Contact tracing

Do privacy right

Simply Privacy

Contact tracing is a vital part of our fight against Covid-19. To operate in Level 2 all businesses and workplaces need to keep contact-tracing records of anyone who will access or use your premises (workers, contractors or customers).

Whatever contact tracing method you choose, it's important to think about privacy so that people can trust you to protect their personal information. If they don't trust your method, they won't want to use it.

This guide will help you 'do privacy right' when contact tracing.

1. Minimise the data you're collecting

- ○ Only collect the personal information you need for the purpose of contact tracing – including a person's name, contact details, and the date and time they were on your premises.
- ○ You might also want to ask people to confirm that they don't have any Covid-19 symptoms or haven't been in contact with anyone who may have Covid-19.

2. Be open and transparent

- ○ Make sure people are aware that you're collecting personal information about them for contact tracing, and how you're doing this.
- ○ Tell people what personal information you're collecting, what it will be used for, who it will be shared with, what will happen if they refuse to provide it, and how they can ask for a copy of it.
- ○ You could do this by including a privacy statement on a register, via the workplace intranet, or by putting up a poster.
- ○ If you want to use the personal information you collect for contact tracing for another purpose, reconsider – people probably won't appreciate this. If you go ahead, make this other purpose very plain and clear.
- ○ If you are using existing systems (such as employee swipe card entry records) make sure this is known to users.

3. Protect the data and be accountable

- ◯ Keep contact tracing information secure from loss or unauthorised access, whether it is in physical or electronic form.
- ◯ Only those who need to access it should be able to.
- ◯ Take steps to make sure people can't see each other's information when they give you theirs.
- ◯ If using a contact tracing method provided by a third-party, check that:
  - they're a reputable provider and their method has not been criticised by others
  - their security is acceptable
  - they will not use the information for their own purposes/on-sell it (if they say they will only do this on a deidentified or aggregated basis, verify this, and think about whether this would meet people's expectations)
  - they can meet your retention/deletion requirements
  - they will tell you about a privacy breach and assist you with any investigation.

4. Remember people have a right to know

- ◯ Individuals have a right to access the personal information you hold about them and ask to correct it if it's wrong.
- ◯ You have an obligation to respond to requests for contact tracing information under the Privacy Act, and your contact tracing method needs to enable you to do this.
- ◯ People aren't entitled to access contact tracing information about others.

5. Make sure the data is accurate

- ◯ Contact tracing will only work if accurate and up to date personal information is available to contact people at risk.
- ◯ Make sure your contact tracing method is simple to use to encourage the collection of accurate information.
- ◯ If you're using existing systems, such as staff swipe cards, you need to have confidence the contact information you have for those users is accurate (or take steps to check it).

6. Stick to your purpose

- Only use contact tracing information for the purpose of contact tracing and only share it with the Ministry of Health and/or a District Health Board unless:
  - you made it very clear that you were also going to use it for another purpose/share it with someone else; or
  - you are legally allowed to (including under the exceptions to Information Privacy Principles 10 and 11).
- Only share the specific information that has been requested.

7. Get rid of the data when you're done

- Keep contact tracing information only for as long as it is needed for contact tracing purposes.
- WorkSafe suggests that this information should be kept for no longer than 2 months.
- Securely and permanently destroy the information when the time comes.

You can find us at **simplyprivacy.co.nz,**
or contact us on **info@simplyprivacy.co.nz**
for more advice.