

**DOCUMENTATION AND RECORDKEEPING:  
WHAT YOU MUST HAVE, SHOULD HAVE,  
AND NEVER WANT TO SEE IN YOUR COMPANY'S RECORDS <sup>1</sup>**  
**Employment Roundtable**

*By Stacey Mark*

*Chair, Labor & Employment Group and  
Chair, Sustainable Practice Advisory Group*

**August 16, 2007**

Documentation and recordkeeping are tasks that many companies too often forego. Despite the excuses supporting avoidance (*e.g.*, it's too time consuming, it's best not to commit to anything in writing, we have no place to store records, we only have a few employees and everyone knows "the rules"), there are many, better reasons to document and retain records.

One reason to keep records is that many laws *require* it. For example, wage and hour laws require employers to keep records of hours worked and amounts paid to employees. Immigration laws require employers to maintain records documenting their employees' eligibility to work in the United States. Tax laws require employees to complete a tax withholding statement annually. Family medical leave laws require employers to maintain requests for leave (if presented in writing), records of leave taken, and required notices provided to employees, among other things. State and federal safety and health laws require employers to track and record workplace injuries and illnesses. The foregoing list is far from exhaustive.

Another reason to keep records is that they aid employers in managing their workforce. As a form of communication, good documentation helps to reduce the risk of misunderstanding and misinterpretation inherent in oral communication. Those who listen "selectively" are less likely to misinterpret a written communication. In addition, documentation is a method of preserving history. It can tell an objective observer what was done or not done and why. This is why employers tell supervisors (and lawyers tell employers) to "document everything."

In addition, records often prove to be critical in litigation. If your organization is not already thinking about how to manage records in the event of litigation, it should be. The federal electronic discovery rules that went into effect on December 1, 2006, which apply only to electronically stored data, require preservation of electronic data as soon as the organization is on notice that litigation is likely. This obligation can be extremely burdensome, particularly in the absence of a document retention policy.

---

<sup>1</sup> This memorandum contains a summary of information obtained from laws, regulations, court cases, administrative rulings, and legal publications and should not be viewed or relied upon as legal advice. Ater Wynne LLP urges readers of this memorandum to consult legal counsel regarding specific legal issues and factual circumstances.

Complying with all of the laws applicable to documentation, recordkeeping, and retention can be overwhelming. In this memorandum, we try to simplify that task by addressing what employment records must be kept by law, what records should and should not be kept as a matter of policy, and how and for how long to main existing records.

## **I. RECORDS THAT MUST BE MAINTAINED BY LAW (EXCLUDING HIPAA)**

Many federal and state laws affect recordkeeping practices. Some of these laws apply to all employers, while others apply only to specified categories of employers or employees. The following is a summary of some of the more common requirements that affect employers in Oregon.

Federal laws and/or regulations that contain recordkeeping requirements include the Americans with Disabilities Act (ADA),<sup>2</sup> Age Discrimination in Employment Act (ADEA),<sup>3</sup> Equal Pay Act,<sup>4</sup> the Family and Medical Leave Act (FMLA),<sup>5</sup> the Fair Labor Standards Act (FLSA),<sup>6</sup>

---

<sup>2</sup> 29 CFR § 1602.14 (requiring retention for at least one year of *any* personnel or employment record made or kept by an employer, “including but not necessarily limited to requests for reasonable accommodation, application forms submitted by applicants and other records having to do with hiring, promotion, demotion, transfer, lay-off or termination, rates of pay or other terms of compensation, and selection for training or apprenticeship”).

<sup>3</sup> 29 CFR § 1627.(3)(b):

(1) Every employer who, in the regular course of his business, makes, obtains, or uses, any personnel or employment records related to the following, shall, except as provided in paragraphs (b) (3) and (4) of this section, keep them for a period of 1 year from the date of the personnel action to which any records relate:

(i) Job applications, resumes, or any other form of employment inquiry whenever submitted to the employer in response to his advertisement or other notice of existing or anticipated job openings, including records pertaining to the failure or refusal to hire any individual.,

(ii) Promotion, demotion, transfer, selection for training, layoff, recall, or discharge of any employee,

(iii) Job orders submitted by the employer to an employment agency or labor organization for recruitment of personnel for job openings,

(iv) Test papers completed by applicants or candidates for any position which disclose the results of any employer-administered aptitude or other employment test considered by the employer in connection with any personnel action,

(v) The results of any physical examination where such examination is considered by the employer in connection with any personnel action,

(vi) Any advertisements or notices to the public or to employees relating to job openings, promotions, training programs, or opportunities for overtime work.

<sup>4</sup> 29 CFR § 1620.32.

<sup>5</sup> 29 CFR § 825.500 (basic payroll and identifying employee data; dates FMLA leave is taken; if FMLA leave is taken by eligible employees in increments of less than one full day, the hours of the leave; copies of employee notices of leave furnished to the employer under FMLA, if in writing, and copies of all general and specific written notices given to employees as required under FMLA; any documents (including written and electronic records) describing employee benefits or employer policies and practices regarding paid and unpaid leaves; premium payments for employee benefits; records of any dispute between the employer and employee regarding designation of leave as FMLA leave, including any written statement from the employer or employee of the reasons for the designation and for the disagreement; and requiring confidentiality of certain medical records).

<sup>6</sup> 29 CFR Part 516 (payroll information; basic biographical data, including name, social security number,

Title VII of the Civil Rights Act of 1964 (Title VII),<sup>7</sup> the Immigration Reform and Control Act (IRCA),<sup>8</sup> the Occupational Safety and Health Act (OSHA),<sup>9</sup> and the Employee Retirement Income Security Act (ERISA).<sup>10</sup> In addition, a number of tax laws, including the Federal Insurance Contribution Act (FICA), the Federal Unemployment Tax (FUTA), and federal income tax withholding regulations, require that employee records related to mandatory federal taxes be retained. Employers conducting special types of employee testing, such as polygraph testing (to the extent it is permitted by law), are often subject to detailed recordkeeping requirements.<sup>11</sup>

Federal contractors and subcontractors are also subject to the Davis-Bacon Act,<sup>12</sup> the Service Contract Act,<sup>13</sup> and the Walsh-Healy Public Contracts Act,<sup>14</sup> all of which require retention of employee demographic information and compensation records. In addition, federal contractors and subcontractors are subject to Executive Order 11246,<sup>15</sup> the Vietnam Era Veterans' Readjustment Act (Vet's Act),<sup>16</sup> and the Rehabilitation Act of 1973,<sup>17</sup> which require maintenance of affirmative action plans (AAPs) and "good faith efforts" documentation.

