

Privacy In the Workplace Is There Any?

2005

Employment Practices
Conference

California
CPA Education Foundation

November 14 & 15, 2005

In Northern California

Michael A. Futterman, Esq.

Futterman & Dupree LLP
160 Sansome Street, 17th Floor
San Francisco, CA 94104

Phone: (415) 399-3840

Fax: (415) 399-3838

mfutterman@dfdlaw.com

In Southern California

Mark E. Terman, Esq.

Reish Luftman Reicher & Cohen
11755 Wilshire Blvd., 10th Floor
Los Angeles, CA 90025

Phone: (310) 478-5656

Fax: (310) 478-5831

markterman@reish.com

SOUTHERN CALIFORNIA MATERIALS

Michael A. Futterman, Esq.

Michael Futterman is a founding partner in the law firm of Futterman & Dupree LLP in San Francisco. Mr. Futterman has broad experience in all areas of employment law, including discrimination, harassment, wrongful termination, disability rights, wage and hour, and similar issues. He also serves as corporate counsel for a wide variety of closely-held for-profit and nonprofit businesses, with expertise in the areas of corporate governance, transactions, contracts and related business issues. Mr. Futterman is fluent in French, and regularly represents French nationals doing business in the United States. He is a member of the California Bar, and is a frequent speaker for the California CPA Education Foundation.

In 2004 and 2005, Mr. Futterman was recognized by his peers in the Northern California legal community as a "Super Lawyer." Approximately 5% of the Northern California Bar received the distinction. In 2002, he served on the California Chief Justice's Blue Ribbon Panel on Arbitrator Ethics. Mr. Futterman is a Trustee of the Larkspur School District, and serves on the board of directors of various Bay Area non-profit organizations.

Mr. Futterman earned his juris doctorate in 1983 from University of California at Davis School of Law (King Hall), where he served as editor of the *Law Review*. He earned his bachelor's degree in 1980 from University of California at Los Angeles. Please see www.dfdlaw.com.

Mark E. Terman, Esq.

Mark Terman is a partner with Reish Luftman Reicher & Cohen where he heads the firm's Employment Law Practice Group. He counsels employers in claim prevention, hiring, policy, crisis, and discipline and termination matters, and represents them in federal and state court, arbitration and government proceedings. Mr. Terman's employment litigation experience extends to wrongful termination, discrimination and sexual harassment, trade secret, fraud and other business torts. He is general counsel for the UCLA Alumni Association and is a member of its Board of Directors, and a former member of the Board of Directors of the Children's Nature Institute.

Mr. Terman served as a Superior Court appointed arbitrator in some 25 cases. His peers selected him as a 2004, 2005, and 2006 California "Super Lawyer", in which some 65,000 California lawyers were polled for each year. Mr. Terman speaks to and writes for client and industry groups on litigation avoidance and management, wage and hour issues, trade secret protection, and avoiding sexual harassment, among other employment law topics. He chaired the California CPA Education Foundation's Employment Practices Conference for four years, is a member of CalCPA's Human Resources Subcommittee of the Statewide MAP Committee, and is on CAMICO's panel of employment defense counsel.

Mr. Terman earned his juris doctorate in 1983 from Loyola Law School, where he served on the *Law Review*. In August 1986, he attended Hasting College of Law as an attorney for jury trial training. He earned his bachelor's degree in 1979 from University of California at Los Angeles. Please see www.reish.com.

PRIVACY – IS THERE ANY?

A. Legal Basis for Right to Privacy

1. California Constitution – Article 1 (includes private right of action against private employers), as amended in 1972 to add right of privacy.
 - a. “[a]ll people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing and protecting property, and pursuing and obtaining safety, happiness *and privacy*.”
 - b. Election brochure stated that “The right to privacy is more than ‘unnecessary wordage.’ It is fundamental to any free society ... This simple amendment will *extend various court decisions* on privacy to insure protection of our basic rights.” (emphasis in original).
 - c. Right to privacy is based upon an individual’s reasonable expectation of privacy. *Hill v. NCAA*, 7 Cal.4th 1 (1994). The court balances that right against the justification for the invasion of privacy. *Loder v. City of Glendale*, 14 Cal.4th 846 (1997) (analyzing pre-employment drug testing of all applicants by City of Glendale).
 - d. All employees have a right to privacy; however, the courts must balance:
 - i. the employee’s expectation of privacy at work against the employer’s need to regulate the conduct of its employees at work; and
 - ii. whether less intrusive means can accomplish the employer’s legitimate objectives.
2. Federal – U.S. Constitution -- Only government employees have a reasonable expectation of privacy at work.
3. Common Law.
 - a. Invasion of privacy claim.
 - i. Is there an invasion of privacy? 3-part test:
 1. a legally protected privacy interest;
 2. a reasonable expectation of privacy in the circumstances; and

3. conduct by defendant constituting a serious invasion of privacy.

Loder v. City of Glendale, 14 Cal.4th 846, 891 (1997)

- ii. If elements of invasion are present, may still not constitute actionable invasion.
 1. "Conduct alleged to be an invasion of privacy is to be evaluated based on the extent to which it furthers legitimate and important competing interests" (balancing test).
 2. "For example, if intrusion is limited and confidential information is carefully shielded from disclosure except to those who have a legitimate need to know, privacy concerns are assuaged. On the other hand, if sensitive information is gathered and feasible safeguards are slipshod or nonexistent, or if defendant's legitimate objectives can be readily accomplished by alternative means having little or no impact on privacy interests, the prospect of actionable invasion of privacy is enhanced."

Hill v. NCAA, 7 Cal.4th 1, 38 (1994).

- b. Other Common Law privacy rights. -- E.g., unreasonable intrusion upon seclusion, public disclosure of private facts, false light privacy, appropriation of name and likeness

B. Contexts Where Privacy Issues Arise

1. Questions in job applications and hiring interviews.
2. Pre-employment investigations.
3. Physical or medical examinations of employees or applicants.
4. Investigations to determine whether employee violated employer policies.
5. Everyday.

C. Background Checks and Investigations

1. California Investigative Consumer Reporting Agencies Act (ICRAA).
 - a. Statutory Coverage – Cal. Civ. Code § 1786 *et seq.* See Cal. Civ. Code § 1786.50.

b. Substantive Rights and Responsibilities.

- i. Requires employers who receive public records about job applicants and employees, whether in written or oral form, to provide a copy of that information to the subject of the background check within seven days after the employer's receipt of the information. Cal. Civ. Code § 1786.53(b)(1).
- ii. Public records are defined by the Act as records documenting arrest, indictment, conviction, civil judicial action, tax lien and outstanding judgment.
- iii. If public records are obtained at the pre-employment stage, they are to be provided to the job applicant within seven days of the firm's receipt of them.
- iv. The seven-day requirement is suspended when the employer is investigating "suspicion of wrongdoing or misconduct" by a current employee until completion of the investigation. Then, the information must be provided within a reasonable time even if the results of the investigation are favorable to the employee. Cal. Civ. Code §§1786.53(b)(3) and (b)(4).
- v. At least 8 business days is "reasonable." *Moran v. Murtaugh Miller Meyer & Nelson*, 126 Cal App 4th 323 (2005).
- vi. An employee may waive his or her rights to that information (which is often included in pre-employment waiver forms) and the investigative information need not be turned over, unless adverse employment action (e.g., demotion, termination, etc...) is taken as a result of that information. Cal. Civ. Code §1786.53.
- vii. Damages – Greater of actual damages or \$10,000, attorney fees, plus punitive damages if grossly negligent or willful violation. Cal. Civ. Code §1786.50.

2. California Consumer Credit Reporting Agencies Act (CCRAA).

- a. This is a complex area of law. Consult an attorney, HR professional or licensed investigator.
- b. Statutory Coverage - See Cal. Civ. Code § 1785.1 *et seq.*
 - i. Applies to consumer credit reports but not to investigative reports (i.e., interviews of friends or neighbors)
- c. Substantive Rights and Responsibilities.

- i. Before requesting a consumer credit report, employer must provide written notice to the person involved (employee or prospective employee).
- ii. Notice document must have a box to check to allow person to receive a copy (to be requested by employer from agency at no charge to employee).
- iii. If employee has placed a security freeze on credit report, employer will need a written authorization or request by the employee to the credit reporting agency to lift the freeze for employer's inquiry in order to obtain report.
- iv. Employers are prohibited from giving credit information to an employee's creditors. Cal. Civ. Code Section 1785.20.5. Employment verification requests from creditors are common. Employers should insist that the employee sign giving consent to any such request.
- v. CCRAA provisions overlap with FCRA (see below); FCRA governs in case of conflict unless CCRAA provision is more beneficial to consumer.

d. Method of Enforcement.

