BERNSTEIN SHUR

COUNSELORS AT LAW

Confidential Personnel Information in the Workplace

by

Linda McGill and Matthew Tarasevich

Bernstein Shur Labor and Employment Practice Group

June 22, 2012

BERNSTEIN SHUR

COUNSELORS AT LAW

Confidential Personnel Information in the Workplace

By Linda McGill | Matthew Tarasevich

1. Acquiring Personal Personnel Information: In the Workplace, It Happens

In the course of the employment relationship businesses acquire, generate and maintain significant personal information about individual applicants and employees. Data collection begins well before any employment relationship is formed, when a job seeker is typically asked to provide a history of his or her education, work experience, reasons for leaving previous employment, names of personal references and permission for the potential employer to delve further into background information. At the next stage, materials on the applicant's credit history, past job performance, criminal records and Internet profile may be collected and scrutinized. Before final hiring the individual may have to take a substance abuse test, pre-employment physical, polygraph (in Maine, limited to law enforcement positions) or undergo other screening that generates even more sensitive, albeit presumably job-related, data.

Once the individual is hired, health and medical information will be collected in the course of dealing with sick leave, family medical leave, health insurance benefits, fitness for duty exams and requests for reasonable accommodations or workers compensation claims. Other personal information may find its way into the employer's files includes, family circumstances that affect job performance, romantic or sexual involvements with co-workers, conduct or habits that are the subject of a workplace investigation, substance abuse problems, child support obligations and the like.

During the course of even the most uneventful employment relationship virtually every business amasses personal and private information on its employees. Some of this information, particularly when related to health or medical issues, is protected by statute from all but the most limited dissemination or use by the employer. Other information is not specifically regulated but may be the source of invasion of privacy, defamation or other tort claims if it is wrongly publicized or otherwise misused, and although existing regulations are already somewhat complex, there is growing movement by state legislatures, congress, the Equal Employment Opportunity Commission (EEOC) and courts to impose further restrictions on employers' access to and use of personal and private information about applicants or employees. In the digital age, when employers are able to collect more information on their personnel, but are under increasing pressure to protect that information and to use it only as permitted by law, it is important for lawyers to know the legal landscape of managing personnel information in order to better advise both employers and individuals when these issues arise in the workplace.

2. Current Laws Regulating the Collection, Maintenance and Dissemination of Medical or Other Confidential Personnel Information

Numerous laws currently regulate the collection, maintenance and dissemination of medical and other confidential personnel information by employers in Maine. The major sources of compliance requirements and/or potential liability, include:

• Maine Human Rights Act, 5 M.R.S.A §4572

• Maine Freedom of Access Act, 1 M.R.S.A. § 401 (governmental employers)

• Confidential Personnel Records Law, 30-A §2702 (governmental employers)

• Americans with Disabilities Act

• Genetic Information and Non-Disclosure Act of 2008

• Maine and Federal Family Medical Leave Acts

• Fair Credit Reporting Act

• Common Law Right to Privacy

3. Key Provisions of Laws Regulating Confidentiality of Personnel Information

Among the numerous legal mandates, limitations and regulations relevant to personnel information, the following are the most commonly invoked and enforced and therefore the most important for employer compliance:

(a) MHRA and ADA: Limiting Collection, Storage and Dissemination of Medical Information

The MHRA and ADA have similar restrictions on acquiring, maintaining and using medical information generated from a pre-employment physical or other medical examination. Information about the medical condition or history of an applicant may legally be obtained if the same information, typically in the form of a pre-employment physical, is required for all similarly-situated individuals who have received a conditional offer of employment. Medical information may be acquired during the employment relationship if it is job-related and consistent with business necessity. Any medical information, which includes information received during the processing of sick leave, family medical leave requests, workers compensation, in disability claims or in any other context that is received by the employer, must be maintained on separate forms and in separate medical files, and must be treated as a confidential medical record. The information may not be accessed by or disseminated to any person in the workplace except:

• Supervisors and managers who need to be informed about necessary restrictions on the work or duties of the employee and necessary accommodations

• First aid and safety personnel, if an employee's disability might require emergency treatment

• Government officials investigating compliance with the MHRA or ADA, on request

Violation of these limitations constitutes employment discrimination under both the MHRA and the ADA. The Maine Federal District Court has recently underscored the strict limits on the use and sharing of employee medical information imposed by the ADA, holding that the restrictions protect even arguably false medical information and apply to intra-corporate disclosures. *Blanco v. BIW*, 2:10-CV-00429-JAW (July 2011) ruled that the company physician's report to the Labor Relations Department that the employee had failed to disclose his medical condition in his pre-employment medical questionnaire violated ADA's confidentiality provision. See also *Bennett v. U.S. Postal Service*, 2011 WL 24417 (E.E.O.C. Jan. 11, 2011) in which an employer that provided employee's medical records in response to a state subpoena without the employee's release, or some other exception under the ADA, violated the ADA's confidentiality restrictions.

