Secure File Transfer – Interim Guidance for Service Providers

Purpose

Transferring files through unsecured networks can compromise sensitive client information and data. As an organisation delivering human services, it is important you and your employees understand the risks and follow the good practice to protect client information.

The Department of Communities and Justice (DCJ) is currently assessing long-term solutions for secure file transfers and data exchange to the DCJ. In the interim, here is some general guidance to meet immediate needs.

IMPORTANT NOTE:

It is essential that your organisation assess your compliance to legislative and contractual requirements and undertake any due diligence for technology solutions including those outlined to ensure they meet operational security and privacy needs.

Privacy principles

The minimum controls for sharing sensitive information include:

- Only disseminate information (personal and/or health) for authorised purposes.
- Assess the information and do not 'over share' – only include what is necessary for the purposes of your work.
- Ensure that recipients, including third-party organisations, have appropriate policies, procedures and systems in place to manage personal information, as well as relevant clearances such as a Working with Children's Check.
- Ensure your network is secure and you are using an approved work device – if you are working remotely, avoid using public Wi-Fi or use a VPN if necessary.
- The use of emails should be limited – emails are unable to be encrypted or restricted, which makes them vulnerable to errors in transfer or possible cyber threat actors.

- Phone calls are subjective to interpretation and should not be used unless the caller's identity has been confirmed and the caller has a right to know.

How to share files safely

DCJ is working to develop processes that enable data to be uploaded directly into data management systems such as ChildStory and Infoshare. Where these systems are not suitable or available for your business needs, a secure online sharing platform should be used.

While further analysis is needed to identify preferred options, we have assessed and are currently using platforms such as Kiteworks and SharePoint. Services such as Dropbox, Google Drive, iCloud and personal OneDrive are not secure and should be avoided.

1 - Kiteworks

As a dedicated Private Content Network, Kiteworks ensures privacy protection and regulatory compliance. It provides a single point of control to manage, monitor and audit the exchange of confidential information.

Kiteworks is currently being used by DCJ to facilitate the safe exchange of sensitive data with some service providers.

2 – SharePoint

SharePoint is a web-based application used to store, organise and share information with internal and external parties. It includes accessibility controls which can be applied site-wide, to specific files/folders or to nominated groups.

SharePoint is included in the Microsoft Office 365 suite. It has been approved as a secure platform for file sharing within DCJ, but we are still in the early stages of development.

If your organisation has SharePoint, you can use the site to transfer information providing the following controls are in place:

1. Access to the file location must be restricted and only viewable/accessible by employees who require direct access to the information.

2. When sharing files, you must select 'specific people' or 'people with existing access' through designated user groups. You must not share to 'anyone with the link' or 'people in your organisation with the link'.

3 - Physical transfer and USB

Person to person sharing may be appropriate for the exchange of physical files. In these circumstances, the information must be stored securely in transit and held by authorised persons.

Sensitive information can also be stored on a Universal Serial Bus (USB) provided the USB has been encrypted and the information is deleted immediately after transfer.

Naming protocols

It is important that you consider security and exclude any identifiable information when naming a document, folder, email or physical files.

- Do not use client names or identifying information in an email title, body or attachments.
- For service delivery information in an attachment, encrypt with a password and send the password via a separate channel (as distinct from a separate email).
- If client names or other personal/health information are included, you must use a secure platform, as outlined above.
- Physical files should be stored in a sealed opaque envelope or similar. No classification or identifying information should be displayed on the envelope.

Data breaches and incidents

A data breach or allegation of a breach, which includes the inadvertent or malicious loss, disclosure or corruption of client information, must immediately be notified to DCJ.

If a data breach occurs, your organisation will be required to work with DCJ to:

- investigate the nature and extent of the breach;
- assess the risks and consequences associated with the breach;
- notify relevant regulators (NSW Information and Privacy Commission, the Office of the Australian Information Commissioner, Cyber Security NSW); and
- review the circumstances of the breach and participate in action to mitigate the risk of any future breach.

Any complaints received in relation to a data breach or breach of privacy must be handled in accordance with the PPIP Act and HRIP Act. This will require you to conduct an audit or investigate the circumstances that gave rise to the breach promptly.

Where improvements to your policies and practices have been identified, we will ask you to share findings and let us know when matters have been addressed.

Additional support

For more information and key resources on privacy, information management and cyber security, please visit our webpage:

Maintaining secure information and notifying us of information security incidents