- i. If employer takes an "adverse action" against employee or prospective employee (i.e., does not hire or promote, terminates) as a result of information in a credit report, employer must.
 - 1. Provide written notice of the adverse action to the consumer.
 - 2. Provide consumer with name, address & telephone number of the reporting agency.
 - 3. State the adverse action was taken based on information in the report.
 - 4. Provide consumer notice of right to receive a copy of the report and to dispute the accuracy or completeness of the report.
- ii. Action for damages.
 - 1. Consumer who suffers actual harm as a result of employer's negligent use of a credit report may sue for damages, court costs, attorney's fees and pain and suffering.

2. For a willful violation, consumer may recover above plus punitive damages of not less than \$100 nor more than \$5000 for each violation.

3. Two year statute of limitations.

3. Federal Fair Credit Reporting Act (FCRA).

a. This is a complex area of law. Consult an attorney, HR professional or licensed investigator.

b. Statutory Coverage – 15 USC § 1681 *et seq.*

i. Generally applies to report by a consumer reporting agency bearing on a consumer's credit, character, general reputation, personal characteristics, or mode of living which is to be used as a factor in determining a person's eligibility for credit or employment.

ii. Generally does not apply if report obtained by employer in connection with investigation of misconduct or criminal activity by employee.

c. Substantive Rights and Responsibilities.

i. Before requesting a consumer credit or investigative report, employer must provide clear and conspicuous disclosure to the person involved (employee or prospective employee).

1. Disclosure must be separate document (not contained within employment application or other document).

ii. Employer must obtain written authorization from the employee.

iii. If report will be **investigative** (i.e., character, general reputation, personal characteristics, or mode of living through personal interviews with neighbors, friends, or associates), additional disclosures are required.

iv. If adverse action taken based on report, employer must disclose a summary of the nature and substance of information relied upon.

d. Method of Enforcement.

i. Criminal penalties.

1. Violation must be knowing and willful; report obtained under false pretenses.
2. Penalties: fine, imprisonment for not more than two years, or both.

ii. Civil liability.

1. Willful noncompliance.
 - a. Employee/applicant's actual damages.
 - b. Punitive damages as allowed by the court.
 - c. Attorney's fees and costs.
2. Knowing noncompliance of report obtained under false pretenses or for improper purpose.
 - a. Liability is to the credit reporting agency, for the agency's actual damages or \$1000, whichever is greater.
3. Negligent noncompliance.
 - a. Employee/applicant's actual damages.
 - b. Attorney's fees and costs.

iii. Statute of limitations.

1. Earlier of
 - a. Two years from discovery of the violation; or
 - b. Five years from the date of the violation.

4. Employer Data Collection, Searches and Surveillance of Employees.

- a. Polygraph and Lie Detector Tests.
 - i. Cannot demand or require an applicant for employment or any employee to take a polygraph, lie detector or similar test as a condition of employment or continued employment. Cal. Labor Code § 432.2. (Statute does not apply to federal, state or local governments, but compulsory tests for certain state and local

employees prohibited by Gov. Code §§ 3301, 3307). Also, there are many federal restrictions.

- ii. However, OK to ask a person to take such a test if employer first advises person in writing if his or her right to refuse to take the test.
 - iii. If polygraph is taken voluntarily, and damaging information is revealed, OK to refuse to hire applicant or take disciplinary action. 43 Ops. Atty. Gen. 25, 27 (1964).
 - iv. *CAUTION* – Easy for employee to claim duress.
 - v. Federal law has similar provisions. 29 U.S.C. Section 2001-2009. Federal law exceptions do not apply in California (e.g., applicants for security guard jobs; employees involved in manufacture, distribution, or dissemination of controlled substances).
- b. Voice Stress Analysis – Not allowed without written consent given by employee prior to examining or recording. Cal. Penal Code § 637.3
- c. Fingerprints and Photographs.
- i. Lawful for employer to require fingerprints and photographs of employees as condition of hiring or retention.
 - ii. BUT employer must carefully safeguard fingerprints and/or photographs and cannot furnish them to another employer or third person who uses them to employee's detriment. Misdemeanor. Cal. Labor Code § 1051.
 - iii. Limited statutory exemptions for industries and agencies required to obtain fingerprint clearance of employees (i.e., banks, securities dealers, child care centers).
- d. Wiretapping and Eavesdropping. Cal. Penal Code § 630.
- i. California Privacy Act (Cal. Penal Code § 631, et. seq.) prohibits eavesdropping and recording of confidential communications by means of an electronic amplifying or recording device.
 - 1. Prohibits listening in on a phone call unless all parties consent.
 - 2. Has not been held to by the court to restrict employer access to gather information recorded on its own computers, e-mail, voice mail systems.

- ii. Federal Electronic Communications Privacy Act (18 USC § 2510, et seq.). Employers who provide the communications service (i.e., computers and phones) are exempt from the Act's prohibition of unauthorized access to or retrieval of electronic communication while it is in storage.
 - 1. "Business Extension" exception. Must be in ordinary course of business." business calls vs. personal calls.
 - 2. Restrictions more lenient for stored communications.
 - iii. The federal Wiretap Act and Patriot Act do not prevent the employer from access to stored email, data and voicemail either.
 - iv. May give advance notice to employees and then randomly place calls to employees by persons claiming to be customers to rate accuracy, courtesy and responsiveness of employee.
- e. Audio and Video Recording/Surveillance.
- i. Apply privacy test: Is there a legally recognized privacy interest? Is the intrusion warranted and narrowly tailored to accomplish its purpose?
 - ii. CANNOT make audio or video recording of restroom, locker room or room designated for changing clothes without a court order. Cal. Labor Code § 435. Cannot use information obtained in violation of this section for any purpose. (Does not apply to federal government.)
- f. Desk Drawers or Lockers Where Personal Effects are Typically Stored
- i. Legitimate work-related purpose.
 - 1. Work-related.
 - a. Ordinary part of daily work.
 - i. Reasonable suspicion of
 - 1. Misconduct.
 - 2. Risk to health and safety of workforce.
 - 3. Risk to security of premises.
 - b. Not a proxy for law enforcement who need a warrant.

- ii. Reasonable suspicion of specific employees and/or misconduct.
 - 1. Reasonable basis to believe that the search will reveal evidence of work-related misconduct.
 - 2. The scope of the search is a reasonable way to obtain the evidence and it is not too intrusive given the severity of the suspected misconduct.
 - iii. Reasonable expectation of privacy.
 - 1. Employer property used exclusively by employee – generally lower.
 - 2. Employee property brought onto employer premises – generally higher.
 - iv. Some areas may be more private than others and a greater level of work related purpose may be needed.
 - 1. Compare: open area work station vs. office, open vs. locked office; shared vs. exclusive unlocked desk; locked/unlocked locker; briefcase/backpack/handbag; lunch boxes; tool kits; pockets.
 - 2. Ways to reduce expectation of privacy. Policies and practices that notify employees that searches will occur for work-related purposes.
 - a. Written policy recites the work-related purpose and employees sign acknowledgement of receiving and reading the policy/notices.
 - b. Include specific examples of areas subject to search.
 - c. The company has a practice of conducting searches in the past.
 - d. Applied uniformly.
- Compare:
- i. *Schowengerdt v. General Dynamics Corp.*, (9th Cir. 1987) 823 F.2d 1328, 1335 (damages action permitted where employee had reasonable expectation of privacy of materials in a locked desk where no advance notice or policy given)

ii. *Law Enforcement Employees District Council 82 v. Carey*, (2d Cir. 1984) 737 F.2d 187 , 202 (handbook provision warning employees that they were subject to search diminished employees' reasonable expectation of privacy in personal belongings).

- e. Supply any lock used on company property and prohibit employees from using their own locks
- f. Maintain keys to each company owned desk, locker, vehicle and notify employees in writing of same
- g. Ask for consent.

3. Confidentiality of Search Results

- 1. Should be limited to those who have a need to know.
- 2. Defamation, intentional infliction of emotional distress and other claims risks vs. making an example out of the violator.

g. DO NOT restrain the employee, "imprison" or physically detain (i.e., impede their ability to leave), get into a physical fight with employee, etc.