---

home address, hours worked, pay rate, *etc.*).

<sup>7</sup> 29 CFR Part 1602 (personnel and employment records, including requests for reasonable accommodation; personnel records relating to charges of discrimination); *see also*, 29 CFR § 1602.7 (requiring employers with 100 or more employees to file the Form 100 (EEO-1) report. Employers must retain a copy of the most recent report at all times at company or divisional headquarters and make it available to the Equal Employment Opportunity Commission (EEOC) upon request.

<sup>8</sup> 8 CFR § 274a.2 (employers must retain I-9 forms but need not retain verification documents).

<sup>9</sup> 29 CFR §§ 1900 to 1999. Recordkeeping requirements are heavily regulated and specific to certain industries, equipment and/or types of operations.

<sup>10</sup> 29 USC §§ 1027, 1029 (must maintain records on the matters for which disclosure is required sufficient for verification or clarification; records sufficient to determine benefits); 29 CFR Part 2520 (describing documents to be retained).

<sup>11</sup> *See, e.g.*, 29 CFR § 801.30 (listing detailed record retention requirements relating to polygraph examinations). As another example, the Department of Transportation imposes recordkeeping requirements on employers conducting drug and alcohol testing. *See* 49 CFR § 40.333. On the other hand, genetic testing information generally may not be retained at all (note that such testing for employment purposes is generally prohibited). ORS 192.537.

<sup>12</sup> 40 USCA §§ 276a-276a-5; 29 CFR § 5.5.

<sup>13</sup> 41 USCA § 351, *et seq.*; 29 CFR § 4.185 (recordkeeping requirements); 29 CFR § 4.6(g).

<sup>14</sup> 41 USCA §§ 34-45; 41 CFR § 50-201.501 (maintenance of records of employment); 41 CFR § 50-201.502 (Record of injuries).

<sup>15</sup> 41 CFR § 60-4.3; 41 CFR § 60-1.12. Under 41 CFR § 60-1.12(c)(ii), a contractor must be able to identify "where possible, the gender, race, and ethnicity of each applicant." In light of Internet job postings and electronic resume submissions, the issue of who qualifies as an "applicant" has become more complicated. The OFCCP has answers to frequently asked questions (FAQs) on this topic available at <http://www.dol.gov/esa/regs/compliance/ofccp/faqs/iappfaqs.htm#Q1GI>.

<sup>16</sup> 41 CFR § 60-250.80.

<sup>17</sup> 29 USC § 79341; CFR § 60-741.80 (recordkeeping requirements; people with disabilities).

Oregon law also mandates recordkeeping under wage and hour laws,<sup>18</sup> the Oregon workers' compensation law (OR-WC),<sup>19</sup> the unemployment compensation regulations,<sup>20</sup> and the Oregon Safe Employment Act (OSEA or OR-OSHA).<sup>21</sup>

### **Types of Employment Records Required by Law<sup>22</sup>**

<b>Type of Record</b>	<b>Law Requiring Retention</b>
Job advertisements and internal job postings	ADEA, FLSA and ADA
Employment applications and/or detailed information on applicants	ADA/Title VII ADEA, and OFCCP affirmative action regulations
Offers and hiring records	ADA, Executive Order 11246, Title VII, Vet's Act
INS Form I-9	IRCA
Basic employee data (name, address, birth date, sex, <i>etc.</i> )	FLSA; many others
Promotions, demotions, and transfers	ADA, ADEA, and Title VII
Time cards	ADEA and FLSA
Payroll records	Oregon minimum wage law and unemployment insurance law, ADEA, Equal Pay Act, FMLA, FLSA, Internal Revenue Code
Records of leaves of absence and disputes regarding leave eligibility	FMLA
Reasonable accommodation records	ADA
Medical records	ADA, ADEA, FMLA and Civil Rights Act

<sup>18</sup> See ORS 653.045 (records to be kept by employers; itemization of deductions from wages); ORS 653.310 (child labor records); OAR 471-031-005 (payroll records); ORS 652.750(3) (personnel records).

<sup>19</sup> OAR 436-050-210 to 436-050-220 (self-insured employers) (payroll records; assessments; contributions; occupational safety and health loss-control program; records of claims and payment of claims); OAR 436-060-0010(4) (Reporting requirements; "When the worker requires only first aid and chooses not to file a claim, the employer shall maintain records showing the name of the worker, the date, nature of the injury and first aid provided for one year. These records shall be open to inspection by the director, or any party or its representative").

<sup>20</sup> ORS 657.660 (records and reports of employing units); OAR 471-031-0005 (payroll records).

<sup>21</sup> ORS 654.120(2): "Each employer shall keep records, in the manner prescribed by the Director of the Department of Consumer and Business Services, of work-related deaths and serious injuries and illnesses, and of such other relevant occupational safety and health matters as are reasonably necessary for achieving the purposes of ORS 654.001 to 654.295 and 654.750 to 654.780. Each employer shall notify the Director forthwith of the work-related death of any employee of the employer, and shall make such other reports as the Director may reasonably prescribe by rule or order." OAR 437-001-0700 (Recordkeeping and Reporting) (Form 300 and Oregon DCBS Form 801; annual summary of injuries and illnesses).

<sup>22</sup> See references in footnotes 3-21, *supra*.

Type of Record	Law Requiring Retention
Employee pay and benefit plans	FMLA, ERISA
Child labor information/certificates	ORS
Employment contracts	Equal Pay Act and FLSA
Records and logs of occupational injuries, illnesses, and deaths	OSHA/OSEA
Employee exposure to toxic substances	OSHA/OSEA
Records of layoffs	ADA, ADEA, and Title VII
Employee terminations	ADA, ADEA, Executive Order 11246, and Title VII
EEO-1 and Vets-100 reports	ADA, Executive Order 11246, Title VII, Vet's Act
Affirmative Action Plans and documentation	Executive Order 11246, Vet's Act, <i>etc.</i>

## II. RECORDS EVERY EMPLOYER SHOULD MAINTAIN

Whether or not a specific law requires it, employers should keep certain employment records because they are critical in many situations. Applicant records, including applications, resumes, test results, licenses, accreditation, references, background checks, drug test results, and any other documents considered in deciding whether or not to hire the applicant, should be retained. To the extent EEO information is obtained in connection with an applicant, it should be maintained in a separate file.

Employers should maintain a personnel file for each employee. The kinds of records that employers should keep in an employee's personnel file are those relevant to qualifications, hiring, transfer, promotion, discipline, and discharge. An employment application, resume or curriculum vitae, records of changes regarding compensation and status, training, performance evaluations, other documentation relating to performance (good and bad), and documentation relating to discipline and discharge are the types of records that would typically be reviewed in connection with employment decisions and, therefore, should be in the personnel file.

