

15, 2008.

310 Under GINA, employers that request medical information from an employee should warn the employee and
©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
ensure that state law does not impose additional or more restrictive requirements on an authorization to release health information. Incorporate any more stringent state law or additional requirements into the authorization.

- Limit the use of the examination results to the purposes identified in the authorization.

§ 4.1(b) **Disclosing PHI to Third-Party Service Providers/Business Associates**

- Determine whether your business administers a covered health plan. If your business does not, then you will not need to comply with the HIPAA Privacy Rule and you will not need to enter into any business associate contracts. However, depending on the nature of the master service agreement, it may be prudent to enter into an addendum covering information security issues.

- If your business does administer a covered health plan, identify all third parties who provide services to the health plan—including, but not limited to, third-party administrators, pharmacy benefits managers, insurance brokers, attorneys, accountants, consultants and claims processors.

- Identify each third-party service provider who creates, receives or maintains PHI for purposes of providing services to the plan or to whom the plan discloses PHI for that purpose.

- Negotiate a written agreement (known as a business associate contract) with the assistance of counsel, containing the provisions described in the section discussing the HIPAA Privacy Rule.

- Implement policies and procedures to ensure that your business will take appropriate actions when, and if, it learns that the business associate has breached the business associate contract.

§ 4.1(c) **Responding to Subpoenas & Civil Discovery Requests Seeking Employee Health Information**

- Determine whether information responsive to the subpoena or civil discovery request is PHI, *i.e.*, information created or received by a covered health plan, by a business associate of a covered health plan, or by an on-site medical provider that engages in standard electronic transactions. Responsive documents that are not PHI, such as employee personnel files, are not subject to the HIPAA Privacy Rule.

- If the party making the request is, or is acting on behalf of, the subject of the PHI, then the information should be produced in accordance with the request. Verify the identity of the person making the request before disclosing any information or documents about the subject of the request.

- If the party making the request is not the subject of the PHI, and is not acting on the subject’s behalf, then the employer should request written documentation that either:


relevant healthcare provider(s) not to provide “genetic information” in response to the employers’ requests. If an employer provides sufficient warning, its receipt of genetic information in response to the request will be deemed inadvertent and, therefore, not a violation of GINA. See 29 C.F.R. § 1635.8(b)(1)(i)(B) for a sample of the “safe harbor” language.

©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
1. the requesting party has notified the subject of the PHI of the request, the subject has had the opportunity to object and no objection was made, or the court overruled the objection in whole or in part; or

2. the requesting party has moved for the entry of a protective order, or a protective order has been entered, limiting the use of the subject’s PHI to the litigation in which the request is made and requiring the requesting party to return or destroy the PHI at the close of the litigation.

- Produce only information that is responsive to the subpoena or civil discovery request and make the production only in accordance with the dictates of the subpoena or civil discovery request. Do not produce any “genetic information” as defined by GINA. Genetic information may be produced to a third party only in response to a court order specifically mandating the production.

§ 4.1(d) **Complying with the ADA’s Confidentiality Requirements**

- Identify all health information that your business collects and stores concerning job applicants and employees, as a result of mandatory, job-related medical examinations, as part of the ADA’s process for determining a reasonable accommodation, in connection with a direct threat analysis or as part of some other process that requires employees to disclose medical information, such as for leave administration purposes.

- Separate the identified health information from the general employee personnel file.

- Put in place administrative, technical and physical safeguards, such as placing paper files under lock and key and imposing restrictions on access to electronic files, to protect the confidentiality of this information.

- Limit the disclosure of information in these confidential files to the following circumstances:
  1. when supervisors and managers need to be informed regarding necessary restrictions on work or duties of the employee and necessary accommodations;
  2. when first aid and safety personnel need to be informed about a disability that might require emergency treatment; and
  3. when government officials investigating compliance with the ADA request access to such records or information.

§ 4.2 **COMPLYING WITH THE GENETIC INFORMATION NONDISCLOSURE ACT**

Practical steps employers can take to maintain compliance with GINA include the following:

- Post an EEO nondiscrimination poster prohibiting discrimination based on genetic information.

- Include nondiscrimination on the basis of genetic information in equal employment opportunity statements.

- Do not request family medical history from applicants and employees, except in limited circumstances in connection with a wellness program.