D. Computers, E-mail and Offices

1. Data/Equipment (Computers, Email, Telephones & Voicemail, Internet Usage)

- a. How the Courts are balancing competing employer and employee interests.
 - i. Legitimate work related reasons for monitoring or search.
 - ii. Employers need to know increases with severity of alleged misconduct.
 - iii. Employer's published policies will usually defeat an employee's expectation of privacy.
- b. Employer's written technology and internet policy.
 - i. Why employers should have one.
 - 1. Not required by law; but, probably will be soon.

2. Deterrence of misconduct.
3. Public relations with employees.
4. Will give employer the best defense against a claim of invasion of privacy.

ii. Key elements.

1. The computers and everything on the system - files and software are the employer's property.
2. Use is permitted for work purposes only or personal use is limited purposes/times.
3. Employer's right to inspect and monitor at any time and employee's passwords do not ensure privacy and employers can override the passwords.
4. No reasonable expectation of privacy when using employer owned equipment.
5. The policy against discrimination and sexual harassment applies – no defamatory, profane, obscene, discriminatory or harassing materials are to be sent or received.
6. Treat e-mail as if it is a permanent record – think about the contents before it is sent.
7. Confidential, proprietary or trade secret information should not be sent unless necessary to carry out the employer's business.
8. Violation of policy will lead to serious discipline up to and including termination.

See TBG Ins. Services Corp. v. Superior Court, 96 Cal.App.4th 443 (2002) (upholding employer's right to terminate employee for using employer-supplied home computer for access to pornographic websites. Employee had signed employer's "electronic and telephone equipment policy statement" which diminished the employee's expectation of privacy).

The employers' policy stated explicitly:

- The company's computers are to be used solely for company business;

- The company reserves the right to monitor the employee's use of company computers, including but not limited to the employee's use of the Internet and e-mail;
- The company keeps copies of all computer passwords and the existence of such passwords does not guarantee the confidentiality of any electronic communications;
- The transmission of any discriminatory, offensive or unprofessional messages is strictly prohibited;
- Access to any discriminatory or offensive Internet sites is strictly prohibited; and
- Employees are prohibited from using company equipment to post personal opinions on the Internet, especially if the opinion is discriminatory, political or offensive in nature.

Id. at 451-52.

- iii. Sample policy ATTACHED.
- iv. Train management and employees.

E. Off-Duty Conduct

1. Effective January 1, 2000, California Labor Code § 96k authorizes the California Labor Commissioner to pursue wage claims against employers for demotions, suspensions, or discharges based on an employee's "lawful conduct" occurring during nonworking hours away from the employer's premises.
2. "Lawful conduct."
 - a. Not defined in the statute.
 - b. Legislature's findings.
 - i. Individual employees are "ill-equipped" and "unduly disadvantaged" in any effort to assert their civil rights—life, liberty, property, safety, happiness, and privacy—as guaranteed by Article I of the California Constitution.
 - ii. Allowing any employer to deprive an employee of any constitutionally guaranteed civil liberties, regardless of the rationale offered, is not in the public interest.

- iii. Necessary to further the state's interest in protecting the civil liberties of individual employees who would otherwise be unable to protect themselves.

3. Untested in Appellate Courts.

- a. Could be a basis for a wrongful discharge in violation of public policy claim.
- b. Employer regulation of off-duty conduct would likely be limited to their most important business interests. For example: health and safety of workers and workplace; conflict of interest; competition; protection of trade secrets and other business assets.
 - i. Example: general anti-moonlighting policy vs. a policy that prohibits working for a competitor or vendor.
 - ii. Example: low level employee vs. senior executive.

4. Employee relationships.

- a. Personal Relationships. Employers are prohibited from discriminating on the basis of marital and registered domestic partner status. However, employers may refuse to place both spouses/partners in the same department, division, or facility if the work involves potential conflicts of interest or other hazards that are greater for married couples. Cal. Gov. Code § 12940(a)(3). Employers are also prohibited from discriminating on the basis of sexual orientation. Cal. Gov. Code § 12940(a)(3).

Example: *Rulon-Miller v. International Business Machines Corp.*, 162 Cal.App.3d 241(1984), an employee was discharged because of her romantic relationship with a former co-worker who had gone to work for a competitor. The court agreed that an employee could be terminated because of a conflict of interest, but held that the question of whether a particular set of circumstances presents such a conflict is one for the jury.

- b. No dating policy. See *Barbee v. Household Automotive Finance Corp.*, 113 Cal.App.4th 525 (2003) (upholding termination of employee for violating company policy restricting dating where employee could not prove a reasonable expectation of privacy in pursuing an intimate relationship with subordinate because of employer's legitimate reasons to restrict such conduct).

F. Electronic Data in Litigation

1. Not just financial and accounting information.
 - a. Includes e-mail, voicemail, video mail, word processing, groupware systems, spreadsheets, databases, CAD, websites, and security systems.
 - b. Discovery of electronic evidence in litigation is becoming more common, not just in high-profile cases.
 - c. Some attributes of electronic evidence.
 - a. Much more of it than paper documents and files.
 - b. E-mail volume and candor.
 - c. More opportunity to find a “smoking gun.”
 - d. Prior consistent or inconsistent versions and drafts.
 - e. Date/time stamps versions, record creation, edit and access.
 - f. The delete button does not mean it’s gone forever.
 - i. Electronic information and versions are stored in multiple places inside and outside company walls.
 - ii. Information thought to be deleted or lost can often be retrieved by experts.
2. Shield and Sword – a litigant can oppress and be oppressed with the time and expense of electronic discovery.
3. Record Management.
 - a. Retention policies must include all forms of electronic information.
 - b. Ensure that delete means delete in appropriate cases.
 - c. Every business will be hit with a discovery request or subpoena that includes electronic records - be prepared.
 - d. Litigation risks from not suspending routine record destruction policy when info is relevant to imminent or pending litigation.
 - i. California Evidence Code § 413 permits the trier of fact to consider a party’s “willful suppression of

evidence,” when it determines “what inferences to draw from the evidence or facts in the case against a party.”

- ii. Standard “BAJI” jury instruction No. 2.03 (8th ed. 2001 Revision) permits the jury to “consider the fact that a party willfully suppressed, altered, damaged, concealed, or destroyed evidence to prevent its being presented in this trial when determining what inferences to draw from the evidence.”
- iii. Trial courts may adapt the instruction “to fit the circumstances of the case, including the egregiousness of the spoliation and the strength and nature of the inference arising from the spoliation” *Cedars-Sinai Med. Ctr. v. Superior Ct.* (1998) 18 Cal. 4th 1.12.
- iv. California Code of Civil Procedure § 2023 (h) permits courts to impose various sanctions “against anyone engaging in conduct that is a misuse of the discovery process,” including:
 - (1) A monetary sanction.
 - (2) An issue sanction ordering that designated facts shall be taken as established in the action in accordance with the adversely affected party’s claim.
- e. Courts base decisions regarding the wrongfulness of evidence destruction on the “temporal proximity between the destruction and the litigation interference and the foreseeability of the harm to the nonspoliating litigant resulting from the destruction” *Willard v. Caterpillar, Inc.*, (1995) 40 Cal. App. 4th 892, 922-923.
- f. A party guilty of intentionally destroying relevant evidence can be subjected to criminal prosecution with maximum punishment of six months in jail and \$1,000 fine. Penal Code § 135.
- g. The existence of a routine document retention policy can influence whether a court gives the jury an adverse inference instruction when a company destroys potentially relevant evidence pursuant to the policy. Several factors are relevant to that inquiry *Willard v. Caterpillar, Inc.* (1995) 40 Cal. App. 4th 892, 922-923:

- i. Whether the policy's retention times were reasonable, considering the facts and circumstances surrounding the relevant documents;
 - ii. Whether the policy was instituted in bad faith;
 - iii. Whether lawsuits concerning a complaint or related complaints have been filed; and
 - iv. The frequency and magnitude of such complaints.
- h. Document Retention Policies:
 - i. Actually involve the routine destruction of documents.
 - ii. Establish reasonable timetables for retaining documents before destruction based on legal and practical.
 - iii. Must be written, widely disseminated and known by employees, and regularly enforced.
 - iv. If properly followed, can shield a company from negative inferences or defaults due to destruction of documents.
 - v. If the party knows or should know that particular documents will become material at some point in the future, such documents should be preserved. (e.g., documents related to "complaints" should be retained for a longer period because of the potential for litigation, relevant to the documents).
- i. Selected Record Retention Requirements
 - i. All are extended for duration of a claim or litigation on the subject.
 - ii. Recruitment, Hiring and Job Placement Records and Personnel files -- 2 years California Fair Employment and Housing Act; Title VII federal Civil Rights Act and ADEA; Americans with Disabilities Act.
 - iii. Payroll Records – 4 years – California Unemployment Insurance Codes; federal Fair Labor Standards Act.

