Advanced Systems Outage: Information Governance Guide for Social Care Providers in Scotland

29 August 2022

Contents

What has happened?

Advanced, a third-party software supplier which provides a number of systems used across the social care sector, has been the victim of a ransomware cyber attack.

What is the impact on the social care sector?

While an investigation is carried out Advanced has taken some services offline. This means that customers may not be able to access:

- **Adastra** – a clinical service user management software application
- **Caresys –** a care home management software system
- **CareNotes** – an electronic service user record software application
- **Crosscare** – a clinical management system for hospices and private practice
- **Staffplan** – a care management software application
- **Odyssey** – a clinical decision support application
- **eFinancials** – a financial management system

Business continuity measures have been put into place to minimise the impact on care, however these processes may involve more manual tasks, requiring additional staff and/or increased time for care and support to be delivered residents/service users.

What action is being taken?

Advanced is working to restore access to these systems, supported by the National Cyber Security Centre and updates on each service are being posted on Advanced's website.

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."

More information will be shared as it becomes available.

What are the potential information governance (IG) impacts and what should I report?

We are still in the emergent phase of this cyber attack, and it is not fully clear what the full range of impacts may be. It is advisable to prepare for a wide range of scenarios, and guidance on the steps providers may need to take is set out below.

A personal data breach can involve one or more of the following:

- Confidentiality breach – where there is an unauthorised or accidental disclosure of or access to personal data.
- Availability breach – where there is an accidental loss of or access to or destruction of personal data. An example of this would be the sort of problem that would arise after a cyber-attack that prevented access to and/or destroyed records.
- Integrity breach – where there is unauthorised or accidental alteration of personal data.

Currently this incident constitutes an 'availability' breach, where there is an accidental loss of, loss of access to, or destruction of personal data.

Advanced has informed the Information Commissioner's Office (ICO) about the attack. Advanced, as your data processor, is responsible for notifying you as the data controller about the cyber attack and the impact upon service if one of your systems has been affected. If your systems have been affected, your Data Protection Officer (DPO) will need to notify the ICO by email to advanced@ico.org.uk. As the situation develops, you might have to make additional notifications.

Do I need to inform service users about this?

Data protection law requires that, where a personal data breach results in a high risk to the rights and freedoms of data subjects, they are informed. This may also trigger Duty of Candour processes.

At present there is no apparent requirement to inform service users as high risk has not yet been identified. This may have to be re-assessed by each organisation as more information becomes available.

If it is confirmed that this incident affects service users within your organisation, action should be taken in line with your organisation's existing processes. Please contact your IG Teams/DPOs for further advice as there may be a requirement to notify service users in due course, if further information provided by Advanced leads to an assessment that there is a risk to their rights and freedoms. This will allow data subjects to take further action to protect themselves for any adverse impact of their information having been accessed by unauthorised persons.

Media enquiries related to this incident should be directed to your communications team or leadership team.

What other actions do I need to take?

You might have already had to implement local business continuity measures. It is essential that appropriate clinical records and other documentation are maintained within those frameworks. You may wish to risk assess any business continuity measures and any return to business as usual. Advice should be taken from your DPO.

Once a local decision is made to reconnect to the Advanced system, you will need to consider how information that has been recorded by other means, through business continuity measures, is captured appropriately within the clinical record.

Where can I get more help if needed?

Please contact your organisation's DPO or IG lead in the first instance. You may also be able to access support from care sector umbrella organisations, if you are a member. If needed, DPOs can also access support from the Scottish Government Digital Health and Social Care

Hub (DHCPolicyHub@gov.scot) or the Information Commissioner's Office via their dedicated mailbox (advanced@ico.org.uk).

What happens next?

As this is a live incident, the situation is developing at pace. Updates relating to IG-related responsibilities and action required will be shared with care providers as it becomes available.