Webinar 11 – November 2026

Privacy and Data Security in the Workplace in 2026 and Beyond

WEBINAR OUTLINE

INTRO/SETTING THE STAGE

- Types of Employee Data Collected in the Workplace
- What Types of Data are Employers Required to Protect?

NEW YORK ELECTRONIC MONITORING LAW (Civil Rights Law § 52-c)

NEW YORK SOCIAL MEDIA PRIVACY LAW (LABOR LAW § 201-I)

THE NEW YORK SHIELD ACT

NEW YORK PERSONNEL FILE ACCESS LAW

HRtelligence TIPS

INTRO/SETTING THE STAGE

The modern workplace privacy and data security environment balances an employer's right to monitor productivity and protect assets with employees' expectations of privacy and legal compliance mandates.

Employers must balance the employer's right to protect company assets, monitor productivity, and ensure security with the employee's reasonable expectation of privacy.

Types of Employee Data Collected in the Workplace

Personal Information and Identification Data
Strict recordkeeping requirements mandate that employers maintain detailed records, including each employee's full name and Social Security Number. Employers may also ask for details such as addresses or birthdates. This information allows organizations to verify eligibility for employment while promoting accurate tax reporting.

Performance and Payroll Records
Employers maintain detailed records capturing attendance (such as hours worked or leave), along with information tied to compensation or performance. Records may detail ratings or feedback granted during performance evaluations, along with insight into promotions or changes in job responsibilities.

What Types of Employee Data are Employers Required to Protect?

Health Insurance Portability and Accountability Act (HIPAA)
HIPAA primarily protects sensitive health information managed by healthcare providers and health plans. For employers, HIPAA applies if they sponsor health plans or wellness programs that collect employee medical data. It mandates strict privacy and security controls to protect employees' health records from unauthorized access or disclosure.

Fair Credit Reporting Act (FCRA)
The FCRA regulates how employers use consumer reports, such as credit checks and background screenings, in employment decisions. Employers must obtain written consent before conducting these checks and provide clear disclosure of the report's use. If adverse action (e.g., not hiring) is taken based on a report, employers are required to notify the employee and provide a copy of the report. FCRA promotes transparency and fairness, helping protect employees from inaccurate or improper use of their credit and background information.

Americans with Disabilities Act (ADA)
The ADA protects employees with disabilities by restricting how employers collect, store, and use medical information related to disabilities. Employers must keep all disability-

related medical records confidential and separate from general personnel files. Medical inquiries and examinations must be job-related and consistent with business necessity. The ADA ensures that sensitive employee health information is handled with strict confidentiality, safeguarding employee privacy and preventing discrimination.

NEW YORK ELECTRONIC MONITORING LAW (Civil Rights Law § 52-c)

Enacted and effective for private-sector employers with a place of business in New York (covering both in-person and remote staff):

- **Mandatory Prior Notice:** You must provide **written or electronic notice** to new hires *upon hiring* informing them that their telephone conversations, emails, and internet access/usage may be monitored at any and all times by any lawful means.
- **Employee Acknowledgment:** You must obtain a **written or electronic acknowledgment** from each new hire confirming receipt of the notice. If an employee refuses to sign, the notice requirement is not legally met.
- **Physical & Digital Posting:** You must post a conspicuous notice of the monitoring practices in a place readily available for viewing by subject employees (such as a physical breakroom board or a company intranet/portal).
- **Exemptions:** Routine system maintenance, spam filtering, or volume-management processes that do not target a specific individual's communications are exempt.
- **Penalties:** Enforced exclusively by the New York State Attorney General with zero private right of action for employees, carrying fines of **$500** for a first offense, **$1,000** for a second offense, and **$3,000** for third and subsequent offenses.

NEW YORK SOCIAL MEDIA PRIVACY LAW (LABOR LAW § 201-I)

Under New York State Labor Law (Section 201-i) employers cannot ask or require employees, or potential employees, to provide their personal social media account password, username and password, or access to their personal social media account in any way.

The law applies to all personal accounts or profiles that are accessible on a computer, phone, tablet or other device where users can create, share, or view user created content such as videos, photographs, blogs, podcasts, instant messages, profiles, or locations for personal purposes.

The law does not apply to employer-provided accounts or devices that are used for business purposes, as long as the employer told the employees in advance of their plan to access such accounts/devices.

THE NEW YORK SHIELD ACT

The Stop Hacks and Improve Electronic Data Security Act applies to *any* employer storing "private information" of New York residents, which explicitly includes employee Social Security numbers, driver's licenses, financial account numbers, biometric data, and work email/password credentials:

- **Reasonable Safeguards Requirement:** You must build, implement, and maintain a data security program featuring:
    - **Administrative Safeguards:** Designating an internal security coordinator, training employees on security procedures, performing risk assessments, and contractually binding third-party vendors.
    - **Technical Safeguards:** Assessing risks in network/software design, securely transmitting and storing data, and monitoring/testing controls.
    - **Physical Safeguards:** Protecting physical filing systems, restricting unauthorized room/device access, and securely disposing of paper and digital employee records when no longer needed.
- **Mandatory Breach Notification:** If an unauthorized *access* or acquisition of private employee data occurs, you must notify affected New York residents and state authorities (the Attorney General, Department of State, State Police, and DFS) **within 30 days** of discovery.

