# Collection, Use & Disclosure of Employee Private Medical Information Compliance Game Plan


Companies and HR directors need to collect employees' personal health information to carry out basic employment functions. For example, you need medical records to determine an employee's eligibility for disability benefits or a doctor's note to verify they were really ill when they called in sick. You might feel that this is a perfectly legitimate request. But employees are apt to see it as an unwarranted intrusion into their personal lives as well as a violation of personal privacy laws like the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA).

Some of these employee privacy complaints are legitimate; some of them aren't. But it's not always easy to tell the difference between the valid and the invalid ones. On the one hand, the law requires employers to respect their employees' privacy rights; but it also lets them have access to employee medical information they need to conduct legitimate business functions. The problem is that the law doesn't tell you where to draw the line. That's a big problem, especially if you're the employer requesting medical information. Here's a 6-step compliance game plan to help you tell the difference between a legitimate request for employee medical information and an unwarranted invasion of privacy.

## Step 1: Recognize that Employees Do Have Privacy Rights Vis-à-vis Their Employers

Privacy laws like PIPEDA and provincial equivalents in Alberta, BC, and Québec impose limits on the use, collection, and disclosure of protected health information (PHI). However, whether those restrictions extend to the workplace varies by jurisdiction:

- **Employees do have statutory privacy rights** in AB, BC, QC and the Federal jurisdiction;
- **Employees don't have statutory privacy rights** in MB, NB, NL, NS, ON, PEI, SK, and the 3 territories.

But keep in mind that personal privacy rights don't derive solely from statutes. They can also be based on the Charter, case law, and/or the terms of employment contracts and collective agreements.

**Bottom Line:** You must be aware and respectful of employee privacy rights no matter what industry you're in or where in Canada you operate.

## Step 2: Recognize that Employer's Right to Conduct Business May Trump Employees' Privacy Rights

Privacy laws also include special rules governing an employer's collection, use, and disclosure of personal information about its own employees. For example, according to an official information sheet from the Alberta government, "An employer has a legitimate need to collect, use, and disclose certain types of personal information about employees in order to operate the business and fulfill its obligations as an employer."

**Basic Rule:** Employers generally have to get consent before collecting, using or disclosing an individual's PHI. But the employer doesn't have to get consent from an employee if:

- It collects, uses or discloses the PHI to manage the employment relationship; and
- It collects, uses or discloses the minimum PHI necessary to accomplish the purpose of such collection, use or disclosure; and
- It notifies the individual employee of the collection, use, or disclosure in advance.

The formula for compliance is to either get employees' consent to the collection, use, and disclosure of their PHI or ensure that you remain within the above 3 boundaries when collecting, using, and disclosing it without consent.

## Step 3. Ensure Collection/Use/Disclosure of PHI Is for a Legitimate Purpose

You don't need consent to collect, use, or disclose employees' PHI if you need that information to carry out a legitimate business or employment function. Examples:

- Verifying an employee's eligibility for sick leave and other forms of leave;
- Verifying an employee's eligibility for disability, health or other benefits;
- Determining whether an employee is physically or mentally fit to perform the essential duties of a job;
- Assessing an employee's physical and mental capacities for purposes of making reasonable accommodations or creating a return to work plan for an employee who has suffered a work-related injury; and
- Filing a workers' comp claim for the employee.

## Rule 4. Limit PHI Collected/Used/Disclosed to Minimum Necessary

Establishing a legitimate business need for an employee's protected information isn't carte blanche to go on a fishing expedition. You must collect, use, or disclose only as much and type of PHI you reasonably need to carry out that essential employment function. For example, you're generally allowed to ask employees who call in sick for a doctor's note verifying that they're really ill. But asking for a diagnosis would be problematic because it would exceed the scope of the information to which you're entitled. Making employees take a physical exam or submit a complete medical history because of one day's illness would also be inappropriate because it's more

information than you need.

But these are obvious examples. In the real world, situations are usually much more subtle. So, it's not surprising that there have been dozens of privacy complaints by employees claiming that the employer asked for more medical information than it needed. Examples:

**Employer Loses:** A transportation company's policy required employees on sick leave to get a doctor's certificate listing a medical diagnosis. An employee complained that the policy violated her privacy. The company claimed that it needed a diagnosis because its drivers often work alone, put in long hours, and need physical strength, agility, and alertness to do their jobs. But the employee in this case wasn't a driver but an office worker. Consequently, the federal Privacy Commission ruled that asking for a diagnosis violated the employee's privacy [*An individual challenged the requirement to provide the medical diagnosis on her doctor's certificate for sick leave*, 2003 CanLII 5181 (PCC)].

**Employer Wins:** A telecommunications company required any employee going on sick leave—even for one day—to submit a medical certification including a diagnosis. An employee complained that the policy was unnecessary and illegal. But the Commission disagreed. The company was administering both short- and long-term disability plans for its employees. Eligibility for both plans was based on the employee's diagnosis. So, the company needed to know each employee's diagnosis so it could run the plans [*Company's collection and disclosure of employee sick leave information*, 2003 CanLII 47746 (PCC)].

## Step 5. Notify Employees of Collection/Use/Disclosure in Advance

Collection/use/disclosure of employee PHI is authorized only when employees are notified in advance. Such notification should be put in writing and specifically describe the exact information you propose to collect, how you propose to use it, and to whom you propose to disclose it, your reasons for such collection, use, and disclosure and how long you plan to retain the information. That includes use of cameras, GPS, monitoring software, and other surveillance technologies to monitor employees while they do their job.

## Step 6. Limit Collection/Use/Disclosure to Terms of the Notification

The final key to ensuring compliance with privacy laws for use of employee PHI without consent is ensuring you limit actual collection, use, and disclosure to the terms set out in your notification. For example, don't provide sensitive medical information to an employee's supervisor if the notification says you'll disclose it only to health insurance personnel for purposes of determining the employee's eligibility for a certain type of medical coverage.