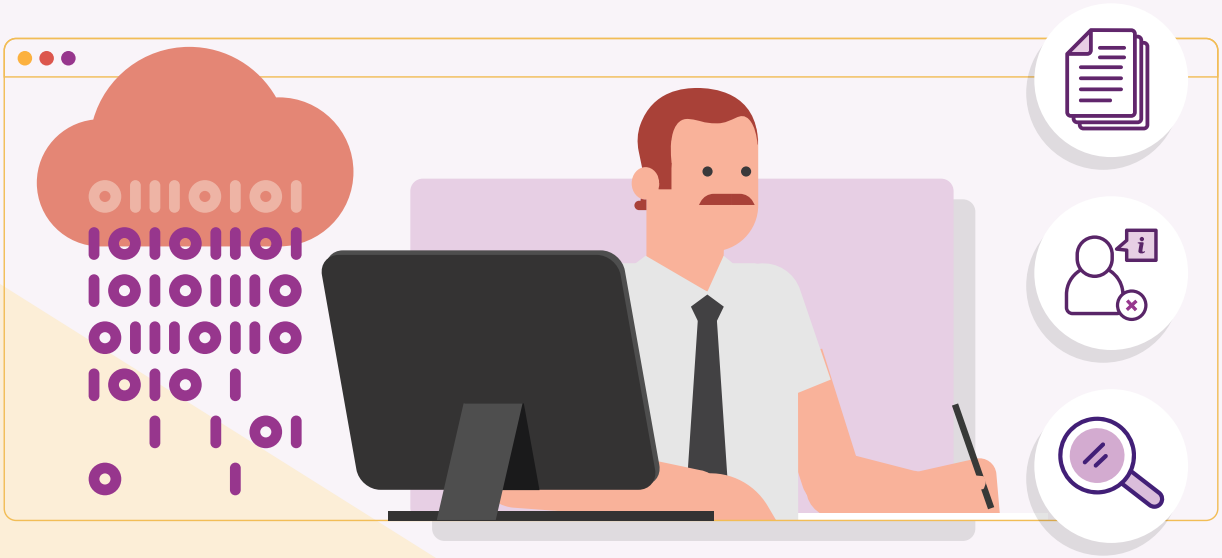

Misuse of sensitive client data for personal research

Guidance material – integrity scenario

This guidance material presents an 'integrity scenario' which is intended to assist in public sector training regarding integrity risks, highlighting the importance of clear policies and governance for data access and use in public sector organisations, especially those handling sensitive client information. In this scenario, a caseworker misused client data for personal research without obtaining proper consent. Although the caseworker's actions did not involve direct financial gain, they still constituted serious misconduct due to a breach of confidentiality and ethical standards. This scenario highlights the need for regular reviews of data access patterns, even for authorised users, and for periodic training that includes practical examples of data misuse.

The situation

A caseworker at a Victorian human services organisation managed sensitive cases involving families and children. Their role required maintaining strict confidentiality and using client information only for providing direct support and services to their clients. The caseworker was also studying family dynamics and child welfare as part of a university thesis.

How did the misconduct start?

The caseworker initially used client data only for their official duties, such as assessing needs and providing support to families. As their research progressed, they saw an opportunity to use client data to enrich their thesis. The caseworker believed that having real-world data would significantly improve the quality of their research, which they hoped would ultimately benefit the families they worked with by contributing to better understanding and services in the field.

However, instead of following proper procedures for obtaining consent to collect and manage personal information, the caseworker accessed sensitive client files without authorisation. They were motivated by a genuine desire to make a positive impact through their research but did not consider the ethical implications of their actions.

Over time, the caseworker became more convinced of the value of real client data for their thesis, to make their findings more relevant. They continued downloading client files, thinking that anonymising the data demonstrated an appropriate level of duty of care to their clients, not recognising the growing ethical issues in their actions.

How did it escalate?

A colleague observed an unusually high frequency of access requests from the caseworker, including at times outside working hours and on weekends, which raised concerns. The colleague reported their concerns to a supervisor, who then reviewed the data access logs. The supervisor discovered that the caseworker had been using client data for their personal academic research, which was unauthorised and violated confidentiality agreements and Victorian privacy legislation.

While the caseworker's intentions were not malicious—they aimed to improve their research and contribute to knowledge in the field—their actions were a serious breach of ethical and professional standards. The caseworker was subjected to performance management, received a formal warning and was reported to their university, which resulted in the disqualification of their entire thesis.

The organisation responded to the misconduct by promoting a culture that prioritises data protection and integrity. They implemented stricter controls on data access, required formal approval for any use of client information outside of official duties and provided additional training with real-world workplace scenarios.

Lessons learned

- Establish a clear policy and process requiring written approval for any use of client data outside official duties, ensuring that all data usage is properly authorised and ethical.
- Review data access patterns regularly to detect unusual or unauthorised activity early.
- Provide periodic training that includes practical examples of data misuse, ensuring that employees understand what constitutes a breach and how to avoid it.
- Foster an organisational culture where employees feel comfortable reporting concerns about data misuse or breaches. Ensure that there are clear, confidential channels for reporting and that employees feel safe coming forward.

This product was prepared based on findings from research and stakeholder consultations from IBAC's 2024 Public Sector Strategic Assessment. It is representative and created for educational purposes only. Any similarities to real persons, organisations, or incidents is purely coincidental.

If you experience or suspect public sector corruption, report it to IBAC

Fill out the secure online form to report at **www.ibac.vic.gov.au**

If you have difficulty accessing the online form, call us on **1300 735 135** for further assistance.

If you need help with translation, call Translating and Interpreting Service on **13 14 50** or visit **www.ibac.vic.gov.au/mylanguage**