(b) Genetic Information Non-Disclosure Act: Prohibiting Acquisition of Genetic Information

While the ADA and MHRA permit the acquisition of medical information under certain prescribed and limited circumstances, the Genetic Information Non-Disclosure Act (GINA) prohibits employers with 15 or more employees from requesting, requiring or purchasing any genetic information of applicants, employees and their family members at any time, including during the post-offer stage of employment, with extremely limited exceptions. Genetic information includes information about an individual's genetic tests, genetic tests of a family member and family medical history. Under GINA, accessing an individual's medical records directly is the same as asking an individual for information about current health status. If an employer lawfully requests access to an applicant's or employee's medical records the employer should include warning language provided by the EEOC to ensure that acquisition of any genetic information in response to the request will be considered inadvertent. If an employer does obtain genetic information under one of GINA's limited exceptions, that information must be kept separate from the personnel file and treated as a confidential medical record. Genetic information may be maintained in the same file as medical information obtained under the ADA.

(c) Confidential Personnel Records Law, 30-A M.R.S.A §2702 (Maine Governmental Employers): Protecting Specific Personnel Information from Public Access

Title 30-A M.R.S.A §2702 provides that certain municipal personnel records are confidential and are not public records under the Maine Freedom of Access Act (FOAA). These records are:

• Certain application materials, including resumes, letters and notes of reference, working papers, research materials, records, examinations, and any other documents or records prepared or used either by the applicant or the municipality in the examination or evaluation of applicants. Once an applicant is hired his or her resume becomes public, as do reference letters unless such letters are submitted in confidence

• Telephone numbers designated as unlisted or unpublished

• Medical information including information pertaining to diagnosis or treatment of mental or emotional disorders. This would include information related to sick leave, family medical leave, medical basis for accommodation requests and the like

• Performance evaluations and personal references submitted in confidence

• Information about the creditworthiness of a named employee

• Information about the personal history, general character or conduct of members of an employee's immediate family

• Complaints, charges or accusations of misconduct, replies to those complaints, charges or accusations and any other information or materials that may result in disciplinary action.

The Confidential Personnel Records Law does not limit otherwise legitimate access to personnel records which may be necessary for a bargaining agent to carry out its collective bargaining responsibilities, and union access does not mean that the records are open to other members of the public.

Because the Maine FOAA broadly mandates that records in any form in the possession of a governmental entity are public unless specifically exempted by statute or privilege, personnel information that is not protected by the Confidential Personnel Records Law or another specific law is likely accessible to the public on request. Examples of public personnel records include payroll data, records of final disciplinary action as defined in 30-A M.R.S.A. §2702 (1)(B)(5), leave records that do not contain medical information of any kind, job descriptions, memoranda and other workplace communications that do not contain otherwise protected material.

(d) Invasion of Privacy: Limiting Publication of Personal and Private Information

Most medical records, as well as other highly personal or private information collected during the course of the employment relationship are not of legitimate concern to the public and may include material that, if disseminated, would be highly offensive to the employee who is the subject of the information. Under certain circumstances the revelation of highly personal and sensitive information, especially if it is relatively widespread, for example, to the media, may amount to an invasion of the employee's common law right to privacy. Unlike a defamation claim, the tort of invasion of privacy by highly offensive publication does not turn on whether the information is true; the revelation of the private and sensitive information, regardless of truth, creates the injury.

For example, an employer's public reference to or public disclosure of an employee's HIV status, substance abuse habit or history, sexual orientation, domestic violence problems or mental health issues may conceivably constitute actionable invasion of privacy, in addition to being in violation of one or more of the employment laws outlined above.

(e) Health Insurance Portability and Accountability Act: Limited Application to Employers

The Health Insurance Portability and Accountability Act (HIPAA) generally protects individually identifiable health information created or maintained by health plans and health care providers. HIPAA does not directly regulate employers or cover medical or disability information obtained by employers for employment purposes, such as leave programs. However, HIPAA does apply to employer-sponsored health plans and certain health care providers and, in certain circumstances, to employers that provide self-funded health plans. HIPAA may also, under some circumstances, apply to information acquired through an employer-sponsored wellness program. In general, covered health plans and providers cannot use or disclose individually identifiable health information without a HIPAA-compliant authorization from the patient or health plan participant, except for purposes of treatment, payment for health care and health care operations. HIPAA imposes a number of administrative responsibilities on health plan sponsors, particularly sponsors of self-funded health plans which are designed to safeguard protected health information. For example, employers who sponsor such health plans must ensure that employees who do not work for the plans do not have access to private health information, and that those who do are adequately trained about their obligations.