The kinds of records that should *not* be kept in a personnel file are EEO data (*e.g.*, those reflecting race, ethnicity, religion, disability, etc.), medical records, worker's compensation records, family medical leave records, detailed pay and benefits records, and insurance forms. Not only are such documents irrelevant to employment decisions regarding hiring, firing, transfer, promotion, discipline and discharge, consideration of the type of information contained in these records, such as marital status, race, religion, disability, or use of FML or the worker's compensation system, is impermissible when making such decisions. In addition, by law, some of this information *must* be maintained in separate, confidential files. Maintaining such records in personnel files may suggest that the information was impermissibly used to discriminate based on protected status.

## A. Documenting Expectations and Performance

Employees need to know what is expected of them, and by whom. Employers can document expectations in job descriptions and employee handbooks (in the form of performance and behavioral standards). Day-to-day expectations may be communicated less formally, in the form of task lists, memoranda, and email.

When identifying and documenting performance problems, it is important to identify the expectations or performance standards that were not satisfied and provide examples, rather than relying on subjective criteria, such as “attitude.” Objective descriptors may include:

- Failure to meet quota or other measure of productivity
- Engaging in disruptive behavior
- Absences from workstation
- Conducting personal business at work/personal calls
- Punctuality/absences (only if not protected, *e.g.*, by family medical or disability leave laws)
- Defective work
- Complaints from customers, co-workers
- Insubordination (refusal to do assigned work, follow directions, act respectfully to supervisor)

It is far easier to identify and document performance deficiencies when you have a written standard for reference. Criticism of tasks that are not part of the employee’s job description or other documented expectations can lead to a perception of unfair treatment and morale problems, which is often what drives employees to file discrimination and other employment-related complaints.

Documentation of performance problems should follow the same guidelines as employee counseling. Identify the issue being addressed, provide specific examples of the employee’s deficient performance, and state that it was communicated to the employee. Documentation of coaching or an oral warning could consist of no more than a note to the personnel file or Human Resources to the effect that the supervisor spoke with the employee on a certain date about a particular issue. It does not need to be signed by the employee. You may want a written warning to be a bit more detailed and signed by the employee as an acknowledgment that the employee read and/or received it. Occasionally, employees want to submit a response or refuse to sign a written disciplinary action. If the employee refuses to sign, the person imposing the disciplinary action should document the refusal on the written warning. If the employee submits a written response, the response should be kept in the personnel file.

## Sample documentation:

*Memo to: HR/personnel file  
Re: [Employee]  
From: SEM  
Re: Disciplinary Action (Oral Warning/Written Warning/Other)  
Date: November 9, 2006*

*I met with employee on [date] to discuss his/her failure to [state performance deficiency]. I gave employee these examples [list examples of deficient performance]. I asked what assistance would enable employee to improve his/her performance. I offered this assistance [state types of assistance offered]. I told employee he/she must demonstrate significant and sustained improvement within [stated time] or [state consequences that will follow].*

You may also want to include in the documentation the employee's reaction to counseling (good or bad).

### **B. Documenting Misconduct**

In instances of employee misconduct, it may be necessary to conduct an investigation, which should be documented. Documentation of the investigation should be maintained in a separate, confidential file, and *not* in the personnel file of the accused or complaining employee. This is because the mere fact that an employee was the subject of a complaint or accused of misconduct is not an appropriate consideration in making employment decisions affecting that individual (and, in fact, may be legally prohibited).<sup>23</sup> Moreover, employees have the right to inspect their personnel files, and investigation materials may contain confidential witness statements that would be inappropriate to provide to the target of the investigation or to the complaining employee.<sup>24</sup>

If an investigation reveals a violation of company policy or other misconduct, documentation of the disciplinary action taken against the perpetrator should be retained in his or her personnel file. Even if the results of the investigation are inconclusive, it still may be appropriate to document any action taken (*e.g.*, requiring employee to review company policies, attend harassment training, etc.) in the alleged perpetrator's file. The documentation should be carefully tailored to avoid any suggestion that the employer (through the perpetrator's conduct) violated the law. No documentation (including complaints and witness statements) should be placed in the personnel files of employees who, in good faith, report misconduct or provide statements in connection with an investigation of misconduct.

---

<sup>23</sup> An exception may be an employee who was the subject of multiple complaints of misconduct of a similar nature, such as harassment, violence, etc., or an employee who makes unfounded accusations against a co-worker.

<sup>24</sup> In documenting an investigation, it may be appropriate to identify individuals who provide information as Employee A, Employee B, etc., rather than by name, and to maintain a separate "key" or identification list.

### III. THINGS YOU NEVER WANT TO SEE IN YOUR RECORDS

There are certain types of documentation you would *never* want to see in your employees' personnel files, email, or general records (often referred to in litigation as the "smoking gun"). These include:

- **References to protected status** (race, sex, sexual orientation, marital status, age, disability, religion, national origin, or veteran status; employee complaints about discrimination, harassment, or violations of the law; an employee's use of or request for employment-related benefits, such as family medical leave, reasonable accommodation, or worker's compensation).
- **Statements admitting wrongdoing by the company.** Examples of this would include a payroll record saying "we misclassified Joe and others in his position as exempt, so we need to fix this going forward." Another example would be "Sally was sexually harassed by Bob at the trade show." Statements like this could be used later in litigation to show that the company violated the law.
- **Editorializing or use of subjective remarks about an employee.** Some employees tend to include subjective comments in documentation in ways that can prove dangerous in litigation. For example, "Susie was absent AGAIN." If Susie's absence is treated as protected under family medical leave or disability law, or her absence is due to her own illness or her child's illness or disability, the next time she is disciplined such a note could provide support for Susie's argument that she was criticized unfairly or treated less favorably because of her protected status (based on use of family medical or disability leave, marital status, etc.).
- **Inaccurate, false, or misleading information.** The publication of false and defamatory information could result in a claim for libel or slander. This could come up in connection with the circulation of inaccurate or misleading information about why an employee is subject to discipline or no longer with the company.
- **Duplicate files.** Supervisors often keep notes or diaries of day-to-day events, but fail to compile these notes in a formal document that is shared with the employee and/or placed in the employee's personnel file.
- **Medical information.** Failing to maintain the confidentiality of medical records violates the ADA, FMLA, and HIPAA, which require that medical information be collected and maintained on separate forms and in separate, confidential, medical files with restricted access. Supervisor files that contain medical information probably violate these laws.
- **Privileged documents and communications.** Attorney-client communications are privileged only when they are kept confidential. Forwarding or sharing communications from the company's attorneys with third parties or employees not covered by the privilege (typically limited to the top level of management) will result in a loss of the attorney-client privilege, particularly if the communication has no appropriate identifier (e.g., "Attorney-Client Privileged Communication"). This means that the company's

discussion with its lawyers (not just the communication, but all discussions on the same topic) may be discoverable in litigation.

