Record-Keeping Policy: Safeguarding Social Security Numbers

6/18/2014

Practice Note

Identity theft occurs when a person fraudulently obtains and uses another person’s personal information, such as name, Social Security number (SSN) and credit card number, without the victim’s authorization, consent or knowledge. The Federal Trade Commission (http://www.ftc.gov/bcp/edu/microsites/idtheft) has estimated that as many as 9 million Americans have their identities stolen each year.

Employers maintain many records, including SSNs, which are of great value to those who would engage in identity theft. The role of HR in safeguarding the collection, maintenance, handling, sharing and destruction of personal information contained in personnel files is critical so that employees do not become the victims of identity theft and that employers are at minimal risk of liability for unauthorized access, breach or theft of personal and confidential information. See Managing Personnel Records: Practical, Legal and Security Issues (/TemplatesTools/Toolkits/pages/managingpersonnelrecords.aspx) and Safeguarding HR Information (/Publications/hrmagazine/EditorialContent/Pages/1105caterinicchia.aspx).

A number of federal and state laws and regulations govern employers’ use, maintenance, storage, access to and destruction of employee and applicant personal information. Most states have passed data privacy and security laws to protect employees’ personal information against unauthorized use and identity theft. In addition, a number of states limit business use and disclosure of SSNs. See Employers Barred from Putting Social Security Numbers of Paychecks (/LegalIssues/StateandLocalResources/Pages/CMS_019970.aspx) and State Mandates Employee Data Protection Policy (/LegalIssues/StateandLocalResources/Pages/StateMandatesEmployeeDataProtectionPolicy.aspx).

To safeguard SSNs, employers should a) verify a new employee’s SSN by contacting the Social Security Administration (http://www.ssa.gov/), b) avoid using SSNs as a form of identification for either employees or customers, and c) require health insurance carriers to not use SSNs. See Guarding Against Identity Theft: HR’s Role (/TemplatesTools/Toolkits/Pages/tIdentityTheftHR'sRole.aspx). Developing policies and procedures, such as those in the sample below, is another way HR can help protect SSNs.
Purpose

It is the policy of [Company Name] to protect the confidentiality of its employees’ and applicants’ Social Security numbers (SSNs) obtained and used in the course of business. All executives, managers and employees are expected to adhere to this policy. Any employee violating the provisions of this policy will be disciplined in accordance with company rules.

Procedures

Collection of SSNs

SSNs will be collected from applicants and employees as required to meet federal or state reporting requirements. These purposes include:

- To conduct pre-employment background checks.
- To verify eligibility for employment.
- To withhold federal and state taxes.
- To comply with state new-hire reporting.
- To facilitate enrollment in company benefits plans.

SSNs may also be collected from creditors, suppliers or independent contractors where no tax identification or employer identification number is accessible. SSNs so obtained will be subject to the same provisions of the privacy policy as those for applicants and employees.

Use of SSNs

Except for verification and reporting uses for the above-referenced reasons, no SSN or portion of an SSN will be used in the conduct of the company’s business. In addition:

- No SSN or portion of an SSN will be permitted to be used for identification badges, parking permits, timecards, employee rosters, employee identification records, computer passwords, company account records, licenses, agreements or contracts.
- No SSN or portion of an SSN will be used in open computer transmissions or company distributions or through the company intranet except where such transmission of information is by secure connection or is encrypted. As examples, reporting of payroll withholding taxes and benefits plan participation require such data; thus, such transmissions of data will be handled through secured computer transmission only.

Storage of SSNs

All documents containing SSNs should be stored in locked, secured areas. All computer applications containing SSNs should be maintained on secured, authorized-access computer stations only.

Access to SSNs

Only persons who have a legitimate business reason will have access to SSNs. Such access will be granted through department heads responsible for functions with reporting or transporting of such data responsibilities. Department heads and employees granted such access must take all necessary precautions to ensure the integrity of records that include such numbers when the records are not being used.

Destruction of SSNs
Records that include SSNs will be maintained in accordance with federal and state law. When such documents are released for destruction, the records will be destroyed by shredding.

**State Laws**

If this policy, or any part thereof, conflicts with a state law in any state in which the company operates, the state law should supersede this policy, or the relevant portion thereof.

**Express Requests**

The HR Knowledge Center has gathered resources on current topics in HR management. Click here (http://apps.shrm.org/HRResources/ExpressRequests.aspx?type=6) to view and request information.

*This material is for informational purposes only and not for the purpose of providing legal advice. You should always contact your attorney to determine if this information, and your interpretation of it, is appropriate to your particular situation.*