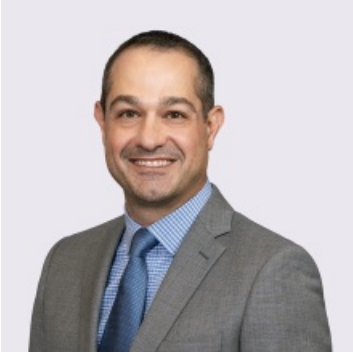
Legal Update Article

Importance of Protecting Employee Information as Privacy and Cybersecurity Laws Proliferate

By Jason C. Gavejian & Joseph J. Lazzarotti

October 2, 2023

Meet the Authors



Jason C. Gavejian
Office Managing Principal
908-795-5139
Jason.Gavejian@jacksonlewis.com

Joseph J. Lazzarotti
Principal
908-795-5205
Joseph.Lazzarotti@jacksonlewis.com

Related Services

Privacy, Data and Cybersecurity

Most human resources professionals are concerned about the privacy and security of the vast amounts of personal information they manage. This article discusses steps to consider taking against the challenges.

Deluge of Data

Challenges HR professionals face to protect the data they manage include:

- The amount of personal information includes not just current employees. It also includes former employees, temporary employees, contractors, and applicants. These numbers can increase quickly with acquisitions, higher levels of turnover, and other workplace changes. Further, added to that amount is the personal information of families and other individuals, such as guardians or beneficiaries.

- That breadth of information is continually increasing. Consider the impact various channels of electronic communication, devices, and applications have had on the generation of confidential and personal information. For the HR professional, the ubiquity of these new technologies has resulted in the collection of more and more data, vastly increasing the data footprint of organizations.

- At the same time, record retention and destruction programs intended to contain the amount of personal information can be difficult to develop and maintain, allowing that footprint to grow virtually uninterrupted.

- This information frequently is some of the most sensitive information about an individual: Social security numbers, bank account numbers, retirement account information, physical and mental health information, genetic information, biometric information, and so on.

- HR departments often have to rely on other departments, the IT department in particular, for the tools or budgets to meet applicable data privacy and security obligations. They also have to rely on third-party service providers that provide a wide range of HR support services, such as payroll, employee benefits, and leave management processing and storing sensitive personal information.

- The growing regulatory burden.

State of the Law for Employee Data

For good reason, many of the statutes or regulations on employee personal information seek to address a concern for cyberattacks. In the third quarter of 2022 alone, there were at least 15 million records exposed throughout the world due to data breaches, a 37 percent increase from the same quarter in 2020 — and this is just from reported

breaches. Additionally, there is an array of existing laws intended to ensure confidentiality and nondiscrimination in the workplace. That is, some of these laws seek to ensure confidentiality and nondiscrimination for employees by limiting the persons who may have access to certain information.

Following are examples of statutes and regulations covering both categories, privacy and security:

- *Health Insurance Portability and Accountability Act (HIPAA):*HIPAA includes comprehensive privacy and security regulations that apply to health plans and health care providers. HR professionals are likely most familiar with these requirements as they relate to the group health plans sponsored by the company, in particular, self-funded group health plans and health flexible spending arrangements. Compliance includes comprehensive policies and procedures, training, and other measures. HR professionals in the healthcare industry potentially have added layers of responsibility, including ensuring employees are training to comply with HIPAA and involvement in complaints regarding misuse of protected health information.

- *Americans With Disabilities Act (ADA):*In the normal course of HR administration, a company is likely to access or acquire information concerning an employee's disability or other medical information. The ADA requires certain protections for medical information obtained from employees in connection with medical examinations and inquiries, leave of absence administration, and processing reasonable accommodations. This includes limiting access to supervisors and managers and third parties.

- *Genetic Information Nondiscrimination Act (GINA):*Under GINA, genetic information of an employee (or applicant) includes information about the manifestation of disease in that employee's (or applicant's) family members, including the employee's (or applicant's) spouse. Except in limited situations, GINA prohibits the collection of that information by employers (and their agents), as well as the use of that information to discriminate. The ubiquity of social media communications and expansive monitoring devices and applications make collection of genetic more common that one might think. In addition, such information is subject to essentially the same confidentiality and reasonable safeguard requirements as medical information under the ADA.

- *The California Consumer Privacy Act (CCPA):*caught many employers' attention when, at the end of 2022, the exemption for employee information expired. This meant that employers needed to, among other things, update their notices to employees and applicants, expand their website privacy policies, and implement reasonable safeguards to protect employee and applicant information. However, California is not an outlier regarding requirements to secure the personal information of employees. New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) requires businesses to implement safeguards for the "private information" of New York residents, including employee information such as social security numbers.

- *State Protections for Social Security Numbers:* Several states (including Virginia) have passed laws on the protection of employee's social security numbers. Some states limit the collection of employee's social security numbers, others require limiting access to employee's social security numbers. Awareness of the state law protections is important as nearly all employers collect this information for employment purposes.

- *Breach Notification Laws:* All 50 states, as well as certain cities such as New York City and Washington, D.C., require a business to provide notice when there has been a "breach" of "personal information" owned by the business. HR professionals should be keyed into not only safeguarding personal information but also the response should a breach occur. Often there are distinct issues to be addressed for employees, including shaping communications about the incident appropriately.

- *Vendor Contract Mandates:* HR departments typically rely on third party service providers to support many HR functions – payroll, benefit plan enrollment, recruiting, retirement plan administration, and so on. A number of states require organizations that share personal information (includes social security number and other data) with third party service providers obtain from those providers written assurances that they will safeguard that personal information. Some of these states include California, Maryland, Massachusetts, New York, and Oregon.

- *Data Destruction Requirements:* Over 30 states have enacted data destruction laws (Delaware being one of the most recent states enacting such a law) that require businesses to destroy records containing certain personal information by shredding, erasing, or using any other means to render the information unreadable or undecipherable. Connecticut, Florida, Maryland, Massachusetts, New York, and South Carolina are among the 30 states with data disposal requirements.

The courts have ruled on employee protections. Most recently, a federal appeals court overturned dismissal of a class action against a company that suffered a ransomware attack that compromised current and former employee's social security numbers. The court found that traditional negligence covered the employees' claims. As far back as 2018, a state court held employers that collect personal information from employees have a common law duty to use reasonable security measures.

Where Can Employers Start?

A good place to start is with the Federal Trade Commission's guide for businesses. It recommends the following steps:

- Know the personal information being collected;
- Scale down the information being collected;
- Protect the information that needs to be collected;
- Ensure proper disposal of information not needed; and
- Create a plan for when security incidents occur.

Checklist for Employers

While cybersecurity may be complicated, the checklist for compliance is not. Following is a high-level checklist for employers:

1. Perform a risk assessment.
2. Ensure leadership and management understand the importance of a compliance plan.
3. Develop policies and procedures for the collection, retention, and protection of data.
4. Train employees on good cybersecurity practices.
5. Obtain cybersecurity insurance.
6. Vet and audit vendors to ensure employee data is not put at risk by their practices.
7. Continually audit and review practices as technology and the company changes.

Please contact a Jackson Lewis attorney with any questions.