- **Drafts of performance evaluations.** It is generally not a good idea to keep drafts of personnel evaluations. In at least one case, a plaintiff argued, unsuccessfully, that the fact that his evaluations were revised downwards showed evidence of discrimination based on his HIV status. Although the court rejected this argument, the issue would have been avoided if the company had a uniformly-applied policy of not retaining drafts and notes of performance evaluations.<sup>25</sup>
- **Other information.** It is generally inappropriate to keep records of after-hours behavior, arrest records, personal finances, family background, club memberships, religious affiliations, union memberships, and political beliefs.

One of the most likely places to find the foregoing types of inappropriate information is in email. There is a misconception that email is transient -- that once it is sent, only the intended recipient will see the contents. Of course, this is not true: email may be forwarded by the recipient to others, it may be printed out and copied, it may be accessed without authorization, and it may be stored electronically even after the sender and recipient have “deleted” the message. Forensic computer experts can locate email on computer backup files that you may not realize is there.

Special problems with email also arise due to its casual, conversational nature. Even when employers intentionally use email to create a permanent record of an employee’s performance, the ease with which email is used may seduce supervisors and human resources professionals into using a casual style that may not always come across well when read by others.

Email messages show up routinely in employment and other types of litigation. For example, email containing derogatory references to women has been used in employment litigation to prove sex discrimination. Email distribution of racist, ethnic and/or sexist jokes is often introduced to prove a hostile environment. There have been lawsuits involving employee claims for invasion of privacy arising from the employer’s access, review and/or retrieval of private email messages.

One well-known example of email used to prove liability is the Department of Justice’s (DOJ) successful antitrust case against Microsoft, in which Microsoft emails suggested that the company sought to put Netscape out of business. Also newsworthy was the DOJ’s use of internal emails to support charges against Hewlett-Packard officials in connection with the Board of Directors’ investigation into leaks of confidential information to the press. Locally, the DOJ used internal emails to support charges against Schnitzer Steel for violation of the Foreign Corrupt Practices Act.

Email has the potential to be problematic, even when inadvertent mistakes are made. For example, an Oregon Bureau of Labor and Industries (BOLI) article addressed the inadvertent use of the word “butt” instead of “but” in an email addressed to an employee who was sensitive about her postpartum weight. BOLI’s advice:

---

<sup>25</sup> It is not permissible to destroy evidence after a complaint has been made or claim has been filed.

Employer's emails need to state things in as purely a factual manner as possible because communicating opinions, judgments or anything that could be interpreted as offensive or flippant in writing, without the benefit of the personal non-verbal interactions you can observe, are easily misunderstood.

Also, an investigation should be initiated to determine whether [the sender] is engaging in inappropriate workplace harassment by utilizing email as a vehicle for improper comments. Given [the sender's] use of the word 'butt' in his email, which you interpreted to be a reference to your backside, you should share the email with your supervisor so they might conduct the appropriate investigation to ensure that [the sender] is not engaging in harassing behavior.<sup>26</sup>

The bottom line is that email should be treated with the same care as any other form of documentation. Employers must assume that email is a permanent record that will be discoverable in the event of a lawsuit. Consequently, whether or not email is used as a formal method of documenting employee performance, it should be carefully reviewed *prior* to sending, and treated as if it will be seen by a judge or jury. With this in mind, the following is a list of do's and don'ts pertaining to the use of email and other forms of electronic communication:

- ✓ Do develop a policy on the appropriate use of email, voicemail, and the Internet.
- ✓ Do use email to communicate business information, instructions, and expectations.
- ✓ Do use email to communicate directly with employees about their performance and conduct.
- ✓ Do use email to communicate factual information to others about employee conduct or performance that is not subject to interpretation (for example, "Joe was absent from January 1 through 10" or "Sally left work without permission today" or "Here is a list of employees in the sales department and their respective sales for the quarter").
- ✓ Do prepare, proofread, and spell check email as you would any other professional correspondence, and as if a judge or jury may read it.
- ✓ Do use email to communicate implementation of and changes to existing company policies.
- ∅ Do not use email to communicate your personal feelings about employees.
- ∅ Do not use email to communicate subjective evaluations of employee conduct or performance.
- ∅ Do not use email to discuss personnel actions taken or contemplated, except when you are communicating directly with the employee at issue.
- ∅ Do not use email to communicate information about an employee complaint or

---

<sup>26</sup> See BOLI Technical Assistance, [http://www.oregon.gov/BOLI/TA/T\\_Newspaper\\_Columns.shtml](http://www.oregon.gov/BOLI/TA/T_Newspaper_Columns.shtml) (*The Trouble with Email*, August 1, 2006).

the investigation of an employee complaint.

- Ø Do not use email to discuss an employee's physical or mental condition (especially a general email like "Sally will be in the hospital for a while getting treatment for cancer in case anyone wants to send her flowers").
- Ø Do not use email to discuss an employee's status in a protected group (age, sex, sexual orientation, race, etc.).
- Ø Do not use email to communicate racist, sexist, religious, ethnic, or age-related jokes.
- Ø Do not use email to communicate information sought or obtained from legal counsel unless it has an appropriate identifier and directions not to forward.
- Ø Do not use email to communicate opinions regarding the company's legal liability.
- Ø Do not access or monitor employee email, voicemail, or Internet use without a policy that clearly states these systems belong to the company and are not private (even so, you should contact legal counsel before accessing any electronic storage systems used by an employee).

#### **IV. ESTABLISH AND ENFORCE AN ELECTRONIC SYSTEMS POLICY**

Email and other electronically stored data is often where the "smoking guns" are found. To minimize the possibility that your email or other electronic data will be successfully used against your company in litigation, it is important to establish some ground rules for the use of all electronically stored data systems in use at your organization, including email, voicemail, Internet access, pagers, memory sticks, PDAs, and cell phones.

- **Make Sure Employees Understand the Risks.** Your systems policy should educate employees about the risks associated with the careless or improper use of electronic storage devices, such as email and the Internet. These include the following:
  - Email can be easily forwarded, modified, forged, or sent to unintended recipients.
  - Improper email or Internet use may result in the spread of computer viruses.
  - Personal use of electronic systems may exceed permissible use.
  - Email encourages informality. Careless use of email or the Internet may result in liability for libel, defamation, harassment, discrimination, or copyright infringement, and may result in a breach of confidentiality or

waiver of privileges.