©2017 LITTLE MENDELSON, P.C. ALL RIGHTS RESERVED.
• If an employer requires post-offer, preemployment medical examinations, the medical examinations may not include any inquiries about family medical history. Although these types of questions are common at routine doctor visits, physicians performing preemployment medical exams should avoid these questions, and employers should consider taking steps to review and revise any potentially outdated questionnaires that may still contain questions relating to family medical history.

Any requests that an employee have a medical professional provide documentation (e.g., in connection with a fitness-for-duty exam, or a request for reasonable accommodation or leave unrelated to FMLA leave) must include a statement that family medical history and other genetic information should not be provided.

• Regularly review and evaluate processes regarding the administration of health benefits to make sure they are compliant.

• Provide confidentiality protections for any personnel records that contain medical information about an employee or employee’s family member (e.g., FMLA certifications seeking leave for the serious illness of a family member) that falls within the broad definition of “genetic information.”

• Verify that there are policies and procedures in place to prevent the inadvertent disclosure of genetic information in response to a subpoena or civil discovery request unaccompanied by a court order compelling disclosure.

• Employers should train human resources personnel and managers on the requirements of GINA and any applicable state or local laws pertaining to genetic information.

§ 4.3 PROVIDING ACCESS TO PERSONNEL RECORDS

• Become familiar with applicable state and federal statutes governing access to personnel records.

• Be aware that most state statutes governing access to personnel records cover such topics as time and place of access, right to make copies, right to correct information, right to protest or seek removal of information and right to insert explanations.

• Implement a procedure (and appoint a contact person where practicable) to ensure consistency and compliance with applicable law when releasing or denying access to personnel information.

• Document the release of any personnel information.

§ 4.4 SAFEGUARDING EMPLOYEE PERSONNEL DATA FROM THEFT

With the latest and greatest technological advancement comes the risk for potential security breaches. Such security breaches can result in damaging publicity, significant out-of-pocket expenses and undercut employee and customer loyalty. Employers should consider the six-pronged approach outlined below protecting the organization’s personnel information from unauthorized access and to mitigate damage to employees when a security breach does occur.

1. Establish a Data Protection/Privacy Policy. The data protection/privacy policy should embody all aspects of the employer’s efforts to reduce the risk of unauthorized access to personnel data. The policy should accomplish at least the following:
• Identify the circumstances in which sensitive data may be collected from job applicants and employees, the types of data to be collected and how the employer may use and disclose the data.

• Strictly limit the collection, use and disclosure of sensitive data to the minimum necessary for the intended purpose.

• Eliminate all unnecessary collection, uses and disclosures of personal information.

• Detail how the employer will safeguard sensitive personal data.

• Explain how employees can identify and report possible security breaches.

• Establish procedures for responding to security breaches. This should include building an incident response team, to include information technology (IT) personnel, human resources professionals, business unit leaders, in-house or outside counsel and public relations specialists. Team members should be assigned specific roles and responsibilities in responding to a security incident.

• Sanction employees who violate the data protection policy.

• Describe how the employer will mitigate potential damages to affected individuals when a security breach does occur.

2. **Control Access to Sensitive Data.** Access to sensitive employee data should be restricted, controlled and monitored. One approach to these tasks entails the following steps:

• Identify the categories of employees who may access sensitive data.

• Identify the categories of sensitive data that may be used and disclosed by each employee granted access.

• Restrict access to the most sensitive data to employees with a track record for trustworthiness or who have been subjected to a background check.

• Periodically review access rights and revise access lists as may be necessary to reflect any change in employers’ job responsibilities.

• Upon terminating an employee with authorized access to sensitive data, promptly change all passwords and security codes available to the terminated employee and require the immediate return of computer disks, compacts disks, keys, laptop computer and other mobile devices; after terminating an employee with authorized access to sensitive data, strip the employee’s computer of sensitive data before reissuing the computer to another employee.

