GENERAL PRINCIPALS OF EMPLOYEE RECORDKEEPING

by

D. Wesley Newhouse
Newhouse, Prophater & Letcher, LLC
3040 Riverside Drive
Columbus, OH 43221
Tel: (614) 255-5441
Fax: (614) 255-5446
www.npllawyers.com
wnewhouse@npllawyers.com

I. SOURCES OF LAW REQUIRING RECORDKEEPING.

A. Federal Law.

1. *Health Insurance Portability and Accountability Act (HIPAA),* 42 USC Sections 1320 *et. seq.* This statute addresses the making, keeping and privacy of protected health information. The act applies indirectly to employers.

2. *Fair Credit Reporting Act (FCRA),* 15 USC Section 1681 *et. seq.* This statute requires that employers who employ outside agencies to obtain background information on employees and applicants restrict access to and use of the information, provide employees and applicants with notice of their rights, and dispose of background reports in a manner that prevents identity theft.

3. *Fair Labor Standards Act (FLSA),* 29 USC Sections 201 *et. seq.* This statute imposes minimum wage and overtime requirements, and requires that employers keep payroll records.

4. *Portal to Portal Act,* 29 USC Sections 251 *et. seq.* This act addresses payment of workers for time spent in transit to the job.

5. *National Labor Relations Act,* 29 USC Sections 151 *et. seq.* This act addresses the right of employees to join unions and otherwise act collectively, and defines unfair labor practices by employers, employees and unions.

6. *Labor Management Relations Act,* 29 USC Sections 401 *et. seq.,* especially Section 433. This addresses reporting regarding payments made by employers to labor unions and employees regarding union-related activities.

7. *Age Discrimination in Employment Act,* 29 USC Section 621, *et. seq.,* especially Section 626.

8. *Occupational Safety and Health Act,* 29 USC Section 651 *et. seq.,* especially Section 657. Prohibits age discrimination in employment.

9. *Employee Retirement Income Security Act,* 29 USC Sections 1001 *et. seq.,* especially Section 1027. Regulates employee benefit plans.

10. *Civil Rights Act of 1964,* 42 USC Sections 2000e, especially 2000e(8). Prohibits discrimination in employment based on race, color, national origin, religion and sex.

11. *Family and Medical Leave Act,* 29 USC Section 2601 *et. seq.* Requires that certain employers make available to certain employees unpaid leave for serious health conditions.

B. State Law.

1. *Worker's Compensation Recordkeeping Requirements,* ORC Sections 4123.22 through .28.

2. *Employment of Minors,* ORC Section 4109.11.

3. *Minimum Wage,* ORC Section 4111.08.

4. *Occupation Safety and Health for State and Municipal Government Employees,* ORC Section 4167.11.

5. *Blood-borne Pathogen Recordkeeping for State and Muncipal Employers,* ORC Section 2167.28.

II. SECURITY OF RECORDS.

A. Protection from Damage or Loss.

1. *Get Organized.* Before you can protect a record, you have to know where it is and who is responsible for it. This may be as simple as developing a list of the files with a notation of who has physical possession of it, or it may involve complicated bar code systems which track the whereabouts of all records at all times.

2. *Centralize.* It is easier to keep a record safe if it is kept in a known, controlled environment.

3. *Duplicate.* With scanning technology and various methods of electronic storage of records, there really is no excuse for not duplicating important records which must be kept.

4. *Off-site Storage.* With the ease of electronic duplication of records comes greater ease in maintaining a duplicate set of records off-site in a secure location for reconstruction of records in the event of catastrophic loss.

5. *Security.* Records stored on-site and off-site need to be secured by locking them up and identifying who may have access. For electronic records, this may include encryption, pass word protection, the use of firewalls, and other security methods.

B. Confidentiality.

1. *Information Security Program.* The Federal Trade Commission adopted rules for the security of information for customers of financial institutions which serve as a good model for employers. See 16 CFR Section 314. The rules require the adoption of a security program with the following elements:

   a. The program is in writing and is readily accessible.

   b. The plan designates an employee or employees who are responsible for coordination of the program.

   c. The record keeper performs an assessment of internal and external risks to the confidentiality of records.

   d. The record keeper provides training to employees concerning security issues.

   e. Information systems include intrusion detection and prevention programs.

   f. The record keeper regularly monitors and tests the security systems.

   g. The record keeper takes reasonable measures to oversee the work of service providers by exercising due diligence in their selection, requiring them to implement appropriate security programs, and monitoring their security efforts.

2. *Record Disposal.* The FTC adopted regulations in June of 2005 addressing the disposal of consumer report records which state best practices for disposal of sensitive information generally. See 16 CFR Part 682. Those regulations state that the keeper of records should do the following when disposing of the records:

   a. Burn, pulverize or shred paper reports so that the information cannot be read or reconstructed;

   b. Destroy or erase data stored electronically so that the data cannot be reconstructed;

c. Delegate these functions to a qualified contractor after exercising due diligence in selecting the contractor.

III. RECORDS THAT SHOULD BE STORED SEPARATELY.

A. Records that Contain Medical and Health Information.

1. *Pre-employment drug screen results.*

2. *Post-employment physical examination results.*

3. *Health insurance claim information.*

4. *Employee requests for leave and resultant medical reports.*

5. *Releases from physicians to return to work.*

6. *Worker's compensation medical records.*

7. *Information detailing disabilities.*

8. *Health and life insurance application information.*

9. *OSHA supplemental incident reports.*

B. Protected Consumer Information.

1. *Consumer Reports.* The Fair Credit Reporting Act and the FTC regulations implementing it make virtually any background information gathered for an employer by a third party protected consumer information. The Act and regulations require that the employer limit access to and use of the information, and requires that the employee who is the subject of the report consent in writing to its release.

