

What to do if you are experiencing a data breach.

As a social care organisation, you have specific responsibilities you need to meet if you experience a data breach. This quick guide will tell you what steps to take.

What should I do?

You will need to start your investigation into what data was involved in the breach. If this is a breach in your own organisation, for example a care plan has gone missing you should investigate with your internal team. If this is a breach which one of your software suppliers is experiencing, you should speak to them about which data is impacted.

You will need to review to identify the scale of the possible personal data breach and the impact it will have on affected individuals. You must then report that the confidentiality of personal data has been breached.

How should I report this breach and to who?

You must report any confidentiality breach in line with your local incident reporting procedure. You must report this to the Information Commissioner's Office (ICO) [ICO website](#) immediately and within 72 hours of becoming aware of it. This is the case even if you have already reported a breach due to data being unavailable.

All CQC registered providers should also report this confidentiality breach via the Data Security and Protection Toolkit (DSPT) [DSPT website incident reporting tool](#). If you are not registered, you can do so on this website.

Once you are signed in, you should look for the "report an incident" menu link. The tool will guide you through a number of questions, for example, what has occurred, when the attack occurred and the severity of the impact of the confidentiality breach.

Once you have reported it on the DSPT, you must email the ICO to confirm you have submitted a report via the DSPT.

Do I need to inform staff and the people we support about this confidentiality breach?

Whether or not you need to inform individuals is determined by the impact of the breach on them. If the impact on individuals is significant, you will need to contact those who are affected by the confidentiality breach. For example, if confidential care data or security data is impacted, you will need to contact affected individuals because this is likely to result in a high risk to their rights and freedoms. The DSPT reporting tool includes questions to help you determine the level of impact please see link [DSPT website](#). The ICO also provides guidance on personal data breaches [ICO website](#).

When informing an individual of a breach, you should describe, in clear and plain English, what has happened and at least:

- the name and contact details of any Data Protection Officer you have, or other contact point where more information can be obtained
- a description of the likely consequences of the personal data breach for the individual
- a description of the measures taken or proposed to deal with the personal data breach and a description of the measures taken to mitigate any possible adverse effects, for example resetting passwords or codes

You will need input from your senior management and staff who know the people you support and their individual circumstances on the best way to communicate the necessary information about the breach. They may also be best placed to advise on any mitigating actions, for example relating to any change to access arrangements to individual's homes.

Careful consideration needs to be given to how to communicate the breach to individuals who may be vulnerable. Care organisations will need to determine how best to inform vulnerable individuals on a case-by-case basis. If you think a person may not have the capacity to understand the impact, you should inform someone who can support them with any steps that need to be taken, for example their next of kin, individual with lasting power of attorney, or care professional.

What other actions should I take?

You should consider locally what data has been impacted and whether any further steps should be taken to mitigate the risks. For example, if access codes to service users' properties are at risk you may wish to contact impacted individuals to ensure that their access code is changed.

You should also consider notifying any Local Authority, which you have a contract with to provide care services, about this confidentiality breach if it relates to individuals who are covered by the contract.

In certain circumstances individuals can seek compensation for personal data breaches. You should consider whether you need to notify your insurance company or seek legal advice.

Where can I get more help if needed?

The ICO have guidance and a [reporting line](#).

The [IG Portal](#) and the Digital Social Care website [Digital Care](#) also have lots of information to support providers on managing their data and information governance.

[The National Cyber Security Centre](#) has also published guidance for individuals who have been the subject of a data breach which may be helpful.