

**Rapid Fire Update II, #2:**

**PRIVACY IN THE WORKPLACE**

**In General**

In the public sector, an employee retains 4<sup>th</sup> Amendment rights against unreasonable searches and seizures

The private sector is not subject to the 4<sup>th</sup> Amendment, but employees can still claim an invasion of privacy

Many areas are clearly public and there should be no reasonable expectation of privacy:

- shared work areas
- joint filing cabinets

Some areas will carry an expectation by their very nature:

- lockers
- unshared desk drawers

The easiest way to prevent a reasonable expectation of privacy is to have an employee handbook that clearly states that an employee should not have a reasonable expectation of privacy while in the workplace

- desk drawers are subject to search
- lockers may be assigned and temporarily locked but right to search
- computers and telephone calls may be monitored

The personnel policy should be acknowledged by the employee

In order to monitor telephone calls, the employee must be aware that the call is or may be monitored, otherwise, the call cannot be intercepted

Wire and Electronic Communications Interception of Oral Communications, 18 USCA § 2511

Also, if you allow employees to make occasional personal calls, do not monitor calls that are known to be personal rather than work-related

If you do not allow personal calls, then once you realize a call is personal, cease monitoring and then take corrective action

### **Social Security Numbers**

As of January 1, 2020, an employer may not request a social security number from a prospective employee on an employment application or during the application process for employment except for the purposes of substance abuse testing under subchapter 3-A or a pre-employment background check. Once hired, you can ask for it.

26 MRSA § 598-A

### **Pay History**

An employer may not inquire about prospective employee's compensation history until after offer of employment has been made with compensation negotiated.

26 MRSA § 4577/26 MRSA § 628-A

### **Social Media Privacy**

An employer may not require an employee or applicant to disclose a password to a social media account

An employer may not even ask

Nor may an employer require the employee to access their account in your presence so you can view it

However, an employer can require an employee to disclose personal social media account information that the employer reasonably believes to be relevant to an investigation of allegations of employee misconduct or violation of laws, but access may only be used to the extent necessary for purposes of that investigation

It is okay to access information that is made available to the general public

It is also permissible for an employer to have a policy requiring employees to disclose passwords for the employer's equipment, software, and email

26 MRSA §§ 615-619

### **Medical Privacy**

Making medical inquires as to whether an applicant is an individual with a disability or as to the nature or severity of the disability before a conditional offer of employment is made is a violation of the MHRA, and even after a conditional offer has been made, the inquiry must be job-related and consistent with business necessity

Where the MHRA does allow medical inquires, the resulting medical records must be kept in separate medical files and treated as confidential

Employees also retain privacy with respect to their genetic information under GINA

5 MRSA §19302

**Personnel Files**

The employer shall take adequate steps to ensure the integrity and confidentiality of personnel file records.

26 MRSA § 631