2. *Identifying Information.* With well-publicized incidents of data theft, employers are well-advised to take measures to separate social security numbers and dates of birth from other records. When employees identify beneficiaries in life and disability insurance policies, or when they include family members in health insurance programs, they sometimes provide identifying information about their family members. This should also be safeguarded.

3. *Employee Financial Transactions.* Some employers lend money directly to employees, and some allow employees to borrow from

retirement savings accounts. Employees would reasonably expect that information about this will not be generally available.

IV. ACCESS TO RECORDS BY EMPLOYEES AND OTHERS.

A. General Personnel Records.

Ohio does not have a law which requires an employer generally to allow an employee to have access to a personnel file. Other states do have such laws. Most employers will allow employees to have reasonable access to such records, with limits on frequency, time, place and manner of access.

Note that Ohio's Public Records Law, ORC Section 149.43, makes general personnel records of public employees accessible to the public.

B. Medical Information.

OSHA recordkeeping requirement require that employees be given access to toxic substance exposure and related medical testing information. Employers must also allow employees to see logs of accidents and injuries and supplemental incident reports that address their own injuries and medical conditions.

OSHA regulations and the Health Insurance Portability and Accountability Act (HIPAA), require that employers limit access of third parties to medical records, and generally require that such information be released only upon written authorization of the employee.

C. Review of Information by Government Agencies.

In most circumstances, the government agency charged with enforcing the statute which requires the keeping of a record has the right to see the record. For example, OSHA has a right to see the incident log that OSHA regulations require the employer to keep. There are some general considerations for the employer in this circumstance:

1. *Scope of the Inquiry.* When an enforcement agency conducts an investigation to enforce a specific statute, the agency should restrict its inquiry to the records pertinent to that law and that investigation. An OSHA inspector, for example, should have no interest in and should not inquire about a background check conducted as part of the process of hiring an employee. Each regulatory agency has its own set of regulations governing the scope of record requests and the protection of the privacy of those whose records are reviewed.

2. *Subpoena Power.* Regulatory agencies have the ability to go to court to get subpoenas to compel an employer to produce records. The same laws that permit this also protect the employer and employee from unreasonable intrusions by allowing interested parties to ask the court to void or narrow the scope of the request for records.

3. *Trade Secret Information.* The regulations authorizing agencies to obtain records usually include provision for the protection and non-disclosure of trade secret information. For example, there are detailed regulations addressing the disclosure of trade secret information in Material Safety Data Sheets, and the provision of such information to medical care providers for employees injured by toxic substances.

V. RETENTION AND DISPOSAL GUIDELINES.

A. General Retention Guidelines.

1. *Medical Records.* Duration of tenure, and then 2 years after termination of employment, except records of toxic substance exposure, which must be kept for the duration of employment plus 30 years. Records of occupational injuries or illnesses not arising from toxic substance exposure are to be kept for the duration of employment plus 5 years.

2. *Recruitment and Selection Records.* These must be kept for one year from the date of the opening of the position.

3. *FMLA Leave Records.* These should be kept for a period of 7 years while the employee is in active employment. If an employee has left employment, the records should be retained for 3 years after the date of termination.

4. *Payroll Records.* Three years from the last date of entry for the employee.

B. Disposal Guidelines.

See preceding discussion of best practices for the disposal of records in a manner intended to minimize data theft.

VI. REQUIRED vs. RECOMMENDED EMPLOYMENT RECORDS.

A. Why Do We Keep These?

If you cannot answer this question in respect to any given record, you need to do the following:

1. *Investigate the Law*. You might keep a record because the law requires it. Laws change, however, and usually at a faster pace than employers' record keeping policies and practices. When you update your employment policies (hopefully at least annually), you should survey the records you keep and identify the law or regulation that requires you to keep them.

2. *Develop New Policies Addressing Record Retention.* If you purge the records once per year to get rid of the records you no longer are required to keep, the records will come back. You must develop record creation and retention policies that will inform others of what records should be made and what should not be made.

3. *Destroy What You Do Not Need.* As the problem of data theft worsens, unnecessary records will become an ever-greater source of liability exposure. If you cannot justify the retention of a record, destroy it in a fashion which will prevent others from using it.

B. Discourage the Uncontrolled Making of Records.

Every management lawyer's nightmare is the supervisor's "private file", which usually contains the record which, when taken out of context, becomes Exhibit A in the former employee's trial. Supervisors are not only making and keeping records for their convenience, they are creating evidence. The law requires that an employer create certain evidence, such as an illness and injury log or a supplemental report of an incident. Everything else should be prepared only if required by the law and required by necessity.

C. How and When to Make Records that the Law Does Not Require.

1. *Disciplinary records* reflecting efforts to correct poor job performance or bad behavior can be helpful if done correctly. This should be done as a matter of routine, and under the supervision of a person experienced with the defense of employment claims.

2. *Job Descriptions.* Although not required by the law, regulations under the ADA create a presumption that a job description validly describes essential job functions. This is helpful in defending

disability discrimination claims. Job descriptions need to be updated regularly, and there needs to be a careful review and designation of the job duties that are essential functions.

3. *Training.* OSHA mandates that hazard communication training be documented, and state licensing laws may require that other training be documented, but most training need not be documented. The provision of training is helpful in the defense of almost every kind of employment claim, so documentation of the training, including attendance records, is helpful.