• Bar temporary, outsourced and vendor employees from sensitive data except when absolutely necessary. When access is necessary, the employer should conduct a background check or ensure that the temp agency, outsourcer or vendor has done so. The employer also should monitor these employees’ use and disclosure of sensitive data to the maximum extent feasible. Consider obtaining confidentiality agreements from the employees of vendors.
Before sharing sensitive data with an outsourcer, conduct due diligence concerning the outsourcer’s “bona fides,” including its security policies and procedures. In addition, negotiate a written agreement with the outsourcer that addresses the following terms:

- the outsourcer’s permitted uses and disclosures of the information;
- the administrative, physical and technical safeguards the outsourcer must implement;
- prompt notice to the employer in the event of a security breach;
- the outsourcer’s obligation to assist in mitigating damages;
- indemnification to the employer for any damages caused by the outsourcer’s security breach;
- the employer’s right to audit the third party’s security controls;
- restrictions on the outsourcer’s use of subcontractor’s or agents and/or a requirement that the outsourcer obtain the written agreement of any outsourcer or agent to provide similar safeguards;
- choice of law and choice of forum;
- amendment of the agreement in the event of any change in controlling law; and
- any other matter that must be addressed in the agreement for legal compliance purposes.

3. **Technical and Physical Safeguards.** The employer’s information technology department should put in place an array of security measures for electronic data, including the following:

- assignment of a unique identifier to each network user to permit monitoring of user activity;
- password protection and, where appropriate, encryption for all files containing sensitive data;
- use of complex passwords (with at least eight characters, at least one capitalized letter and at least one number) that are changed regularly;
- installation and regular updating of firewalls and antivirus software;
- prompt implementation of patches for security holes;
- lockdown of workstations capable of accessing sensitive data during periods of inactivity;
- logging access to files containing sensitive data and monitoring any outward transfer or duplication of those files;
- use of hardware and software to record and examine activity on information systems;
- prohibiting the downloading of sensitive data to laptops, mobile devices and portable storage media except when necessary to perform job responsibilities and when feasible if the downloaded information will be encrypted; and
• destruction of electronic files in a manner that ensures that they cannot be retrieved.

Implementing the following procedures for securing sensitive data in paper format remains essential as well:

• paper documents containing sensitive data should be stored only in areas with employees authorized to access those documents;

• employees with access should lock all file drawers, cabinets and offices containing sensitive paper records when unattended;

• computer printers, scanners and fax machines for employees who use and disclose sensitive data as part of their job functions should be maintained in a controlled area;

• the memory dial program on the secure fax machine should be regularly monitored for outdated and incorrect numbers; and

• sensitive data in paper form should be shredded either internally or by a bonded company.

4. Training. Like any workplace policy, a data protection/privacy policy has value only if employees understand it and abide by it. Consequently, central to the policy’s success will be a program to train employees—especially those with access to sensitive data—to reduce security risks and vulnerabilities, to detect possible security breaches and to respond to a suspected security breach. The training should encompass at least the following:

• “password etiquette,” i.e., selecting unpredictable passwords and avoiding disclosure of passwords to coworkers and outsiders;

• teaching employees proper procedures for storing, printing, transmitting and destroying documents containing sensitive data; and

• training employees to recognize and report a suspected security breach.

5. Responding to a Security Breach. If the employer has established an incident response team, the team should be prepared to investigate, mitigate and remediate the breach immediately. The team will also need to address potential employee, customer and/or media relations issues and oversee compliance with all applicable data breach notification requirements.

6. Notice of Security Breach. All states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands have implemented security breach notification laws. (See discussion at § 2.2(c)(iii).) Even when not legally required to provide notice, employers evaluate whether doing so is appropriate from an employee relations perspective. Prompt notice provides employees with an opportunity to protect themselves before identity thieves have the opportunity to misuse the personal data stolen from an employer. In addition, employees who act promptly most likely will spend less time (including time at work) trying to restore their credit. Providing prompt notice as well as additional assistance also is a way for employers to demonstrate concern for employee welfare and generate employee loyalty.

While breach notification laws may impose additional requirements, some recommendations concerning the content of such a notice include the following:
• Briefly describe the circumstances that caused the security breach, including the date that the breach was discovered.

• Specify the categories of employee personal information (i.e., Social Security number, account numbers, health information, etc.) that were, or might have been, subject to unauthorized access.

• Describe the steps taken to mitigate the security breach and the steps that will be taken to prevent a recurrence.

• Describe any offer of identity protection services, such as credit monitoring or fraud resolution services.

• Encourage employees to act promptly to protect their identity by closing potentially affected accounts and warning creditors of potentially fraudulent activity.

• Advise employees to consider exercising their rights under federal law for potential victims and victims of identity theft, including the right to place a fraud alert and an extended fraud alert with the nationwide credit bureaus, the right to block consumer reporting agencies from reporting information that results from fraud, and the right to obtain from businesses information concerning accounts or transactions resulting from fraud.