Sample (alternative) policy language limiting personal use:

- The purpose of internal communication systems, including email and access to the Internet, is to conduct company business. Personal use of these systems are to be kept to a minimum. Personal use of communication systems (including the Internet) that interfere with the user's productivity or work performance, or the productivity or work performance of others, is prohibited.
  - The Company's internal communication systems, including email, voicemail, and access to the Internet, are strictly for business purposes. Use of these systems to send personal emails or surf the Internet for non-business related reasons is strictly prohibited.
- **Eliminate Privacy Expectations.** Make it clear that employees do not have an expectation of privacy when using company systems.

Sample policy language:

- All of the Company's communication systems, including electronic mail, voicemail, Internet access, and electronic storage systems, are Company property, and are not confidential. The Company reserves the right to access, monitor, and review these systems at any time, and to read and retrieve messages.
- **Set Content Limitations.** Set guidelines for proper and improper content.

Sample policy language:

- Email should be used in a respectful and appropriate way. The Company expects everyone who uses the email system to exercise good judgment and common sense with regard to mail generated both internally and externally. The Company's policies prohibiting discrimination and harassment apply equally to the email system.
  - Email may not be used for any commercial purpose other than Company business. Employees are not permitted to use the Company's email system for "spamming" (distributing commercial, religious, or political messages indiscriminately) or for pyramid or chain letters or other junk mail.
- **Establish Access and Download Limitations.** Prohibit or limit the type of information employees may access, download, or forward.

Sample policy language:

- Employees are not permitted to read, intercept, copy, use, or disclose email communications directed to others without express authorization. Accessing another employee's electronic mailbox without the latter's express permission is strictly prohibited.
  - Employees may not forward any email that is marked "confidential," "privileged," or that contains proprietary or sensitive company information.
  - The Company's access to the Internet is to be used solely for Company business purposes. Authorized business use does not include sites that contain sexually explicit materials, news groups dedicated to hate or violence, gambling, shopping, or job searches. This list is not exhaustive. The Company reserves the right to access and review records of employee use of the World Wide Web.
  - Employees are not permitted to download any software from the Internet without authorization from the Information Systems Department.
  - Employees are not permitted to access or download any pornographic, obscene, or indecent material from the Internet.
- **Anticipate Misdirected Emails.** Email is not guaranteed to be secure, reliable, or free of unwanted viruses. You may wish to remind employees to follow-up on important communications and require emails sent from the company system to carry a disclaimer.

Sample policies:

- The Internet is not necessarily secure or confidential, nor is there any guarantee that email will be delivered timely or at all. Those employees who rely on Internet email should consider the time-sensitivity of the communication, and consider following up by telephone.
- This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager.
- Any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the Company.
- The recipient should check this email and any attachments for the presence of viruses. The sender accepts no liability for any damage caused by any virus transmitted by this email.

- **Establish a Storage/Archiving Protocol.** The company should establish an email retention system.

Sample policy language:

- All emails will be automatically deleted after 60 days. If you need to retain an email for business purposes, the message must be printed or moved to the folder “for archiving.”
- **Consistently Enforce Your Policy.** Once established, companies can and should actively enforce electronic communication policies to minimize liability. Courts will often credit an employer’s consistent enforcement of an email policy as an exercise of reasonable care.<sup>27</sup> Advise employees of the consequences of misuse of electronic systems and consider having them acknowledge the policy in writing.

## V. HOW TO MAINTAIN EMPLOYMENT RECORDS

### A. Non-Medical Records

Some laws restrict what may be placed in an employee’s personnel file. Others restrict access to sensitive information (typically medical information, discussed below). To the extent recordkeeping methods are not mandated by law, certain rules of thumb, nevertheless, should be followed. Specifically, documentation reflecting protected status should be maintained separately from the employee’s personnel file.<sup>28</sup> By separately maintaining such data, an employer can avoid any negative inference that might otherwise be drawn from the fact that decision-maker had access to documentation reflecting the employee’s protected status.

---

<sup>27</sup> See, e.g., *Schwenn v. Anheuser-Busch Inc.*, 1998 WL 166845 (ND NY 1998) (court dismissed sexual harassment claim where the employer showed it promptly responded to an employee’s complaint by issuing a warning to employees not to abuse email); *Mieritz v. Hartford Fire Ins. Co.*, 2000 WL 422909 (ND Tex 2000) (employee who “witnessed” his Christian faith by including biblical quotes in emails to his co-workers, speaking to co-workers about his faith, posting copies of prayers in his work area, and using a Christian screen-saver on his office computer was laid off when his position was eliminated along with three others. In suit for religious discrimination, employer prevailed on summary judgment by showing that the employee was aware of the company’s policy prohibiting the use of company computers for “solicitation or proselytizing,” but did so anyway); *Daniels v. Worldcom Corp.*, 1998 WL 91261 (ND Tex 1998) (employer avoided liability for discrimination based on racially offensive email by demonstrating prompt remedial action of issuing disciplinary warning to employee who sent email and holding a company-wide meeting to discuss the policy on email use); *Sherrod v. Commonwealth Edison Co.*, 2000 U.S. Dist. LEXIS 1626 (ND Tex 2000) (court upheld company’s decision to terminate employee who violated the company’s policy prohibiting employees from downloading and storing pornographic images company computers).

<sup>28</sup> For example, the EEOC recommends that employers maintain records of their employees’ racial/ethnic backgrounds (which covered employers are required to compile for an EEO-1 Report) only when the records are kept separately from the employee’s basic personnel file or other records available to those responsible for personnel decisions (e.g., as part of an automatic data processing system in the payroll department). 29 CFR §1602.13.