NEW YORK PERSONNEL FILE ACCESS LAW

While once confidential, now New York State has passed legislation allowing current and former employees to access their personnel files. On November 8, 2026, the NY Personnel File Access Law was enacted.

<u>Employee Right to Inspect Files</u>
5-Day Turnaround: Upon a current or former employee's written request, employers must provide a complete copy of their personnel file within five business days at no charge.

Best Practice (Form Requirement): While the law does not mandate a specific statutory form, we strongly recommend implementing a standardized internal "Personnel Record Request Form" to ensure requests are handled consistently.

What is a "Complete Copy"? This broadly includes applications, resumes, compensation details, performance evaluations, written warnings, and termination notices. Secure electronic copies (e.g., PDF via email or portal) are fully sufficient. You may exclude legally distinct files (such as separate ADA/medical records) or records containing personal information about other individuals if disclosure would be an unwarranted invasion of privacy.

Annual Limits: Employers may limit access to two requests per calendar year.

Best Practice (Tracking): Employers should utilize an internal HR or payroll log to track the number of requests per employee per calendar year. Note that any file inspection triggered specifically by the employer adding new negative material does not count against this annual cap.

Mandatory 10-Day Notice for "Negative" Information

Notice Requirement: Employers must notify employees within 10 days of placing any negative information into their personnel file.

What Constitutes Notice? While not rigidly defined, delivering a copy of the document directly to the employee (via email or hand-delivery with a written acknowledgment of receipt) satisfies this requirement.

Scope: This applies to any information that may negatively affect an employee's qualifications for employment, promotion, transfer, additional compensation, or the possibility of disciplinary action.

Best Practice (Broad Interpretation): Because the statute does not tightly define what qualifies as "negative," we strongly recommend interpreting this standard broadly. Routine written performance counseling, disciplinary notices, and even informal written performance commentary should be handled with this 10-day notice rule in mind. Whenever discussing an employee's performance or any type of disciplinary action, it is critical to document those interactions and issue the required notice.

Employee Rebuttal and Dispute Rights

Rebuttal Process: If an employee disagrees with the contents of their file, they can submit a written statement or rebuttal explaining their position, which must become a permanent part of the record.

Best Practice (Rebuttal Windows): The law does not set a strict time limit for the employee to submit this statement. To maintain control over the process, it makes sense to include a designated "opportunity for rebuttal" section or standard form directly attached to disciplinary notices.

Enforcement and Penalties: The law allows employees to pursue legal or administrative processes to seek the removal of false information. This statute is enforced by the New York Attorney General, and violations carry civil penalties ranging from $500 to $2,500 per violation. Retaliating against an employee for exercising these rights also creates liability.

Record Retention Mandate

Employers are required to retain complete personnel records for *at least three years* following the termination of employment.

Best Practice (Clear Dating): Ensure the dates of all documents and the dates they were added to the file are clearly marked on the documents themselves to easily demonstrate compliance in the event of an audit.
"Personnel records" are broadly defined under the law and also extend to relevant documents managed through third-party payroll or HR software vendors.

Recommended Next Steps
To mitigate the risk of statutory penalties and compliance violations prior to November 8, we recommend taking the following steps:

- Update Employee Handbooks and Policies: Revise your internal personnel record policies to account for the tight 5-day disclosure window and 10-day negative notice requirement.
- Train Management and Supervisors: Educate managers on how performance documentation, emails, and informal notes may be scrutinized, and ensure they understand the workflow for flagging negative entries.

HRtelligence

T TRENDS I INSIGHTS P PRACTICAL GUIDANCE S STRATEGIES

Employers can protect workplace data and employee privacy by implementing clear technical, physical, and administrative safeguards.

- **Create a Written Information Security Program:** Document how employee and customer data is collected, handled, stored, and destroyed.
- **Define Acceptable Use:** Clearly outline what employees can and cannot do on company-issued devices and networks (e.g., banning unauthorized file-sharing services, personal email usage on work devices, or connecting unapproved personal drives).
- **Clear-Desk and Clear-Screen Policies:** Require employees to lock their computers whenever they step away and to secure physical documents (such as personnel files or client lists) in locked drawers at the end of the day.
- **Onboarding & Ongoing Training:** Train new hires on data privacy during orientation and conduct mandatory annual refresher courses for all staff.
- **Secure Remote Connections:** Require all remote employees to use a secure company Virtual Private Network (VPN) and prohibit working on unsecured public Wi-Fi without protection.
- **Mobile Device Management:** If employees use personal devices for work, install MDM software to separate personal and professional data, enable remote wiping capabilities in case of loss, and enforce automatic updates.
- **Data Minimization:** Only collect and retain employee and customer data that is strictly necessary for business operations or legal compliance.
- **Secure Destruction:** Implement strict protocols for disposing of physical records (shredding) and digital files (secure permanent deletion) once retention periods expire.
- **Update Policies for Personnel File Access Law:** Create clear internal processes for tracking and responding to employee requests with the five-business day deadline and set up procedures for notifying employees about negative information.