- iv. Employee Wage Records – 3 years – California Labor Code; FLSA.
- v. I-9 Forms – later of 3 years after hire or 1 year after termination – Immigration Reform and Control Act.
- vi. Affirmative Action Programs – 5 years -- Title VII; Executive Order 11246.
- vii. Employee benefits data – 6 years -- (e.g., ERISA plan related documents, COBRA documents) – ERISA.
- viii. Workplace First Aid (where one day or more of work was lost) and Drug and alcohol test records – 5 years (toxic exposure and chemical safety records – 30 years – OSHA; Cal-OSHA).

G. Examination and Testing

1. Medical and Physical Examinations.

- a. Must be job related and consistent with business necessity and all entering employees in the job classification must be tested. Cal Gov. Code § 12940(E).
- b. Cannot charge the employee for the any testing (physical, medical, drug, etc...). Cal. Labor Code §§ 222.5, 231.
- c. Before deciding to test and what decisions are to be made with its assistance, analysis is needed under the federal Americans with Disabilities Act and the California Fair Employment and Housing Act (e.g., abilities needed to perform the essential functions of the job, reasonable accommodation, etc...).
- d. Employer must refrain from pre-employment medical questions or examinations until all other pre-employment contingencies have been removed. Specifically, employer needs to make offer of employment, complete reference checks, background investigations, etc., before requiring that applicants submit to job-related physicals.
- e. See *Leonel v. American Airlines, Inc.*, 400 F.3d 702 (9th Cir. 2005). Plaintiffs applied for flight attendant positions. Given conditional offers of employment contingent on background checks and medical examinations. Immediately upon receipt of offer they were sent to an on-site medical department, where they filled out medical questionnaires and gave blood samples. They did not fill out consent forms, nor were applicants told the purpose of the blood test. Blood tests showed applicants were HIV - positive, which was confirmed by their doctors. Employer withdrew the

offers. Employees sued, alleging violation of ADA, FEHA and right of privacy under California Constitution.

f. HOLDING:

- i. This violated ADA and FEHA because medical examination and inquiries only allowed after a “real” job offer, meaning that employer must either (a) have completed all non-medical components of the application process, or (b) be able to demonstrate that it could not reasonably have been expected to do so before issuing the offer.
- ii. Privacy – plaintiff stated a claim under privacy clause of California Constitution because (a) the drawing and testing of blood implicates a legally protected privacy interest, (b) the conduct of the test amounts to a serious invasion of the privacy interest, and (c) although applicants did not have a reasonable expectation of privacy that would prevent the drawing of blood, they did not give consent for any and all medical tests to be run on the samples (and may have been given misleading information re testing).

2. Psychological Tests.

- a. Legitimate work-related basis?
- b. Pre or Post offer of employment?
- c. MMPI considered “medical” exam and must therefore only be given post-job offer. *Karraker v. Rent-A-Center Inc.*, (7th Cir. U.S.C.A ., No 04-2881, June 14, 2005)
- d. Caution to use tests properly validated and in compliance with EEOC guidelines.
- e. Avoid privacy and discrimination traps – e.g., sexual orientation, religious beliefs, etc.

3. Drug and Alcohol Tests.

- a. No federal or state statutes that generally prohibit drug and alcohol testing. Therefore, same rules applicable to medical exams apply here.
 - i. However, local ordinance may restrict testing. For example, San Francisco “worker privacy” ordinance prohibits testing unless:
 1. Employer has reasonable grounds to believe employee’s faculties are impaired on job;

2. Employee's impairment presents clear and present danger to physical safety of employee, another employee or member of public; and
 3. Employee is given opportunity, at employer's expense, to have test done by state-licensed independent lab and provides employee with reasonable opportunity to rebut or explain results. See S.F. Police Code § 3300A.5
- b. Balancing Test: Balance privacy against "legitimate and important competing interests." *Loder v. City of Glendale*, 14 Cal.4th 846, 896-98 (1997) (applies balancing test to determine when it is permissible to use drug testing to maintain a workplace free of substance abuse).
- i. Urinalysis –
 1. Privacy right applies to *act* of urination, which is a private act. So, any third person observing the act implicates a privacy interest.
 2. Privacy right applies to *testing*, because it may reveal private information such as presence of prescription drugs, and certain medical conditions, such as pregnancy, unrelated to use of illicit drugs.
 - ii. *Loder* – drug testing by employer requiring persons to give urine sample under surveillance, uses sample to acquire information about person's physical state, and requires individual to disclose medications being used, "clearly intrudes on both autonomy privacy interests and informational privacy interests which are protected by the state Constitution." *Id.* at 896.
 - iii. Random off-duty drug tests found to violate right to privacy. *Edgerton v. State Personnel Board*, 83 Cal.App.4th 1350 (2000) (off-duty random tests of CalTrans workers violated reasonable expectations of privacy of workers. On-duty testing OK).
- c. FEHA and ADA do not prohibit drug or alcohol testing.
- i. State regulations expressly exclude alcoholism and narcotics addiction from definition of physical disability. 2 Cal. Code Regs. § 7293.6(a)(4).
 - ii. *Loder* found that nothing in FEHA or ADA restrict testing of job applicant to determine existence of illicit drug use.

- d. Applicants vs. Employees.
 - i. All applicants can be tested post job offer if job related and consistent with business necessity and all entering employees in the job classification must also be tested.
 - ii. Existing employees only on reasonable suspicion.
 - 1. However, certain positions subject to mandatory drug/alcohol testing under law (e.g., commercial motor vehicle operators).
- e. Sample drug and alcohol in the workplace policy ATTACHED.
- f. Drug Screening Program – prudent steps for employer to take:
 - i. Identify nature problem testing is designed to address.
 - ii. Design program narrowly to address that problem.
 - iii. Screening should be part of broader anti-substance abuse program.
 - iv. Publicize program before it begins, and obtain written consents from employees before testing.
 - v. Have screening done by independent, reputable third party labs.
 - vi. Focus on use of illegal drugs, not legal medications.
 - vii. Keep test results confidential.
 - viii. Confirm accuracy of test results before taking action.
 - ix. If there is a performance problem, consider taking disciplinary action before testing.
- g. Rehabilitation – Employer has duty to accommodate employee in alcohol or drug rehabilitation program. Cal. Labor Code § 1025 et seq.
 - i. Private employer that regularly employs 25 or more persons must reasonably accommodate any employee who wishes to voluntarily enter an alcohol or drug rehabilitation program, provided it does not impose undue hardship on employer.
 - ii. Employer has statutory obligation to keep confidential the fact that employee is in a rehabilitation program.

- iii. Compensation while in rehabilitation is not required, but employee may use sick leave.

H. Criminal Records

1. Job applications and pre-employment interviews should inquire whether the applicant has been convicted of a felony or serious misdemeanor.
2. California Labor Code Section 432.7 prohibits employers from inquiry about, or use for employment related decisions.
 - a. Arrests or detentions that did not result in a conviction (other than an arrest for which the applicant or employee is currently awaiting trial),
 - b. Convictions for certain marijuana related offenses that are more than two years old, and convictions that have been sealed, expunged or eradicated).
3. If felony or serious misdemeanor criminal convictions are found, determine whether they can be lawfully considered under Labor Code Section 432.7 and then evaluate the nature and date of each offense for relevancy to your workplace (certainly convictions involving dishonesty, such as theft, fraud, and perjury, and involving violence should weigh against granting an offer).
4. Employers should: (1) inquire about felony and serious misdemeanor convictions as part of the pre-employment process; (2) engage reputable background investigation firms who can provide appropriate forms and waivers to applicants as well as conduct the searches of relevant criminal, civil judicial action, credit (if relevant) and other background check inquiries; (3) if public records are obtained at the pre-employment stage, they are to be provided to the job applicant within seven days of the firm's receipt of them; (5) if public records are obtained in connection with an investigation of employee misconduct, those records are generally to be provided to the employee within a reasonable time after the investigation concludes. (See discussion above re California Investigative Consumer Reporting Agencies Act).