The following types of records should be maintained in file separate from the employee's personnel file:

- **I-9 Records** – These records reflect national origin and/or citizenship status.
- **Insurance and Tax Records** – These may reflect marital status and the existence of dependents.
- **Family Medical Leave, Disability, and Accommodation Records** – These records reflect the employees' use of employee benefits and/or medical conditions or disabilities.
- **Detailed Payroll Records**
- **OR-OSHA 300 Log and Accident Reports Generally**<sup>29</sup> – These records may reflect worker's compensation status, confidential medical information, and/or disability status.
- **Grievance/Investigation Records** – These records may reflect the employee's opposition to harassment, discrimination, or other illegal conduct, or participation in the investigation of such conduct.
- **Security Clearance Data (Credit History/Criminal Records)** – Employees may not be excluded from consideration for employment based solely on a poor credit history or a criminal record unless it is relevant to the position sought.
- **Garnishment Records** – Employees may not be discharged based on the fact that their pay has been garnished.<sup>30</sup>
- **Drug and/or Alcohol Test Results**
- **Worker's Compensation Claims Records**<sup>31</sup>
- **Confidential, Attorney-Client Privileged Material**

---

<sup>29</sup> See OAR 437-001-0700 (14)(g) (requiring employers to refrain from entering an employee's name on the OSHA 300 Log in "privacy concern" cases, and requiring employers to keep a separate, confidential list of the case numbers and employee names for your privacy concern cases). "Privacy concern cases" are those involving an illness or injury to an intimate body part or the reproductive system; and illness or injury resulting from a sexual assault; mental illness; HIV infection, hepatitis, or tuberculosis; needlesticks or cuts from objects contaminated with blood or other infectious material; other illnesses if the employees requests that his or her name not be used on the log. Employers who voluntarily disclose the logs to third parties may be required to first remove personally identifying information.

<sup>30</sup> ORS 23.186(9).

<sup>31</sup> See generally, ORS 656.360 (insurers and their assigned claims agents shall maintain the confidentiality of worker medical and vocational claim records; worker medical and vocational claim records may not be disclosed to persons other than the worker unless the disclosure is within statutory exceptions).

- **Medical Information**

There are a number of federal and state laws that dictate the storage and use of and impose restrictions on access to employee medical information. Among these laws are ADA, FMLA, and their state counterparts, and the Health Insurance Portability and Accountability Act (HIPAA).

**B. Records Relating to Accommodation of Disabled Employees**

Both state and federal laws require employers to reasonably accommodate employees with disabilities.<sup>32</sup> As part of the accommodation process, employers often request and obtain information about an employee's medical condition. Both state and federal disability laws restrict the types of medical or health information an employer can obtain from employees and regulate how employers must keep such information. Specifically, employers are required to maintain an employee's medical condition or history "on separate forms and in separate medical files [that must be] treated as a confidential medical record \* \* \*." This law has been widely interpreted as requiring an employer to keep medical records in a separate, locked file cabinet and allow only limited access to it. Medical information may be disclosed to supervisors and managers as necessary to accommodate work restrictions or a disability, to first aid and safety personnel if the disability might require emergency treatment, and to state and federal agencies in connection with a compliance investigation.<sup>33</sup>

**C. Records Relating to the Use of Family and Medical Leave**

Both the FMLA and the Oregon Family Leave Law (OFLA) contemplate that the employer will request and obtain medical information about employees.<sup>34</sup> OFLA (applicable to employers of 25 or more employees) does not specifically address the confidentiality of medical records. FMLA (applicable to employers of 50 or more employees) has detailed regulations regarding the collection, use, and maintenance of such records.<sup>35</sup>

Medical information gathered for the purpose of administering FMLA must be "maintained as confidential medical records in separate files/records from the usual personnel files."<sup>36</sup> It is permissible to allow access to supervisors and managers with a need to know (*e.g.*, if the individual has a work-restriction), first aid or safety personnel, and government agencies.<sup>37</sup>

---

<sup>32</sup> Oregon employers with six or more employees must comply with the state law. *See* ORS 659A.100, *et seq.* Employers of 15 or more employees must also comply with federal law. 42 USC § 12111(5)(A).

<sup>33</sup> 29 CFR § 1630.14(c); ORS 659A.133(3)(c).

<sup>34</sup> 29 CFR § 825.305; OAR 839-009-0260.

<sup>35</sup> *See* 29 CFR § 825.500.

<sup>36</sup> 29 CFR § 825.500(g).

<sup>37</sup> *Id.*

## **D. Records Subject to the Health Insurance Portability and Accountability Act (HIPAA)**

HIPAA is a comprehensive federal law that protects the confidentiality of an individual's medical records under a wide array of circumstances.<sup>38</sup> The law became effective for most employers as of April 1, 2004.<sup>39</sup> The primary purpose of HIPAA's privacy regulations is to restrict the dissemination and use of individual medical records by insurance companies, group health plans, and health care providers (covered entities). Health information that identifies an individual, or provides enough specificity to create a reasonable basis to believe that the information would identify an individual, is considered protected health information or "PHI."<sup>40</sup> The law imposes onerous, detailed, and technical requirements with regard to the maintenance, use, disclosure, and transmission of PHI.

Not all employers are covered by HIPAA. Only employers that offer certain health plans will be subject to HIPAA's extensive requirements.<sup>41</sup> Employers that are excused from HIPAA's technical requirements experience the secondary effects of HIPAA when they seek medical information about their employees from insurers, health care providers, or group health plans. Covered entities are now more reluctant to provide the information and impose conditions on providing it.

The critical question for an employer, and the starting point for HIPAA compliance efforts, is determining whether the employer must comply with the full panoply of HIPAA requirements. To assist in this determination, The United States Department of Health and Human Services, the federal agency charged with enforcing HIPAA, has developed an on-line decision tree/questionnaire.<sup>42</sup>

Generally speaking, an employer will not be subject to HIPAA's more onerous provisions by merely maintaining worker's compensation insurance, life insurance, short or long term disability plans, or accidental death and dismemberment plans.<sup>43</sup> Among the benefits that will likely subject the employer to HIPAA are group health plans, HMOs, employee assistance plans, and medical flexible spending accounts.<sup>44</sup>

An employer is generally covered by HIPAA if it sponsors a health plan (including group health plans, as defined by another federal employee benefit statute<sup>45</sup>) for its employees, and the plan has 50 or more participants, or the plan has fewer than 50 participants and is administered by a third-party administrator. Self-funded plans that are self-administered and have fewer than 50

---

<sup>38</sup> HIPAA's privacy regulations appear at 45 CFR parts 160 and 164. HIPAA has been described as being even more complicated than the Internal Revenue Code. Accordingly, it is important to emphasize that this memorandum provides only a general overview of HIPAA that is intended to provide an introduction to certain aspects of the law.

<sup>39</sup> 45 CFR § 164.534.

<sup>40</sup> 45 CFR § 164.501.

<sup>41</sup> See generally, 45 CFR § 160.103.

<sup>42</sup> See [www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport](http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport).

<sup>43</sup> 45 CFR § 160.103.

<sup>44</sup> Id.

