* A blue square on a black surface

  Description automatically generated

# Advanced System Outage - Information Governance (IG) Guidance for Adult Social Care Providers

# Background

As we advised in our [update](https://www.digitalsocialcare.co.uk/update-on-the-recent-external-cyber-incident-from-the-digitising-social-care-team-in-the-nhs-transformation-directorate/) posted on the Digital Social Care website, Advanced, a third-party software supplier, has advised us that they have been subject to an external cyber attack. Advanced has confirmed to customers that this is as a result of a ransomware attack in an update posted on their [website](https://www.oneadvanced.com/cyber-incident/#updates).

Advanced has also published an update for each service on their [website.](https://www.oneadvanced.com/cyber-incident/)

While an investigation is carried out Advanced has isolated all services and taken them offline to mitigate the risk of further impact. This means that their customers will have lost access to a number of different systems.

The affected systems are:

* **Caresys –** a care home management software
* **Crosscare** – a clinical management system for hospices and private practice
* **Staffplan** – a care management software
* **eFinancials** – a financial management software

There has been no immediate cyber security threat to NHS or adult social care systems identified as a result of this ransomware attack. The attack was not targeted against the NHS or any specific organisation, rather the third-party software provider. While Advanced works to resolve the availability of their software caused by this cyber incident, the NHS immediately put in robust defences to protect our own networks – this is in line with cyber security advice.

The National Cyber Security Centre is supporting Advanced with the investigation and response to the cyber-attack. The priority is the knock-on impact of the systems listed above being offline for affected providers, particularly where this relates to access to care records and financial systems.

There is an ongoing investigation into the attack both looking at the cause and potential impacts around cyber and data security. Advanced has advised “With respect to potentially impacted data, our investigation is underway, and when we have more information about potential data access or exfiltration, we will update customers as appropriate. Additionally, we will comply with applicable notification obligations.”

# What are the potential IG impacts and what should I report?

There are several different potential impacts. How these should be reported are set out below. If there is an impact upon the availability of the data, you should have reported what you knew at the time of the attack. If you haven’t done this, you should do so as soon as possible as set out in this guidance. You may have to submit more than one report if things change. This guidance will be updated if we become aware of any significant change at a national level.

## Cyber incident

Advanced is responsible for notifying you, as their customer, about the attack and impact upon service if one of your systems has been impacted. Advanced has informed the Information Commissioner’s Office (ICO) about the attack so you do not need to separately report this. If there is an impact upon the availability of data you may need to report this as an adequacy breach (see below).The ICO is the UK’s independent body set up to uphold information rights.

**Availability of data**

If data has been made unavailable as a result of the cyber attack, this may be considered an adequacy breach and you should report this via the Data Security and Protection Toolkit (DSPT) (see below).

The rating you give will depend on the system which has been impacted. For example a high rating would be likely for a situation where your care data is unavailable and this has led to difficulties in providing care because you do not have access to an individual’s record.

# How should I report an adequacy breach?

You must report any adequacy breach in line with your local incident reporting procedure. Your local reporting procedure may involve completing a form or notifying senior staff.

All Care Quality Commission (CQC) registered providers should also report this adequacy breach on NHS Digital’s reporting tool, which can be accessed via the [Data Security and Protection Toolkit](https://www.dsptoolkit.nhs.uk/Account/Login). If you are not registered, you can do so on this [website](https://www.dsptoolkit.nhs.uk/Account/Register). This will ensure that we can monitor the impact nationally. 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.

Once you have reported it on the toolkit, you must also report it to the ICO. You should use the [data breach reporting form](https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach) on the ICO website at and send your breach report form to the dedicated inbox at [Advanced@ico.org.uk](mailto:Advanced@ico.org.uk)

# When should I report this adequacy breach?

You must report any adequacy breach immediately and within 72 hours of becoming aware of it. You may not have reported the adequacy breach because you did not recognise that an adequacy breach includes instances where there is an impact on the availability of personal data. If this is the case you should report the adequacy breach as soon as possible.

# Do I need to inform service users about this adequacy breach?

Where people drawing on care are impacted, you should consider making them aware and you will need to assess the best way to do this. If you think a person may not have the capacity to understand the impact, you should inform their power of attorney (or if appropriate a named deputy). You should take into account the following:

For issues relating to the availability and accuracy of the data you could make information available on your website or noticeboard. We have included some template text for you to use below.

If there are higher than average calls coming in then consider including a message on your phone system to inform callers that it may take longer than normal for you to respond. It is likely where there is a high impact on individuals drawing on care that you will be communicating directly with them or where appropriate their power of attorney or deputy in the course of your service provision to them.

Organisations impacted by the cyber attack may find it difficult to respond to [subject access requests](https://transform.england.nhs.uk/information-governance/guidance/subject-access-requests/) in the usual timeframes. A subject access request is when someone asks for access to their personal information, for example a copy of their social care record. Where this is the case, you should inform the individual who is requesting access of the expected delay, the reason for the delay and when you believe you will be able to provide the information to them. You should keep them informed throughout the process.

You may need input from your senior management on the best way to communicate about this. As some of the individuals impacted may be vulnerable, care professionals will need to determine how best to inform them.

# What other actions do I need to take?

Your organisation may have to use an alternative system, such as on paper or on a different electronic system, for making records as a result of the unavailability of data. You must ensure that information entered on any back up system is accurate, made available to the relevant staff when needed, and stored securely. You should consider any risks to the back up system, which may include using out of date data from existing paper records or other systems, or the potential for missing out necessary details when recording new information.

Once a local decision is made to reconnect the Advanced system, you must ensure that any recorded information on paper or another electronic system is appropriately transferred to the Advanced system.

# Where can I get more help if needed?

For IG related support you can contact - [datapolicyhub@nhsx.nhs.uk](mailto:datapolicyhub@nhsx.nhs.uk)

If you need support from the Information Commissioner’s Office you can contact their dedicated mailbox - [advanced@ico.org.uk](mailto:advanced@ico.org.uk)

If you require immediate advice and guidance related to a cyber security incident, please contact the NHS Digital Data Security Centre on: 0300 303 5222.

The [IG portal](https://transform.england.nhs.uk/information-governance/) and the [digital social care website](https://www.digitalsocialcare.co.uk/) also have lots of information to support providers on managing their data and information governance.

**Template website or noticeboard text**

Advanced, a third-party software supplier, has advised us that they have been subject to an external cyber attack. As a precaution, some of the software that is used by care providers has been taken offline.

The system(s) impacted at our organisation is [add system name(s) and description(s) from following list:

Caresys – which we use for care home management

Crosscare – which we use for clinical patient management

Staffplan – which we use for care management

eFinancials – which we use for financial management]

This means that we cannot access the system(s) we usually use or have our usual access to the information needed to support people who receive care from us. However, we can assure you that we have plans in place to ensure our services continue to operate. As these measures are more labour intensive, it may take us longer to answer the phone or respond when you contact us.

We are working closely with Advanced to restore services and to ensure that we only reconnect services when it is safe to do so. This process is standard practice for a complex incident of this nature, so it may take some time. [Add anticipated timescales for resolution if known, for example we currently anticipate that it may take at least three to four more weeks for systems to be restored, but we are working to resolve this quicker where possible. Advanced has also published an update for each service on their [website.]](https://www.oneadvanced.com/cyber-incident/)

As with any cyber-attack of this nature, there is an ongoing investigation into the attack to fully understand the impact. Rest assured that Advanced, the NHS and Adult Social Care organisations will comply with the strict requirements around reporting concerns about data.

We will provide you with an update once the situation changes. On behalf of [organisation name], I apologise for the impact this has on you.