I. Protecting Personnel Records And Other Confidential Information

1. Confidentiality of Medical Information.
 - a. Confidentiality of Medical Information Act ("CMIA") – Cal. Civ. Code § 56.05 et seq.
 - i. Protects any "individually identifiable information" in the possession of or obtained from a healthcare provider or healthcare service regarding medical condition, treatment or history.

- ii. Employer must handle employees' medical information to ensure confidentiality and avoid unauthorized use or disclosure.
 - iii. Employer may not use or disclose medical information without a signed authorization from the employee permitting the use (see sample authorization ATTACHED, designed to meet both HIPAA and CMIA).
 - 1. Authorization must be handwritten by employee or printed in 14 point type.
 - 2. Authorization must be clearly separate from other information on page (sentence at the bottom of employment application, for example, is insufficient).
 - 3. Must be signed and dated by the patient or his/her legal representative (minor, incompetent, deceased).
 - 4. Must specify an expiration date.
 - iv. Many provisions of the CMIA may be preempted by HIPAA (see below).
- b. HIPAA.
- i. Covers use and disclosure of any "Personal Health Information" ("PHI").
 - ii. HIPAA regulations may preempt many provisions of the California CMIA.
 - 1. California has an Office of HIPAA Implementation (CalOHI) responsible for coordinating HIPAA compliance in state agencies and affiliates.
 - 2. CalOHI website is a good resource for basic HIPAA compliance information:
 - iii. <http://www.ohi.ca.gov/state/calohi/ohiHome.jsp>.
 - iv. Whether a particular company or employer is covered by particular provisions of HIPAA must be determined on a case-by-case basis.
- c. Should keep medical information separate from other personnel records, under lock & key if possible, and limit access to those employees with a "need to know."

- d. FORM – Authorized Release of Medical Information (ATTACHED).
2. Employee's Right to Inspect/Obtain Copies of Records.
- a. Employees have the right to **INSPECT** personnel records maintained by the employer relating to the employee's performance or to any grievance concerning the employee. Cal. Labor Code § 1198.5.
 - b. Employer must do ONE of the following:
 - i. Keep a copy of each employee's personnel records at the place where the employee reports to work; OR
 - ii. Make the employee's personnel records available within a reasonable time following employee's request to review; OR
 - iii. Permit employee to inspect the records where they are stored with no loss of compensation to the employee.
 - c. Employer may withhold (not allow employee to inspect):
 - i. Records relating to investigation of potential criminal offense;
 - ii. Letters of reference;
 - iii. Ratings reports or records
 - 1. obtained prior to the employee's employment;
 - 2. prepared by identifiable examination committee members;
and
 - 3. obtained in connection with a promotional examination.
 - d. Current and former employees have the right to obtain **copies** of personnel records if employee has **signed** the document and it relates to his or her "obtaining or holding employment." Cal. Labor Code § 432.
 - i. Examples include: employment applications, employee evaluations, employment agreement, confidentiality agreements, etc.
 - ii. Violation is punishable as a misdemeanor. Cal. Labor Code § 433.

- e. Current and former employees have the right to review and obtain copies of any documents related to payment of wages. Cal. Labor Code § 226.
 - i. Must be furnished within 21 days after request.
 - ii. \$750 penalty for failure to provide on time. Attorneys fees if civil action to compel.
 - iii. What if the records do not exist? “An employee suffering injury due to employer’s knowing and intentional failure to” issue specified paystubs or maintain specified wage records for 3 years may recover the greater of their actual damages or \$50 for the initial pay period and \$100 for each additional pay period up to a maximum of \$4,000.
3. Dealing with Subpoenas of Employment Records – Cal. Civ. Proc. Code §1985.6.
- a. Applies to records regarding current and former employees.
 - b. Date for production must give employer reasonable time to locate and produce records.
 - c. Produce records only if you receive:
 - i. Written authorization signed by employee or employee’s attorney;
OR
 - ii. Proof that employee (or his/her attorney) received a copy of the subpoena at least 10 days prior to the date employer must produce records.
 - d. Do NOT produce records prior to the production date on the subpoena .
 - e. If you receive notice of a motion by a party employee to protect the records, or an objection to production from a non-party employee, do not produce the records until authorized by the employee or court order.
4. Disclosure of Information to Law Enforcement Agencies – Cal. Gov. Code § 1031.1(a). Disclosure allowed if:
- a. Request is made in writing;
 - b. Request is accompanied by notarized authorization by applicant releasing employer of liability; and
 - c. Request and authorization are presented to employer by sworn officer or other authorized representative of the law enforcement agency.

5. Business Records Act – Cal. Civ. Code §§ 1799-1799.3.

- a. No business entity that performs **bookkeeping services** may disclose in whole or in part the contents of any record to any person other than the individual or entity that is the subject of the record, without the express written consent of that individual or business entity.
- b. Restriction applies even if the identity of the individual or business entity is not disclosed.
- c. Exemptions:
 - i. Does not include chartered or licensed financial institutions.
 - ii. Disclosures made pursuant to subpoena or court order.
 - iii. Disclosure of information that is discoverable.
 - iv. Compliance with lawful search warrant.
 - v. Disclosure to law enforcement agency when required for lawful investigation of criminal activity.
 - iv. Disclosure to taxing agency for purposes of tax administration.

J. Privacy of Social Security Numbers and Other Personal Identification.

- 1. Identity Theft And Consumer Fraud Concerns; Recent Legislation.
- 2. Duty to Notify of Computer Security Breach.
 - a. Cal Civil Code §§ 1798.29 and 1798.82 (effective July 1, 2003) requires companies and state agencies with own or license "personal information" on their computers to promptly notify those California residents affected of unauthorized access to such unencrypted information.
 - b. Personal information is defined as someone's first name (or first initial) and last name combined with any of the following: social security number; driver's license or California Identification Card Number; or account number, credit or debit card number combined with any required security code, access code or password.
- 3. Limitations on Uses of Social Security Numbers.
 - a. Cal Civil Code Section 1798.85 prohibits companies from
 - i. Publicly posting or displaying social security numbers (SSN), printing an individual's SSN on a card that the individual is required

to show to access products or services or on materials mailed to the individual (unless state or federal law requires it);

- ii. Requiring the individual to use their SSN on the internet unless it is encrypted, secure, and some other form of authentication is also required; or
 - iii. Embedding SSNs in a chip, or other media contained on a card or document.
 - iv. Prior SSN uses that would violate the statute today are “grandfathered” if the uses existed before July 1, 2002, were continuous after July 1, 2002 and the individual is informed annually that he or she has the right to stop this use.
 - v. Companies may still collect and use SSNs as required by state and federal law (e.g., W-2 and W-4 forms, pay stubs) and for internal verification of administrative purposes.
4. Pay Stub Rules for Social Security Numbers.
- a. California Labor Code Section 226 requires employers to give employees an itemized statement along with each paycheck that contains the basis for wage earnings and all deductions and SSNs.
 - b. Effective July 21, 2005, employers may use the last four digits of social security numbers, or use new or existing alternate employee identification numbers, on the paystubs now.
 - c. Effective January 1, 2008, must not use full SSNs on paystubs.
5. New Regulations Govern Disposal of Personal Information.
- a. Effective June 1, 2005, new regulations (16 C.F.R. 682, et seq.) issued pursuant to the 2003 federal Fair and Accurate Transactions Act (“FACTA”) amendments to the Fair Credit Reporting Act.
 - b. Employers must shred or burn paper, and permanently erase hard drives and other computer memory devices, before disposing of documents and files containing personal information.
 - c. Applies to all employers, regardless of size.
 - d. Examples of personal information are social security numbers, home addresses, phone numbers, certain background check information, and information received from a consumer reporting agency such as credit data.

K. Requests for References

1. Any person, agent or officer of employer who, after termination of employee's employment, voluntarily or involuntarily, by any misrepresentation prevents or attempt to prevent former employee from obtaining employment is guilty of a misdemeanor. Cal. Labor Code § 1050. Treble damages also available. Cal. Labor Code § 1054.
2. Any person who knowingly causes or permits a violation of § 1050, or who fails to take all reasonable steps within his/her power to prevent the violation, is also guilty of a misdemeanor. Cal. Labor Code § 1052.
3. Truthful response to a request for information is protected, unless statement is accompanied by something else that gives it different meaning. Cal. Labor Code § 1053.
4. Defamation/interference with prospective economic advantage risk.
5. Employer's truthful response to questions whether former employee is eligible for rehire is privileged. Cal. Civ. Code § 47(c).