• Suggest that the employee visit the FTC’s website to obtain additional resources for victims of identity theft, such as the FTC’s publication, “When bad things happen to your good name.”

• Provide employees with information for obtaining a free annual credit report from each of the three national credit bureaus, and encourage them to monitor their credit reports.

• Several states mandate specific additional content in a security breach notification. Consult with counsel regarding these requirements.

• When notice to employees is legally required, the employer also may be required to notify government agencies, the national credit bureaus, and/or the media. Employers should consult counsel to determine whether such notices are required.

Employers should maintain a copy of each notice mailed to employees, or of a template notice, and a mailing list in the event the employee ever files a lawsuit alleging that the employer is responsible for losses from the identity theft. Employers should also maintain documents evidencing a decision not to provide notice to potentially affected individuals.

§ 4.5 THIRD-PARTY INQUIRIES

• Establish procedures for responding to third-party inquiries, and, if possible, require that all inquiries be directed to the human resources department or a specified contact person.

• Specifically prohibit (in writing) employees, including the supervisor of any employee at issue, from responding to inquiries for personnel information.

• Require that all inquiries be in writing. Agree to provide only information regarding dates of employment and classification without the employee’s consent.
• Consult legal counsel before complying with any third-party request for personnel information in cases potentially involving tort or employment liability.

• Never give a troublesome or violence-prone former employee a misleadingly good reference.

• Require employees who leave the organization to sign a release allowing the organization to discuss with prospective employers the employee’s job performance and reasons for leaving.

• When calling another employer for information on a job applicant, ask nondiscriminatory questions and ask for verifiable, documented facts. Document any responses, including a refusal to provide any information.

• Verify that e-mails requesting employee personnel data are from the sender by checking the sender’s email address.

The last suggestion stems from the potential for “spoofing” schemes. In April 2016, the Federal Bureau of Investigation (FBI) issued a warning that e-mail “spoofing” schemes had dramatically risen, resulting in law enforcement receiving complaints from victims in every U.S. state.³¹¹ These e-mail spoofing schemes involve third parties generating what appear to be company e-mails, which are then sent to individuals within a company requesting a wire transfer of money or documents containing sensitive employee personnel information, such as employee Form W-2s or Social Security numbers. The FBI has also reported that similar fraudulent scams are perpetrated via telephone, in which a third party contacts a business and requests payment or confidential information.³¹²

§ 4.6 TRANSBORDER DATA TRANSFERS
The European Union is undergoing a major reform of its data privacy laws following the invalidation of the Safe Harbor Framework and the passage of the General Data Protection Regulation (GDPR). New guidance from E.U. data protection authorities is being issued as the data privacy law in Europe continues to evolve. Multinational employers should continue to monitor these developments and watch for additional guidance. Additional recommendations include:

• U.S.-based multinational employers should monitor the status of the Privacy Shield and consider implementing alternative methods for lawfully transferring the personal data of E.U. employees to the United States.

• U.S. multinationals should take advantage of the two-year grace period to come into compliance with the GDPR. To comply with the GDPR, virtually all U.S.-based multinational employers likely will need to update at least some of their existing policies and procedures, and re-align some of their practices, for handling the personal data of employees of their E.U. subsidiaries.

• The invalidation of the Safe Harbor framework has had a domino effect in other jurisdictions that had similar agreements with the United States. U.S. multinational employers should review the jurisdictions in which they operate to confirm that no other transborder data transfers were affected by the invalidation of the Safe Harbor framework.


©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
§ 4.6(a) Implementing a Privacy Shield Compliance Program for Transfers of HR Data

Satisfying the formal requirements for self-certification under the new Privacy Shield will be relatively straightforward, but achieving meaningful compliance that mitigates enforcement risk will be far more complicated, and enforcement risk, particularly for transfers of HR data, has increased materially. To begin with, virtually all enforcement will take place in the European Union, not the United States. Second, E.U. DPAs, particularly in countries like France, Germany and Spain, appear to be primed to flex their enforcement muscle. Third, while E.U. employees may not grasp all the nuances of the debate over the Safe Harbor, they and their works council or trade union have become generally leery of large-scale transfers of HR data to the United States. As a result, they may initiate complaints, especially if they sense that the U.S. parent corporation is not taking data protection seriously.

