Receipt-based wellbeing allowances: privacy considerations.

buddlefindlay.com

BUDDLE FINDLAY

Introduction

Employers often adopt receipt-based wellbeing reimbursement models with the best intentions, aiming to support their employees' health and wellness. These allowances typically involve employees submitting receipts for reimbursement of health or wellbeing-related expenses. While this approach may seem straightforward, it can create legal risks if personal information is not handled appropriately.

It is important that employers are aware of their obligations under the Privacy Act 2020 (Privacy Act) when receiving receipts from employees for reimbursement for health and wellbeing-related expenses. This is especially important if those receipts contain sensitive health information about the employee (for example, details of visits to therapists, doctors or other health providers and what services were provided). Without clear policies, procedures, and transparency around how this data is managed, employers risk legal exposure, financial penalties, and damage to employee trust. This article highlights key privacy concerns and the importance of compliance with privacy laws when handling receipt-based wellbeing reimbursement programmes.

The Privacy Act and your responsibilities

Many employers are unaware of the privacy issues that can arise when managing receipt-based wellbeing reimbursements. Under the Privacy Act, employers are responsible for collecting, storing, using, and disclosing personal information in a lawful and fair manner. Reimbursement models often require employees to submit detailed receipts, which may contain sensitive health information.

Employers must ensure that the collection of this information is necessary for a legitimate purpose and that employees are fully informed about how their information will be used. Moreover, safeguards must be in place to prevent misuse or unauthorised access to this information. A failure to meet these obligations can result in privacy breaches, leading to legal consequences and a loss of employee confidence.

Privacy principles and their application to receipt-based reimbursement

The Privacy Act outlines a series of principles that govern how personal information should be handled. Receipt-based wellbeing reimbursements may present several potential risks in meeting these principles.

Collection of information (Principles 1-4)

As personal information should only be collected if it is directly relevant and necessary for the purpose at hand employers should carefully consider what information they reasonably require from an employee to enable the employer to facilitate the reimbursement of health and wellbeing receipts. The submission of detailed receipts may result in the collection of information that is not essential to the reimbursement process (for example, details or particulars of medical treatments, therapies or health services provided).

Employers must be transparent with employees about the purpose of collecting this information, what the employer will do with the information, who will have access to it, and what will happen if the information is not provided. Failing to communicate these details could breach the collection principles under the Privacy Act.

Storage and security of information (Principle 5)

Sensitive health information contained in receipts needs to be securely stored to prevent unauthorised access or misuse. If multiple departments or individuals are involved in processing these reimbursements (eg HR, finance), this increases the risk of sensitive data being accessed by personnel who do not need it.

Employers must ensure that only authorised individuals can access sensitive data, and appropriate safeguards should be in place to prevent any data breaches.

Access and correction of information (Principles 6-7)
Employees have the right to request access to their personal information and correct any inaccuracies. Employers must have processes in place to allow employees to exercise these rights effectively, ensuring that any incorrect or incomplete information is promptly rectified.
Accuracy and retention of information (Principles 8-9)
Employers must take care to ensure that the information they collect through receipts is accurate and up-to-date. Inaccuracies or incomplete data can lead to further complications, such as incorrect reimbursement amounts or improper data storage. Personal information should only be kept for as long as necessary to fulfil the purpose for which it was collected. Employers must ensure that receipts and any accompanying sensitive data are not retained beyond what is legally required or necessary for processing reimbursements.
Use and disclosure of information (Principles 10-11)
While there are some exceptions under the Privacy Act personal information can generally only be used for the purpose for which it was collected. Employers must avoid repurposing this information for unrelated reasons, such as monitoring employee health patterns or behaviour. Unauthorised disclosure of sensitive information can occur if privacy safeguards are inadequate. Employers must ensure that sensitive data is only used and disclosed to relevant parties for the purpose for which it was collected (unless an exception applies in the Privacy Act) and is not used or shared further without the explicit consent from the employee
Disclosure outside of New Zealand (Principle 12)
If personal information collected through receipts is disclosed to organisations or individuals outside New Zealand, employers must ensure that, where clause 12 is applicable, the receiving party has comparable privacy safeguards. This is crucial if third-party providers are involved in processing or managing reimbursement claims and will be using the information for their own purposes.

Real-world privacy risks

Even with good intentions, the collection and processing of sensitive personal information through receipt-based reimbursement systems can lead to unintended privacy breaches.

Below are examples of how privacy risks can manifest:

- **Sensitive data exposure**: An employee submits receipts for mental health services or other private health treatments and those receipts include health information or reference detail as to the health services provided. These receipts are reviewed by multiple staff members, exposing sensitive health information to more people than necessary, increasing the risk of a privacy breach.
- **Perceived discrimination concerns**: An employee submits frequent detailed receipts for medical treatment. This results in more information than is necessary being collected and accessible to a range of individuals within the organisation. If the employer later makes decisions about that employee's employment (e.g. non-promotion, redundancy or other termination), and the information has not been managed well, the employee may perceive that the decision was influenced by the employer's knowledge of the employee's health status which may lead to a discrimination claim.
- **Unauthorised access**: Inadequate security measures could result in unauthorised access to sensitive health data on receipts. This could lead to privacy breaches, legal action, and reputational damage for the employer if sensitive data is mishandled or leaked.

Conclusion

While receipt-based wellbeing reimbursement models may seem to offer a practical solution for supporting employee health and wellness, they come with privacy risks. Employers must ensure compliance with the Privacy Act by implementing robust privacy policies, safeguarding sensitive information, and maintaining transparency with employees.

Failure to comply with these privacy requirements could result in legal penalties and a breakdown in employee trust. Employers should carefully assess whether their reimbursement practices adequately protect employee privacy and consider steps to mitigate any potential risks.