L. Employee Literacy Assistance

1. Employer has duty to accommodate employee who has literacy problem and wants assistance. Cal. Labor Code § 1040 et seq.
 - a. Private employer that regularly employs 25 or more persons must reasonably accommodate and assist any employee who reveals a problem of illiteracy wishes assistance in enrolling in adult literacy education program, provided it does not impose undue hardship on employer.
 - b. Employer has statutory obligation to keep confidential the fact that employee has a literacy problem.
 - c. Employee not entitled to time off with pay. If employee reveals problem with literacy and who satisfactorily performs his or her work is not subject to termination.
 - d. Employer has duty to accommodate employee who has literacy problem and wants assistance. Cal. Labor Code § 1040 et seq.

M. Competition and Trade Secrets

1. General Rule Re Covenants Not To Compete. “Every contract by which anyone is restrained from engaging in a lawful trade or business of any kind is to that extent void.” Cal. Bus. & Prof. Code § 16600.
2. Statutory Exceptions.
 - a. Employee of a Corporation. Sale of goodwill of the business, all of the stockholder's stock, or substantially all assets of a corporation. Cal. Bus.& Prof. Code §16601.
 - b. Employee of a Partnership. Sale of partnership interest or dissolution of the partnership. Cal. Bus. & Prof. Code §16602.
 - c. Must be reasonable under the circumstances of each case. Geographic scope, duration of covenant, and activities precluded.
 - d. Covenant is strictly construed. Courts will not enforce “sham covenants.”
3. Case Law Exceptions. Partial restraints which limit, but do not preclude competitive activities or employment, may be enforceable. Employer generally cannot preclude employee from working for a competitor, but may limit how that employee may compete.
 - a. Confidentiality agreements prohibiting unauthorized disclosure or use of confidential and proprietary information or trade secrets.
 - i. Public policy protects:
 1. Legitimate trade secrets of the employer.
 2. Employee's right to earn a living in his or her business, trade or profession.
 - ii. Important provisions: (1) an identification, at least by category, of the information the company claims to be confidential and proprietary; and (2) the employee's acknowledgment of the company's designation of its trade secrets, the employer's effort to assemble the information, and the economic value of ensuring that the information is not known outside the company.
 - iii. California's enactment of the Uniform Trade Secrets Act defines a “trade secret” as: Information, including a formula, pattern, compilation, program, device, method, technique or process that:
 - (a) Derives actual or potential economic value from not being generally known to the public or to other persons who can obtain

economic value from its disclosure or use; and (b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. Cal. Civil Code §3426, et seq.

- iv. Examples of confidential and proprietary information that may be a trade secret: research and development of new products, marketing and business plans, customer lists, pricing research and strategies, sales sources and other data, and manufacturing processes. This work product may not yet be developed fully enough to warrant patent or copyright protection.
- v. Customer list cases are among the most common.
- vi. Trade secret protection programs.
- vii. Covenants prohibiting solicitation of customers. [But note, mailing announcements of new employment or business affiliation without asking for business is permissible because it is not a "solicitation."]
- viii. Covenants prohibiting "employee raiding."
- ix. Covenants limiting employee's preparations for a competing business while still employed. Similar to employee's fiduciary duty of loyalty to employer.
- x. Covenants prohibiting only a limited or small part of a business, trade or profession, but not all business activities.
- xi. Why use agreements if the unfair competition and other laws may already provide a remedy for such conduct?
 1. Deterrence before the conduct occurs.
 2. Evidence after the conduct occurs.
- xii. Should be signed as a condition of initial employment. Post employment issues - consideration.
- xiii. Do not include a covenant not to compete in agreements with non-owner employees – it may invalidate the entire agreement.
- xiv. Stock Option Agreements:
 1. "Bad boy" clause
 2. Non-compete provisions -- federal or state court?
- xv. Personal Service Contracts.

1. Special, unique, unusual, extraordinary or intellectual character that gives the employee “peculiar value”.
2. Generally limited to “one-of-a-kind” entertainers.

xvi. Post-termination consulting agreements.

4. Key Steps to Develop a Trade Secret Protection Program.

- a. Identify “real” trade secrets and their value.
 - i. Evaluate confidential and proprietary information and answer two questions: (1) What information, if taken by a competitor, could damage or destroy your business? and (2) How much money has or will the company spend to develop this information?
- b. Identify and place legend key documents.
 - i. Mark key documents containing trade secrets with legend: “TRADE SECRET. This document contains confidential and proprietary information of QRS, Inc. Do not copy or circulate.”
 - ii. Avoid dilution of protection and loss of credibility by stamping as “confidential” documents that are clearly not confidential.
- c. Pre-hire investigation of criminal and employment history and other information, subject to applicable law governing such inquiry.
- d. Use confidentiality/trade secret agreements with every employee whose duties bring them into contact with trade secrets (sample ATTACHED).
- e. Restrict access to those who need to know.
- f. Update the employee handbook.
 - i. State company policy and deterrence; grounds for termination of employment, civil action and criminal prosecution.
 - ii. Limit employees' expectation of privacy in their use of the company's telephones, computers, and work areas.
- g. Update computer security. Use a computer consultant who first signs a confidentiality agreement.
- h. Document controls. Examples: locked and/or guarded single depository, sign-in and sign-out procedure, access limited to those who need to know, limit or restrict photocopies, shred discarded confidential documents, limit faxes.

- i. Consider other security measures. Examples: security guards, logbook of all persons entering or leaving the company's premises, briefcases and handbags subject to inspection by exit guards.
- j. Effective exit interview procedures to remind departing employees of confidentiality.
 - i. Consider use of acknowledgment of prior and continuing confidentiality obligations; a severance benefit may be useful to obtain employee's signature.
 - ii. Require return of company equipment and documents (e.g., sample confidentiality policy, confidentiality agreement, and termination certification ATTACHED).
- k. Include independent contractors and other outsiders as part of the program.
- l. Sue to enforce employer's confidentiality rights. Deterrence and credibility issues.

.....

THESE MATERIALS ARE INTENDED FOR INFORMATIONAL PURPOSES ONLY, AND ARE NOT INTENDED AS LEGAL ADVICE. DUE TO PAGE AND TIME CONSTRAINTS, THE MATERIALS ARE AN OVERVIEW AND SUMMARY ONLY, AND THEY DO NOT CONTAIN AN EXHAUSTIVE EXPLANATION OF THE LAW AND ITS MANY EXCEPTIONS. LEGAL COUNSEL SHOULD BE CONSULTED IF YOU HAVE SPECIFIC QUESTIONS.

Appendix

SAMPLE TECHNOLOGY/INTERNET POLICY

USE OF TECHNOLOGY AND THE INTERNET

The Company's technical resources--including desktop and portable computer systems, fax machines, voice mail, electronic mail (e-mail), Internet and World Wide Web access, electronic bulletin boards, and its intranet--enable Employees quickly and efficiently to access and exchange information throughout the Company and around the world. When used properly, we believe these resources greatly enhance Employee productivity and knowledge. In many respects, these new tools are similar to other Company tools, such as stationery, file cabinets, photocopiers, and telephones. Because these technologies are both new and rapidly changing, it is important to explain how they fit within the Company and within your responsibilities as an Employee.

This policy applies to all technical resources that are owned or leased by the Company, that are used on or accessed from Company premises, or that are used on Company business. This policy also applies to all activities using any Company-paid accounts, subscriptions, or other technical services, such as Internet and World Wide Web access, voice mail, and e-mail, whether or not the activities are conducted from Company premises.

NOTE: As you use the Company's technical resources, it is important to remember the nature of the information created and stored there. Because they seem informal, email messages are sometimes offhand, like a conversation, and not as carefully thought out as a letter or memorandum. Like any other document, an e-mail message or other computer information can later be used to indicate what an Employee knew or felt. You should keep this in mind when creating e-mail messages and other documents. Even after you delete an e-mail message or close a computer session, it may still be recoverable and may even remain on the system.