<sup>45</sup> See the Employee Retirement Income and Security Act of 1974 29 USC § 1002(1).

participants are not subject to HIPAA.<sup>46</sup> An employer with a fully-insured group health plan may or may not be subject to HIPAA's privacy requirements. If the employer has a fully-insured plan and does not receive or maintain any PHI, or if the employer has a self-funded plan but uses a third-party administrator and does not receive PHI, the employer is relieved of many of HIPAA's requirements.<sup>47</sup> Those requirements are, instead, borne by the insurer or third-party administrator. If, on the other hand, the employer has a fully-insured plan but wishes to have access to PHI, then the plan will be required to comply with the full range of HIPAA privacy requirements.<sup>48</sup>

If the employer maintains the type of plan that subjects it to HIPAA's privacy requirements, the employer must develop and implement certain procedures to ensure the confidentiality and appropriate use of PHI.<sup>49</sup> HIPAA's most fundamental requirement in this context is that PHI disclosed by the plan to the company must be handled by the plan sponsor, used only for limited purposes, and there must be a "firewall" (*i.e.*, a set of policies and procedures defining which employees may access PHI and for what purposes) between the plan sponsor and the employer.<sup>50</sup> The plan sponsor may not generally share PHI with the employer. For example, without the employee's authorization, the plan could not transmit an employee's PHI to the employer for the purpose of enabling the employer to evaluate the employee's worker's compensation claim.

## **VI. THE USE OF DOCUMENTATION IN LITIGATION**

Good documentation can make or break an employer in the event of a lawsuit. To appreciate why documentation is important, it is helpful to understand how documentation is used in connection with employment claims. The thrust of most discrimination, retaliation, and wrongful discharge claims is that the employer took adverse action against the employee for an impermissible reason (*e.g.*, because the employee was of a particular race, sex, or age, or because the individual asserted an employment related right, such as filing a worker's compensation claim). An employer's primary defense to such a claim is that the employer took the action for permissible reasons, such as poor performance or violation of work rules. Documentation can be critical in proving that the reason for a termination or other personnel action was a legitimate, non-discriminatory one, and not the illegal reason asserted by the employee.

When employees file lawsuits or administrative complaints against their employers, the first place the employee's lawyer will look for evidence is the employee's personnel file. Cases may be won or lost, or parties may be motivated to settle quickly, based solely on the contents of the personnel file or other documents kept by the company.

The kind of documentation that will prove important in any given litigation depends upon the type of claim asserted. For example, in a failure-to-hire case, there will be no personnel file, and the employer will have to rely on resumes, applications, written communications, interview notes, and verification or accreditation, licensing, and references to explain why an individual

---

<sup>46</sup> 45 CFR § 160.103.

<sup>47</sup> 45 CFR § 164.500.

<sup>48</sup> *Id.*

<sup>49</sup> 45 CFR § 164.102, *et seq.*

<sup>50</sup> 45 CFR § 164.504(f)(2).

was not hired. In connection with a reduction-in-force (RIF) or restructuring, documentation of the employer's need for the action taken, the selection criteria employed, and the employee's performance records will provide an explanation of who was selected for layoff and why. In circumstances where an employee with a spotless record is fired for a violation of company policy or misconduct, a personnel file is of no use, but a clear, written, employment policy or standard and the record of any investigation conducted are critical. In cases of discrimination where the company has discharged or failed to promote an employee, the critical documentation is ordinarily the employee's performance evaluations or other documentation of performance or misconduct.

An employee's performance history is extremely important when defending a discrimination claim. At a minimum, plaintiff-employees must be able to establish a "*prima facie*" case of discrimination. This requires proof that the employee is a member of a "protected class," applied for and was qualified for the job, got rejected, and the position remained open or was given to a less-qualified person not in the protected class. Although this *prima facie* test was designed for failure-to-hire cases, it has been adapted for use in discharge and failure-to-promote cases. Once the plaintiff makes out a *prima facie* case, the employer may still defeat the claim by showing a "legitimate, nondiscriminatory reason" for the personnel action. If the employer has such an explanation, the plaintiff must then show that the employer's explanation is "pretextual" or not worthy of belief.

Records of employee performance or misconduct are important for proving: (1) the employee was not "qualified" for the position sought, (2) the action was taken for a legitimate, nondiscriminatory reason, or (3) the action taken was consistent with action taken against other employees who were not in the plaintiff-employee's protected class. For example, in one case, an employer was able to show that an employee claiming age discrimination was not qualified for the job with documentation reflecting she was warned about the consequences of her failure to meet sales quotas, and her performance evaluations showed poor performance over a long period of time. An age discrimination claim was dismissed in another case based on performance evaluations showing the employer had repeatedly addressed the employee's slow processing of files and that the employee agreed with the criticism. One court dismissed a race discrimination claim where the plaintiff's performance ratings showed he was "marginal in almost all respects" for the first year, "nearly satisfactory" for the second year, and other documentation showed he was not punctual, failed to communicate, did not retain clean production areas, and made costly errors.

While performance records may be important in defeating the plaintiff's *prima facie* case by establishing that the individual was not qualified for the job, employers most often rely on such documentation to establish a "legitimate, nondiscriminatory reason" for the employment action. Performance records are routinely used in wrongful discharge litigation. To prevail on a wrongful discharge claim, the plaintiff must show that he or she was discharged for exercising a job-related right (*e.g.*, filing a worker's compensation claim or lodging a harassment complaint) or for complying with a public duty (*e.g.*, serving on a jury). In each type of case, the key question is why the employer discharged the employee. An employer that can point to a job evaluation or other documentation of poor performance or misconduct made prior to the employee's protected activity is much more likely to win than an employer that must rely solely on oral testimony.

It is important to keep in mind that an employee who files suit may be able to review not only his or her own personnel file, but the personnel files of other employees. The personnel files of other employees may be used to show that the employer was aware of past discrimination or harassment, that the plaintiff was more qualified for a promotion than the person who received it, or that the plaintiff was not treated the same as similarly-situated employees. For example, in a sexual harassment case, the accused harasser's personnel file may reveal that the employer was aware of the harasser's conduct and failed to take adequate steps to remedy the problem. An employee laid off in a reduction-in-force can use the performance evaluations of his or her peers to show the employer targeted a particular class of workers for layoff without regard to performance or qualifications.