While HIPAA does not generally apply to health information collected in the course of the employment relationship and moreover does not provide an individual cause of action when a covered entity violates HIPAA, HIPAA standards and protections have been cited to support a claim of invasion of privacy. See, e.g., *Poli v. Mountain Valleys Health Center*, et al., Case No. 2:05-2015-GEB-KJM, 2006 WL 83378 (E.D.Cal.). Jan.11, 2006) a case of an employee whose health center employer obtained his prescription drug records without authorization, terminated his employment and shared information with police, stated a claim for invasion of privacy. HIPAA was cited as part of "community norms" that determine what is a highly offensive disclosure.

4. Legal Issues Arising from Maintaining Personnel Files.

Maine employers are not legally mandated to maintain a personnel file on each employee. Under 26 M.R.S.A. §631, an employee has the right to review and inspect his or her personnel file "if the employer has a personnel file for that employee." See also 30-A M.R.S.A. §2702 (2) municipal employees may review and inspect if a file is maintained. Nevertheless, most employers maintain employee personnel files in some form, among other reasons, because personnel file documents provide key evidence in the litigation of most employment law disputes.

Regardless of how or where they are maintained, personnel file documents include, but are not limited to any formal or informal employee evaluations and reports relating to the employee's character, credit, work habits, compensation and benefits in the employer's possession. Files can be kept in an official jacket maintained by human resources, in a supervisor's desk drawer, in separate medical files or electronically, including the form of email. 26 M.R.S.A. §631. See *Harding v. Wal-Mart Stores*, 2001 ME 13 where a company's confidential investigation materials regarding employee's misconduct related to her character and work habits were personnel file documents to which she was entitled.

Under the MHRA, Title VII and other anti-discrimination laws, it is unlawful for an employer to elicit or attempt to elicit information directly or indirectly pertaining to race, color, sex, sexual orientation, physical or mental disability, genetic information, religion, age, ancestry or national origin, workers' compensation claim history, or any previous actions protected under the Maine Whistleblowers' Protection Act. Once an individual is hired the subject of physical or mental disability may be legitimate for inquiry or documentation, but only in a non-discriminatory context.

Regardless of how or where personnel file documents are maintained, the employer must take "adequate steps to ensure the integrity and confidentiality" of the records. 26 M.R.S.A. §631. There are no reported cases based on violations of the "integrity and confidentiality" requirements of §631. However, the legal duty imposed on Maine employers could give rise to claims of negligent disclosure or violation of privacy if records are mis-handled by allowing access to unauthorized individuals, by casual dissemination or by maintaining files without adequate security protections.

5. New Regulations and Trends Affecting Employers' Access to and Disclosure of Employee and Applicant Information

In the digital age employers have the opportunity, and the temptation, to search for personal information about applicants or employees through the Internet, through vendors of electronic information and through nationwide data bases. The information provided by these sources may lead to more well-informed employment decisions. For example, a Google search may reveal aspects of an applicant that do not appear on his resume or an employee's Facebook page may contain a diatribe against a supervisor or denigration of the company's products that the employer finds inconsistent with continuing employment. In another electronic-age development there is heightened risk that sensitive employee information will be stolen by an insider with a flash drive or an outsider who hacks into the computer system, posing risks to employees of identity theft and risks to employers of business interruption, unfavorable media treatment or lawsuits for negligence. These and other digital age realities are in turn generating new laws and proposals for increased regulation of how employers collect, store and use information on applicants and employees. A few examples:

(a) Updated EEOC Position on Employer Use of Criminal Background Checks

On April 25, 2012 the EEOC issued updated guidance on the use of criminal background checks in employment entitled "Enforcement Guidance on the Consideration of Arrest and Conviction Records in Employment Decisions Under Title VII of the Civil Rights Act of 1964." The updated guidance, the first in twenty years, recognizes that employers have access to criminal background checks through nationwide data banks, and that nearly three quarters of U.S. employers now conduct some form of criminal background screening. While the use of arrest and conviction data is not directly discriminatory, the higher rates for African-Americans and Hispanics may lead to a disparate impact on these groups from reliance on this data, in the agency's view. The EEOC has indicated that it will use its enforcement authority to investigate cases of suspected or claimed disparate treatment and disparate impact related to criminal background check policies.

The Massachusetts Criminal Offender Record Information Act, passed in 2010, prohibits Massachusetts employers from asking questions about criminal history on written job applications, although an applicant may be asked such questions at an interview. An applicant must be provided with a copy of the criminal history information obtained by the employer before being questioned about the information. Massachusetts employers must use a common data base to obtain conviction information, and information that is more than ten years old may be sealed. Other states have similar restrictions on the use of criminal history information by employers.