1. Acceptable Uses

The Company's technical resources are provided for the benefit of the Company and its customers, vendors, and suppliers. These resources are provided for use in the pursuit of Company business and are to be reviewed, monitored, and used only in that pursuit, except as otherwise provided in this policy. Employees are otherwise permitted to use the Company's technical resources for occasional, non-work purposes with permission from their direct Manager. Nevertheless, Employees have no right of privacy as to any information or file maintained in or on the Company's property or transmitted or stored through the Company's computer, voice mail, e-mail, or telephone systems.

2. Unacceptable Uses

The Company's technical resources should not be used for personal gain or the advancement of individual views. Employees who wish to express personal opinions on the Internet are encouraged to obtain a personal account with a commercial Internet service provider and to access the Internet without using Company resources.

Solicitation for any non-Company business or activities using Company resources is strictly prohibited. Your use of the Company's technical resources must not interfere with your productivity, the productivity of any other Employee, or the operation of the Company's technical resources. Employees may not play games on the Company's technical resources.

You should not send e-mail or other communications that either mask your identity or indicate that they were sent by someone else. You should never access any technical resources using another Employee's password. Similarly, you should only access the libraries, files, data, programs, and directories that are related to your work duties. Unauthorized review, duplication, dissemination, removal, installation, damage, or alteration of files, passwords, computer systems or programs, or other property of the Company, or improper use of information obtained by unauthorized means, is prohibited.

Sending, saving, or viewing offensive material is prohibited. Messages stored and/or transmitted by computer, voice mail, e-mail, or telephone systems must not contain content that may reasonably be considered offensive to any Employee. Offensive material includes, but is not limited to, sexual comments, jokes or images, racial slurs, gender-specific comments, or any comments, jokes or images that would offend someone on the basis of his or her race, color, creed, sex, age, national origin or ancestry, physical or mental disability, veteran status, marital status, medical condition, sexual orientation, as well as any other category protected by federal, state, or local laws. Any use of the Company's technical resources to harass or discriminate is unlawful and strictly prohibited by the Company. Violators will be subject to discipline, up to and including discharge.

[Company Name] does not consider conduct in violation of this policy to be within the course and scope of employment or the direct consequence of the discharge of one's duties. Accordingly, to the extent permitted by law, the Company reserves the right not to provide a defense or pay damages assessed against Employees for conduct in violation of this policy.

3. Access to Information

The Company asks you to keep in mind that when you are using the Company's computers you are creating Company documents using a Company asset. The Company respects the individual privacy of its Employees. However, that privacy does not extend to an Employee's work-related conduct or to the use of Company-provided technical resources or supplies.

The Company's computer, voice mail, e-mail, or telephone systems, and the data stored on them are and remain at all times the property of the Company. As a result, computer data, voice mail messages, e-mail messages, and other data are readily available to numerous persons. If, during the course of your employment, you perform or transmit work on the Company's computer system and other technical resources, your work may be subject to the investigation, search, and review of others in accordance with this policy.

All information, including e-mail messages and files, that is created, sent, or retrieved over the Company's technical resources is the property of the Company, and should not be considered private or confidential. Employees have no right to privacy as to any information or file transmitted or stored through the Company's computer, voice mail, e-mail, or telephone systems. Any electronically stored information that you create, send to, or receive from others may be retrieved and reviewed when doing so serves the legitimate business interests and obligations of the Company. Employees should also be aware that, even when a file or message is erased or a visit to an Internet or Web site is closed, it is still possible to recreate the message or locate the Web site. The Company reserves the right to monitor your use of its technical resources at any time. All information including text and images may be disclosed to law enforcement or to other third parties without prior consent of the sender or the receiver.

4. Copyrighted Materials

You should not copy and distribute copyrighted material (e.g., software, database files, documentation, articles, graphics files, and downloaded information) through the e-mail system or by any other means unless you have confirmed in advance from appropriate sources that the Company has the right to copy or distribute the material. Failure to observe a copyright may result in disciplinary action by the Company as well as legal action by the copyright owner. Any questions concerning these rights should be directed to your Manager.

5. Confidential Information

E-mail and Internet/Web access are not entirely secure. Others outside the Company may also be able to monitor your e-mail and Internet/Web access. For example, Internet sites maintain logs of visits from users; these logs identify which company, and even which particular person, accessed the service. If your work using these resources requires a higher level of security, please ask your Manager or the MIS Department for guidance on securely exchanging e-mail or gathering information from sources such as the Internet or World Wide Web.

All Employees should safeguard the Company's confidential information, as well as that of customers and others, from disclosure. Do not access new voice mail or e-mail messages with others present. Messages containing confidential information should not be left visible while you are away from your work area.

E-mail messages containing confidential information should include the following statement, in all capital letters, at the top of the message: CONFIDENTIAL: UNAUTHORIZED USE OR DISCLOSURE IS STRICTLY PROHIBITED.

6. Security of Information

Although you may have passwords to access computer, voice mail, and e-mail systems, these technical resources belong to the Company, are to be accessible at all times by the Company, and are subject to inspections by the Company with or without notice. The Company may override any applicable passwords or codes to inspect, investigate, or search an Employee's files and messages. All passwords must be made available to the MIS Department upon request. You should not provide a password to other Employees or to anyone outside the Company and should never access any technical resources using another Employee's password.

In order to facilitate the Company's access to information on its technical resources, you may not encrypt or encode any voice mail or e-mail communication or any other files or data stored or exchanged on

Company systems without the express prior written permission from the MIS Department and your Manager. As part of this approval, the MIS Department will indicate a procedure for you to deposit any password, encryption key or code, or software with the MIS Department so that the encrypted or encoded information can be accessed in your absence.

7. [Company Name]'s Software Policy

If you want to install software on Company computers, you must contact the MIS Department and request to have the software installed. Employees are prohibited from installing any software on any Company technical resource without the express prior written permission from the MIS Department.

Involving the MIS Department ensures that the Company can manage the software on Company systems, prevent the introduction of computer viruses, and meet its obligations under any applicable software licenses and copyright laws. Computer software is protected from unauthorized copying and use by federal and state law; unauthorized copying or use of computer software exposes the Company and the individual Employee to substantial fines and exposes the individual Employee to imprisonment. Therefore, Employees may not load personal software onto the Company's computer system and may not copy software from the Company for personal use.

8. Your Responsibilities

Each Employee is responsible for the content of all text, audio, or images that they place or send over the Company's technical resources. Employees may access only files or programs, whether computerized or not, that they have permission to enter.

Violations of any guidelines in this policy may result in disciplinary action up to and including termination. In addition, the Company may advise appropriate legal officials of any illegal violations.

SAMPLE DRUG & ALCOHOL ABUSE POLICY

The use of alcohol, illegal drugs, intoxicants and controlled substances, whether on or off duty, can impair Employees' ability to work safely and efficiently. The Company prohibits the use of these substances to the extent that they affect, or have the potential to affect, the workplace. Company will not jeopardize the safety of the Employee, other Employees, our clients, the public, and Company operations due to an individual's poor judgment. Accordingly, the Company prohibits the following:

1. Possession, use or having alcohol or an illegal drug, intoxicant or controlled substance in your system during working hours.
2. Operating a vehicle owned or leased by the Company while having alcohol or an illegal drug, intoxicant or controlled substance in your system.
3. Distribution, sale, manufacture or purchase--or the attempted distribution, sale, manufacture or purchase--of an illegal drug, intoxicant or controlled substance during working hours or while on premises owned or occupied by the Company.

Any Employee suspected of possessing alcohol, an illegal drug, intoxicants or a controlled substance is subject to inspection and search, with or without notice. Employees' personal belongings, including any bags, purses, briefcases and clothing, and all Company property, are also subject to inspection and search, with or without notice. Employees who violate the Company's drug and alcohol abuse policy will be removed from the workplace immediately. The Company may also bring the matter to the attention of appropriate law enforcement authorities. Any conviction for criminal conduct involving illegal drugs, intoxicants or controlled substances, whether on or off duty, or any violation of the Company's drug and alcohol abuse policy, including having a positive drug-test result, may lead to disciplinary action, up to and including termination.

The use of prescription drugs and/or over-the-counter drugs may also affect Employees' job performance and seriously impair Employees' value to the Company. Any Employee who is using prescription or over-the-counter drugs that may impair his or her ability to safely perform the job or may affect the safety or well being of others must submit a physician's statement that the prescription drug use will not affect job safety. The Employee is not required to identify the medication or the underlying illness. Various federal, state and local laws protect the rights of individuals with disabilities and others with regard to the confidentiality of medical information, medical treatment, and the use of prescription drugs and substances taken under medical supervision. Nothing contained in this policy is intended to interfere with individual rights under, or to violate, these laws.

