

# WORKPLACE PRIVACY CHECKLIST

---

Workplace privacy is a growing employer concern. While this list is not meant to be exhaustive, nor cover every regulation, it will help you to avoid the vast majority of claims filed in this area. *All tools* mentioned are on HR That Works.

## Hiring Process

- Make sure you don't ask questions that step on EEO, disability, or other privacy concerns in the interviewing process. See the *Questions to Avoid During an Interview Form*.
- Comply with the Fair Credit Reporting Act (FCRA) when requesting background checks. Employees must provide their consent to any information obtained through third party means. See the *FCRA Disclosure Form*
- Make sure you handle any information obtained from a background check properly. Whether it is criminal information, credit history, past employment verification, school verification, degree or certification verification, etc. If you fail to hire someone because of any information you obtain make sure there's a legitimate business reason for doing so. For example, a poor credit score may knock out a bank teller, but not a ditch digger.
- Do not make inquiries into an applicant's medical condition until after you make a conditional job offer. Any inquiries made should be relevant to an employee's essential job functions. See the *Conditional Job Offer and Medical Questionnaire*.
- Discuss workplace privacy rules around internal use, emails, social media, desks, lockers, etc. as part of employee orientation.

## Record Retention Policies

- Make sure to keep all personnel records and other private information in separate files, with secure access, limited to those who "need to know." For example, a manager should be able to get access to the personnel files of his employees, but not those of other managers.
- Separate out an employee's medical records from the rest of their personnel forms and keep it under separate lock and key. A manager should not have access to employees' medical records unless absolutely necessary.
- Employees should be given access to their medical records at all times. Remember that HIPAA and state Medical Confidentiality Acts govern the dissemination of medical information.
- Employees have access to their personnel forms on a limited basis. This access varies on a state-by-state basis. For example, in California employees are able to obtain a copy of those documents they have signed.
- Be clear about the disposal of documents including personnel records. Please watch the excellent *Webinar on Record Retention*. It is recommended that most employee records be saved for up to seven years. Medical related to exposure to toxic elements should be saved for thirty years.

- Be very clear about providing any information to third parties without employee, client, or customer consent, or without a subpoena. Even if consent is given, do not provide more information than necessary. For example, if a medical office is requesting information about an employee's lower back injury, they should not sloppily send the employer information about that employee's cancer treatment.

## **Surveillance**

- The general rule is that employees and others can be videoed in public areas without notice or consent. Private monitoring is discouraged unless there is a legitimate business reason and notices posted to all those who may be concerned.
- There are limitations on what is considered "public." For example, locker rooms are considered off-limits for video surveillance.
- As a general rule, employees have no expectation of privacy in using company equipment, internet, email systems, and so on. This is true even if an employee may have to use a password to access the system. Make sure your employees are notified that they have no expectation of privacy in company property, either through your employee handbook or other means. See the *Internet and Email Usage Policy*
- Employers have the right to, and should, monitor employee emails. Same for phone calls. Once again, do not do this monitoring without posting some form of notice to employees that you intend to do so. If, at any time, during communication you run into an employee's private communication, cut it off even if on your equipment.
- As a general rule, you have the right to use information found on the internet from sites such as MySpace and FaceBook unless the employee, clients, or other persons are making an effort to keep that information secure.
- Consider using a program such as Net Nanny or Cyber Surf to monitor employee online activity.
- Register your company and officers on Google Alerts so you can see who is talking about you.

## **Privacy Protocols**

- Create and publish a privacy statement in your handbook and website that discusses notice, choice, access, and security.
- Have a protocol for any cookies, emails, and other information collected on your website.
- Prepare a privacy policy—see the examples on HR That Works.
- Make sure someone is in charge of your privacy protocols, be clear what their level of authority is, and what resources they have available.
- Engage in employee training to help avoid privacy breaches.
- Have a plan in place in case there is a breach of privacy.

## Security Protocols

- Have measures in place to protect the security of social security numbers, bank accounts, credit cards, payroll information, benefits information, and other client and employee data.
- Have password protocols, proper safeguards, and regular backups. Be clear about how any information you have is used with third party partners, vendors, clients, and so on. Make sure any vendors or partners comply with your privacy protocols.

## Post Employment Process

- Employers are encouraged to restrict information provided about past employees to name, dates of employment and last position held. If you wish to give out additional information, have the former employee sign the *Reference Release*.
- Make sure the employees return all data sources including computers, lists, etc.; they may have collected during employment. Remind them that any information collected is confidential and property of the company.

## Miscellaneous Employee Actions

- Privacy claims can come about any time you're handling medical information. As a general rule, whether dealing with the ADA, FMLA, pregnancy leave acts, or other laws, limit the information you need to the scope of the leave request.
- Another area where privacy pops up is during investigations into wrongful conduct either by employees or third parties. The rule remains the same: limit information on a "need to know" basis. Because of the delicate and confidential nature of many investigations, it would be wise to have them done by a professional attorney or investigator.
- If you have company trade secrets or other competitive information, make sure you have protocols in place with your employees to protect it. Confidentiality agreements, non-competition agreements (where allowable), non-solicitation agreements, can all help protect private or confidential company information.
- Make sure third parties don't get you in trouble (independent contractors, temp employees, investigators, consultants, etc.).

Again, this was meant to be a general snapshot of what you can do to help prevent privacy intrusion and claims. For additional information please consider the following resources:

- Webinar on Privacy in the Workplace Webinar
- Privacy Rights Clearinghouse – [www.privacyrights.org](http://www.privacyrights.org)
- FTC's Business Site – [www.ftc.gov/bcp/edu/microsites/idtheft/business/index.html](http://www.ftc.gov/bcp/edu/microsites/idtheft/business/index.html)
- Better Business Bureau Security and Privacy Made Simpler – [www.bbb.org/securityandprivacy](http://www.bbb.org/securityandprivacy)
- Health Information Privacy (HIPAA) – [www.hhs.gov/ocr/privacy/index.html](http://www.hhs.gov/ocr/privacy/index.html)