In addition to discrimination and wrongful discharge cases, documentation is important in connection with many other types of employment claims. For example:

- **Wage Claims.** Payroll records and signed authorizations for payroll deductions can disprove a claim for making an unauthorized deduction or failing to pay all wages upon termination. Job descriptions are used to show that an employee is properly classified as exempt from overtime pay requirements. Attendance and payroll records are used to prove damages. Time records (which can include time cards, security records, computer log-in and log-out times, etc.) can be used to defeat claims for overtime and missed breaks.
- **Breach of Contract.** Offer letters, handbooks, and documents signed by the employee acknowledging at-will status are used to defeat a claim for breach of an employment contract for a specific term and/or that employment may be terminated only "for cause." Where termination is permitted only "for cause," or constitutional or internal policies require disciplinary procedures prior to termination, the employer will need documentation establishing that cause existed for termination and timely and proper procedures were followed.
- **Breach of Confidentiality and Non-Competition Agreements.** Employers seeking to enforce a confidentiality or non-competition agreement are more likely to prevail if the agreement is in writing. In Oregon, when the non-competition agreement was not presented sufficiently in advance of starting work, documentation showing that the agreement was signed upon a subsequent "bona fide advancement" will be crucial.
- **Discrimination and Harassment Claims.** An employer will be strictly liable for unlawful harassment, even when it does not result in a tangible, job-related injury (*e.g.*, discharge or failure to promote), unless the employer can show that it exercised reasonable care to prevent and promptly correct the harassing behavior, and the employee unreasonably failed to take advantage of any preventative or corrective opportunities provided by the employer. As a result, an employer is hard-pressed to defend a discrimination or harassment case without at least a written policy that prohibits discrimination and harassment in the workplace and provides for a complaint procedure. Other documents relevant to defending such a

claim would include diversity and harassment training materials, a list of attendees at any training session, complaints of policy violations, documentation of any investigations, and any disciplinary actions taken as a result.

- **Disability Claims.** Disability laws require employers to engage in an interactive process and provide reasonable accommodation to qualified individuals with a disability. Communications with the individual's health care providers (and records of any independent medical examination conducted) are used to determine whether the individual is "disabled" and entitled to protection under the law. Job descriptions are used to identify "essential functions" of the job and whether the individual is qualified to perform them. Documentation of the attempts made to identify and provide reasonable accommodation, including related communications with the disabled individual, is important to prove the employer complied with its obligations and that any breakdown in the process was attributable to the employee.
- **Family Medical Leave Claims.** Personnel and attendance records, and FMLA policies, forms, and medical certifications are used to show whether an employee requested and qualified for leave, whether the employer provided the required notice, whether the employee exceeded the amount of leave allowed and complied with the terms of the employer's call-in and notice requirements. Payroll and benefits records show whether the employee was paid properly during the leave period and upon returning to work.
- **Whistleblowing and Opposition Claims.** Detailed policies and procedures relating to the reporting of discrimination, harassment, or corporate wrongdoing may be used to show that a company took steps to prevent unlawful conduct from occurring and had procedures in place to report and correct it. Records of employee complaints or reports of wrongdoing and the company's efforts to investigate and resolve the issues may be used to show the company complied with its underlying obligations. The employer will need to rely on documentation of poor performance or misconduct to show that adverse action was taken against the employee for legitimate reasons.

## VII. PRESERVATION AND RETENTION OF DOCUMENTS IN LITIGATION

Parties in litigation are entitled to request production of documents deemed relevant to any claims or defenses asserted. "Discovery" is the process by which the parties to a lawsuit exchange information about each other's claims and defenses.

"Electronic discovery" refers to the litigants' requests for documents that are stored in electronic form. Electronic discovery requests routinely require production of files residing on laptops, office PCs, network servers, floppy disks, personal digital assistants (PDAs), CD-ROMs, MP3 players, Blackberries, cell phones, pagers, backup tapes, flash memory cards and devices, and other archive media. Electronic discovery also refers to metadata or digital "fingerprints" that, with the assistance of computer forensics, can be used to determine background information

regarding when electronically-stored documents were created, modified, sent, viewed, etc. This information is often more important than the substance of the document itself.<sup>51</sup>

When litigation is threatened or pending, it is critical to preserve the integrity of all files, both hard copy and electronic.<sup>52</sup> The duty to preserve evidence arises as soon as the organization becomes aware of facts or circumstances suggesting that litigation is imminent or should otherwise be expected, which could occur long before a formal complaint is served. For example, an employee's statement that he/she intends to sue, or receipt of a demand letter or agency charge should trigger a litigation hold.

The intentional destruction of evidence (called "spoliation") is illegal. Even purely inadvertent destruction of evidence will be viewed as suspect. Therefore, all documents that could have any bearing on the lawsuit should be maintained in their original state (*i.e.*, unaltered, in the same file folders or storage location).<sup>53</sup>

As part of a document retention policy, it is useful to designate a litigation response team that will be responsible for preserving documents, halting any routine or planned document destruction (including email), and alerting employees to the necessity of preserving all relevant documents. To insure that no files are inadvertently altered or destroyed, it is wise to include a procedure for advising employees who may have custody or control of relevant documents of their obligation to preserve these documents during the litigation (typically referred to as a "litigation hold"). The failure to have an established procedure for managing electronically stored information in anticipation of and during litigation increases the risk of inadvertent destruction, which can result in monetary sanctions and/or an adverse instruction from a court.<sup>54</sup>

---

<sup>51</sup> For example, in *Lee v. Oracle Corp.*, 1999 WL 595455 (Cal App 1999), an Oracle employee, Adelyn Lee, successfully sued Oracle for wrongful termination, claiming that she was fired by her supervisor after she refused to have sex with Oracle CEO Larry Ellison. During the discovery process, Oracle's lawyers found an email in which Lee's supervisor told Ellison "I have terminated Adelyn per your request." Although Oracle settled immediately for \$100,000, Lee's supervisor insisted that he never sent the email. By using forensic analysis to determine when and how the email was created, Oracle later was able to show that Lee had broken into Oracle's computer system, accessed her supervisor's email using his password, and forged the email. Oracle successfully sued Lee for perjury and falsification of evidence.

<sup>52</sup> A government investigation or audit, as well as certain business events, such as a merger or acquisition, or bankruptcy, may also require a suspension of the normal document destruction procedures.

<sup>53</sup> Some employers routinely remove and store the hard drive of every employee who leaves the company. For some employers, it may be desirable to engage a vendor that specializes in electronic discovery to insure that electronic data is not altered in the process of copying and/or storage.

<sup>54</sup> The prominence of electronic discovery resulted in a change in the Federal Rules of Civil Procedure that took effect in 2006. For a more comprehensive discussion of these changes, see the Ater Wynne Employment Group Roundtable Memo from 2006 entitled *Electronic Discovery*, [http://www.aterwynne.com/files/ERT\\_%20Electronic%20discovery.PDF](http://www.aterwynne.com/files/ERT_%20Electronic%20discovery.PDF).