NOTE: On occasion, managerial staff may entertain clients during work hours or after work hours as representatives of the Company. These occasions may include lunches, dinners and business conferences. On these occasions, only the moderate and limited use of alcoholic beverages is acceptable. In addition, occasionally, alcohol is served at social events sponsored by the Company. Alcohol may be served at these events only with the approval of _____. Only the moderate and limited use of alcohol is acceptable. Employees are expected to remain responsible, professional and sober at all times.

The Company will attempt to reasonably accommodate Employees with chemical dependencies (alcohol or drugs), if they voluntarily wish to seek treatment and/or rehabilitation. Employees desiring that assistance should request an unpaid treatment or rehabilitation leave of absence. The Company's support for treatment and rehabilitation does not obligate the Company to employ any person who violates the Company's drug and alcohol abuse policy or whose job performance is impaired because of substance abuse. The Company is also not obligated to reemploy any person who has participated in treatment or rehabilitation if that person's job performance remains impaired as a result of dependency. Employees who are given the opportunity to seek treatment and/or rehabilitation and are involved in any further violations of this policy will not be given a second opportunity to seek treatment or rehabilitation.

AUTHORIZATION FOR RELEASE OF MEDICAL INFORMATION

I _____, hereby authorize the use or disclosure of my health information as described in this authorization.

1. Specific person/organization (*or class of persons*) authorized to provide the information:

2. Specific person/organization (*or class of persons*) authorized to receive and use the information:

3. Purpose of the Request: Please state the purpose of the request below. If you do not wish to state a purpose, please state, "At the request of the individual".

4. Right to Revoke: I understand that I have the right to revoke this authorization at any time by notifying _____ in writing at _____. I understand that any use or disclosure made prior to the revocation under this authorization will not be affected by a revocation.

5. I understand that after this information is disclosed, federal law might not protect it and the recipient might disclose it again.

6. I understand that I am entitled to receive a copy of this authorization.

7. I understand that this authorization will expire on _____. (*Expiration date or event, for example one year*)

Signature of Individual

Date

If a Personal Representative executes this form, that Representative warrants that he or she has authority to sign the form on the basis of: _____

This authorization reflects the requirements of 45 CFR & 164.508

SAMPLE CONFIDENTIALITY POLICY

CONFIDENTIALITY

Information about [Company Name], its Employees, customers, suppliers, and vendors is to be kept confidential and divulged only to individuals within the Company with both a need to receive and authorization to receive the information. If in doubt as to whether information should be divulged, err in favor of not divulging information and discuss the situation with your Manager.

All records and files maintained by the Company are confidential and remain the property of the Company. Records and files are not to be disclosed to any outside party without the express permission of the [appropriate management]. Confidential information includes, but is in no way limited to: financial records; business, marketing, and strategic plans; personnel and payroll records regarding current and former Employees; the identity of, contact information for, and any other account information on customers, vendors, and suppliers; inventions, programs, trade secrets, formulas, techniques, and processes; and any other documents or information regarding the Company's operations, procedures, or practices. Confidential information may not be removed from Company premises without express authorization.

Confidential information obtained during or through employment with the Company may not be used by any Employee for the purpose of furthering current or future outside employment or activities or for obtaining personal gain or profit. The Company reserves the right to avail itself of all legal or equitable remedies to prevent impermissible use of confidential information or to recover damages incurred as a result of the impermissible use of confidential information.

Employees may be required to enter into written confidentiality agreements confirming their understanding of the Company's confidentiality policies.

**SUMMARY OF KEY PROVISIONS TO
CONFIDENTIALITY AND NON-SOLICITATION AGREEMENT
WITH NON-OWNER EMPLOYEE**

R E C I T A L S

Recitals include that: the Company has developed and will continue to develop proprietary and confidential information and Trade Secrets; Employee would not be given access to this information if not employed; the Employee's execution of the Agreement is a condition of employment; and that it is not intended to unfairly restrict Employee's ability to earn a living after the employment ends.

A G R E E M E N T

Proprietary and Confidential Information and Trade Secrets. Definition of "Trade Secrets" for purposes of this Agreement to include information which derives independent economic value for not being generally known in the industry and for which the Company takes reasonable efforts to maintain secrecy. Include multiple examples of Company Trade Secrets. Acknowledgment that these items constitute Trade Secrets which are the sole and exclusive property of the Company.

Nondisclosure. Strict non-disclosure provisions that apply both during and after employment ends.

Employee's Further Obligation. No copying or removal of Trade Secrets and confidential information. Take reasonable precautions to prevent unauthorized use by others. Disclose and transfer to Company any improvements, discoveries and inventions developed during employment. No personal financial gain using Company Trade Secrets and confidential information. Must show a copy of this Agreement to any future employers.

Prior Knowledge and Relationships. Acknowledgment that Employee has not taken and will not use any Trade Secrets belonging to any prior employer.

Noncompetition During Employment. Employee will not directly or indirectly compete against Company while employed by Company.

Non-Solicitation of Employees. Prohibition on soliciting or pirating Employees and consultants away from Company.

Non-Solicitation of Clients. For a period after employment ends, prohibition on soliciting clients or customers away from Company.

Ownership of Copyrights and Inventions. Acknowledgment that anything created by Employee during the scope of employment is a "work made for hire" that belongs to the Company. Requirement that Employee assist Company in securing patents copyrights or similar protections of such works. Written notification to Employee required by the California Labor Code regarding Employee Inventions.

Term of Agreement. Usually beyond the end of employment.

Default; Cumulative Remedies. Company may seek injunctive and other relief against Employee in addition to money damages in the event of a breach.

Entire Agreement. Acknowledgment that this Agreement contains everything regarding the subject matter and supersedes any prior agreements or discussions. Provision that nothing in this Agreement is intended to vary or modify the "at will" nature of Employee's employment with Company.

Amendment. Any changes need to be in writing.

Applicable Law and Jurisdiction. Agreement to submit to personal jurisdiction in California and selection of specific court geographic venue within California for any lawsuit.

Benefit and Burden. The Agreement is binding on the respective successors and assigns.

Waiver. No party can waive the requirements/protections of the Agreement unless it is in writing.

Severability. If a court finds certain provisions of the Agreement to be unenforceable, the court and enforce the balance of the Agreement.

Interpretation. Guidance for interpretation of the Agreement.

SAMPLE TERMINATION CERTIFICATION
XYZ Company
TERMINATION CERTIFICATION

This is to certify that I do not have in my possession nor have I failed to return any devices, records, data, notes, reports, proposals, lists, correspondence, specifications, drawings, blueprints, sketches, materials, equipment, or any other documents or property or any reproductions of any aforementioned items belonging to the Company, its subsidiaries, affiliates, successors or assigns (together, the "Company").

I further certify that I have complied with all the terms of the Company's Employment, Confidential Information, Invention Assignment and Arbitration Agreements signed by me, including the reporting of any inventions and original works of authorship (as defined therein), conceived or made by me (solely or jointly with others) covered by that agreement.

I further agree that, in compliance with the Employment, Confidential Information, Invention Assignment, and Arbitration Agreement, I will preserve as confidential all trade secrets, confidential knowledge, data or other proprietary information relating to products, processes, know-how, designs, formulas, developmental or experimental work, computer programs, data bases, other original works of authorship, customer lists, business plans, financial information or other subject matter pertaining to any business of the Company or any of its employees, clients, consultants or licensees.

I further agree that for twelve (12) months from this date I will not hire any employees of the Company and I will not solicit, induce, recruit or encourage any of the Company's employees to leave their employment.

Date:

(Employee's Signature)

(Type/Print Employee's Name)

.....
THESE MATERIALS ARE INTENDED FOR INFORMATIONAL PURPOSES ONLY, AND ARE NOT INTENDED AS LEGAL ADVICE. DUE TO PAGE AND TIME CONSTRAINTS, THE MATERIALS ARE AN OVERVIEW AND SUMMARY ONLY, AND THEY DO NOT CONTAIN AN EXHAUSTIVE EXPLANATION OF THE LAW AND ITS MANY EXCEPTIONS. LEGAL COUNSEL SHOULD BE CONSULTED IF YOU HAVE SPECIFIC QUESTIONS.