To demonstrate its commitment to compliance to its E.U. employees (and their representatives) and, if needed, to regulators, the U.S. parent corporation should consider taking the following steps:

1. **Confirm that E.U. subsidiaries comply with local requirements for cross-border data transfers to the United States.** The Privacy Shield framework document emphasizes that the “Privacy Shield Principles are relevant only when [HR data is] transferred or accessed” and that collection and processing of HR data “prior to transfer will have been subject to the national laws of the EU country where it was collected, and any conditions for or restrictions on its transfer according to those laws will have to be respected.”313 As a practical matter, this requirement to comply with local laws means that E.U. subsidiaries must take the following steps before transferring their employees’ personal data to the United States pursuant to the Privacy Shield: (1) provide their employees with notice of data processing, including transfer to the United States; (2) consider local law restrictions on cross-border data transfers, particularly on transfers of sensitive personal data, such as employees’ health information; (3) confer with works councils or trade unions, if any and if legally required, concerning data transfers to the United States; and (4) depending on the country, register with or notify the local DPA of data processing, including cross-border data transfers.

   In a world where technology permits a small or medium-sized U.S. business to be a multinational employer, many E.U. subsidiaries of organizations that will certify to the Privacy Shield are only small sales offices or factories with no locally-assigned HR professional or legal counsel. As a result, these subsidiaries likely will address compliance with local data protection laws for the first time when the U.S. parent corporation decides to transfer E.U. employees’ personal data to the United States.

2. **Establish policies and procedures to implement the privacy shield privacy principles.** While the HR privacy policy submitted to the Commerce Department will contain the high-level principles that should guide the handling of E.U. employees’ personal data transferred to the United States, that policy typically will not instruct U.S.-based HR professionals, payroll personnel, managers and others on exactly what it is they need to be doing to achieve compliance. For example, the Privacy Shield framework document requires certifying organizations to satisfy the Security Principle by “tak[ing] reasonable and appropriate measures to protect [transferred personal data] from loss, misuse and unauthorized access, disclosure, alteration and destruction.”314 However, that document identifies no specific measures to be taken. Because there is a similar lack of detail for most of the other Principles, certifying organizations will need to develop detailed policies and procedures to implement the Principles. Some of those policies and procedures include:

314 Principles, § II.4.a.
a. **Notice & Choice Principles:** U.S.-multinational employers typically will transfer E.U. employees’ personal data to the United States to store it in a centralized HR information system (“HRIS”) that facilitates global workforce management. Given this purpose, the HR privacy policy likely will inform the E.U. workforce only about the use and disclosure of their personal data for HR administration purposes. If the U.S. parent subsequently were to use transferred personal data for other purposes, such as to market the company’s products to the E.U. workforce or to support a global charitable campaign, it would be required to give E.U. employees the opportunity to opt out from the previously undisclosed use. According to the Privacy Shield framework document, such “choices must not be used to restrict employment opportunities or take any punitive action against such employee.” In other words, E.U. employees cannot be confronted with a choice between consenting to the new use or losing their job. As a benefit to employers, the Privacy Shield specifically excludes from the Notice and Choice Principles processing E.U. employees’ personal data for “promotions, appointments or other similar employment decisions.” This exclusion applies only “[t]o the extent and for the period necessary to avoid prejudicing” the decision-making process. This exclusion should help to avoid a situation where notice disrupts the employment decision-making process.

To handle transferred data in compliance with the Notice and Choice Principles, the certifying organization should consider implementing several policies and practices. By way of illustration, it should specifically identify the categories of employees authorized to access E.U. employees’ personal data; the categories of data that can be accessed; the permissible purposes for access, use and disclosure; and the steps to be taken before using such data for a purpose not previously disclosed in the HR privacy policy or otherwise.

b. **Accountability for Onward Transfer Principle:** Under the Accountability for Onward Transfer Principle, certifying organizations must require, by written agreement, that third parties who receive transferred personal data provide the same level of protection for that data as required by the Privacy Shield. The U.S. parent corporation must enter into these “onward transfer agreements” with both agents, such as HR service providers and non-agents that will use transferred personal data for their own purposes. Organizations that certified to the Privacy Shield within 60 days of its effective date (i.e., September 10, 2016) had 9 months from the date listed on the Privacy Shield List to bring contracts with third parties into conformance with this Principle.