(b) New Focus on Employers' Use of Information Under the Fair Credit Reporting Act

On May 28, 2012 Wal-Mart Stores Inc. was sued by a proposed class of potential workers who allege that the company violated the federal Fair Credit Reporting Act (FCRA) by failing to properly disclose information related to criminal background checks on job applicants. Plaintiffs, who were rejected for jobs with Wal-Mart, allege that the company has a policy or practice of requesting that consumer reporting agencies provide consumer reports containing criminal background information on employment applicants, and of taking adverse employment action based on information contained in those reports without providing the reports and an opportunity for dispute to its applicants, in violation of the FCRA. *Landry et al. v. Wal-Mart Stores Inc.*, Case No. 2:12-cv-03113 (U.S. D.C. N.J.). Wal-Mart has previously settled at least one suit based on the same allegations. See also *Singleton v. Domino's Pizza LLC,* 8:11-cv-01823-DKC (D. Md.) (Jan. 12, 2012) where the court denied a motion to dismiss claims of FCRA violations in the hiring process.

The requirements of notice and disclosure under the FCRA are well-established, as is their application to employers that use credit and related background information in employment decisions. The FCRA has additional stringent disclosure and notice requirements if an employer uses FCRA information in an investigation. The current Wal-Mart suit, especially if the facts are found to be correct, may result in a push to further restrict employers' use of credit information in employment decisions.

(c) State and Federal Efforts to Ban Employer Access to Individuals' Social Networking Sites and Regulate Use of Postings in Employment Decisions

Several state legislatures, including Illinois, Ohio, Delaware, Michigan, New York, California and Washington, are considering measures that would prevent employers from demanding Facebook and other social networking website passwords from employees or applicants. Maryland enacted the first such law on April 9, 2012. Similar bills have been introduced in both the U.S. House and Senate. These measures are rooted in the view that social networking sites are an individual's private and personal space to which an employer should not have access. Many of the proposed bills make no exceptions to the employer ban, for example, it would not allow an employer to request or require access even when a complaint has been received that an employee is posting harassing or threatening messages to a co-worker on a social networking site or is publishing the employer's confidential or proprietary business information.

These bills are related to the current legal firestorm over whether or when adverse actions by employers based on employees' negative statements about the workplace on Facebook, Twitter or other social networking sites violate an employee's right to engage in protected, concerted activities under the National Labor Relations Act. The National Labor Relations Board continues to be hard-focused on this issue, filing numerous complaints against union and non-union employers in the past year. See, *Design Technology Group, LLC et al*., Case No. 20-CA-35511 (Apr. 27, 2012) an administrative Law Judge found that Bettie Page Company committed unfair labor practices when it discharged three employees who engaged in discussions on Facebook that mocked and criticized a supervisor and owner, but also involved complaints of working in an unsafe neighborhood. The employees were reinstated. See also Memorandum OM 12-31, Office of NLRB General Counsel, Division of Operations-Management (January 24, 2012), reviewing 14 cases decided in 2011 involving employer use of employees' social media postings as basis for discipline and whether employees were engaging in activities protected by the National Labor Relations Act. Legal protection for work-related complaints posted on an employee's "private" social networking site will continue to generate claims, controversy and confusion for the foreseeable future.

6. Conclusion: The Duty to Manage Personal Personnel Information is Subject to Both Well-Established and Newly Developing Law

Because of more sophisticated decision-making and the ease of collecting personal data on individuals over the Internet and through third parties, today's employers acquire significantly more personal information on applicants and employees than at any point in the past. It is now the norm to share one's personal information with hundreds, sometimes thousands, of electronic friends, and cultural notions of what information is truly private are changing rapidly. It is unclear whether society's privacy comfort zone will eventually accommodate the view famously expressed by Sun Microsystems's Scott McNealy, "you already have zero privacy, get over It." See Connie Davis Powell, *"You already have zero privacy. Get over it!" Would Warren and Brandeis Argue for Privacy for Social Networking, 31 Pace L. Rev. 146 (2011).* The trend in protecting the privacy of personal information about employees that is maintained in workplace files, as evidenced by the steady increase in legislation, enforcement, proposals and claims, is heading in the opposite direction from zero. The laws governing management of personnel information acquired during the course of the employment relationship will continue to evolve, presenting challenges for employment lawyers and their clients well into the 21st century.

For more information please contact Linda McGill at 207-228-7226 or lmcgill@bernsteinshur.com or Matthew Tarasevich at 207-228-7158 or mtarasevich@bernsteinshur.com.