The Privacy Shield establishes an important exception from the requirements described above for cross-border data transfers within a corporate group. The U.S. parent corporation can make such transfers without an “onward transfer agreement” provided that “other instruments, such as EU Binding Corporate Rules [BCRs] or other intra-group instruments (e.g., compliance and control programs), ensuring the continuity of protection of personal information under the Privacy Shield Principles” have been implemented. The italicized phrase gives U.S. parent corporations greater flexibility because it allows them to forego not only onward transfer agreements but also the potentially onerous process of implementing BCRs when those organizations need to share E.U. employees’ personal data with non-U.S. and non-E.U. affiliates, for example,
when an HR director for Europe, the Middle East and Africa ("EMEA") resides in the United Arab Emirates.

c. **Security Principle:** To satisfy this Principle, the U.S. organization will need to implement specific measures, such as access controls, restrictions on storage of E.U. personal data on portable storage media, safeguards for paper records containing E.U. personal data, and secure methods of document disposal. The organization may be able to leverage for this purpose policies and practices used to safeguard other types of sensitive employee data, such as Social Security numbers and protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA).

d. **Access Principle:** Under the Access Principle, individuals have the right to access their personal data, to correct personal data that is inaccurate and to delete personal data that the U.S. organization processes in violation of the Principles. However, the detailed procedures established by the Privacy Shield framework for implementing these rights have limited applicability to HR data transferred in the context of the employment relationship. The Privacy Shield dictates that “employers in the European Union must comply with local regulations and ensure that European Union employees have access to such information as is required by law in their home countries, regardless of the location of data processing and storage.” The Privacy Shield also mandates, in light of E.U. employees’ rights under local law, that the U.S. parent corporation “cooperate in providing such access either directly or through the EU employer.” Consequently, certifying organizations will need to implement policies and procedures to facilitate a coordinated response to requests by E.U. employees to exercise their rights to access, amend and delete their personal data.

3. **Establish an annual verification process.** The Privacy Shield requires that certifying organizations recertify annually, and that before recertification, they verify on-going compliance with the Principles. The verification can be conducted as a self-assessment or by an outside entity. In either case, the certifying organization must verify that the attestations in its self-certification and assertions in its HR privacy policy are true and that “privacy practices have been implemented as represented and in accordance with the Privacy Shield Principles.” To meet those standards, organizations that choose to conduct a self-assessment must verify that:

a. the HR privacy policy is “accurate, comprehensive, prominently displayed, completely implemented and accessible;”

b. the HR “privacy policy conforms to the Privacy Shield Principles;”

c. individuals are informed how to submit complaints, both internally and to the relevant E.U. data protection authority;

d. employees with access to transferred personal data have received training and will be disciplined for policy violations; and

e. the organization conducts periodic compliance reviews.

The verification must be signed by an authorized corporate representative and must be produced upon request to employees, or in the context of an investigation or complaint proceeding.

---

318 Supplemental Principles, § III.9.c.i (emphasis added).
319 Supplemental Principles, § III.9.c.i (emphasis added).
320 Supplemental Principles, § III.7.a.
321 Supplemental Principles, § III.7.c.

©2017 LITTLER MENDELSON, P.C. ALL RIGHTS RESERVED.
4. **Be prepared to resolve complaints in the European Union.** U.S. organizations that certify to the Privacy Shield to transfer HR data are required to agree to cooperate with investigations by, and abide by the advice of, E.U. data protection authorities. Notwithstanding this certification by the U.S. parent corporation, the Privacy Shield framework document emphasizes that even after HR data is transferred, “primary responsibility for that data vis-à-vis the employee remains with the organization in the EU.”322 Consequently, the framework document provides that E.U. employees who are not satisfied with the internal resolution of their data protection complaints “should be directed to the state or national data protection or labor authority in the jurisdiction where the employees work” even if the U.S. parent corporation is responsible for the alleged violation.323

To fulfill its representation in the self-certification form, the U.S. parent corporation would be required to participate in the complaint proceeding in the European Union with its E.U. subsidiary. Significantly, this proceeding will be governed by the relevant E.U. Member State’s law and not by the Principles or U.S. law. In addition, the U.S. parent corporation will be required to abide by the advice of the DPA, which could include an order to implement remedial measures and/or to compensate the employee.

---

322 Supplemental Principles, § III.9.d.i.
323 Supplemental Principles, § III.9.d.i.