Mental Health Tribunal for Scotland

Data Protection and IT Supplement

Data Security Update - Important

The way in which we all work has changed significantly over the last two years, however one thing that remains is the importance of data security. Now, more than ever, we need to remain hyper-vigilant in ensuring that we follow the processes that are in place for handling confidential data.

There has been a recent real life example of why we all need to have the topic of data security at the forefront of our thoughts when dealing with confidential information. A Tribunal member was the unfortunate victim of a cyber-attack which was part of a wider attack on an organisation they worked for. The attack resulted in files relating to MHTS cases being harvested maliciously – along with many other files from the organisation's servers. The files were able to be taken as they were stored on the organisation's servers, which were not encrypted, and the files had not been deleted after they had been downloaded from the website and printed.

Although this incident is an extreme example of problems that can occur, it serves to highlight what can happen. There are three main points to highlight from this incident. Firstly, and something that every member should be abiding by, is that you should only ever use a device that has the appropriate level of encryption active on it. Everyone should currently be using a device that is suitably encrypted - there was an email update sent out regarding encryption on 18 February 2022. The content of this is repeated below.

Secondly, and this will be relevant to those who use a suitably encrypted device which belongs to their employers (such as the NHS or a local authority), you must only save files to the hard drive of the device and not to a shared server. If documents are saved to a shared server, such as a P:drive, it completely defeats the purpose of having encryption on a device, as the encryption only protects information that is stored on the device's hard drive. If information is stored on a server, it is only protected to the extent of the security which is on that server.

Lastly, you should not save data on your device for any longer than necessary. If you are printing papers from the members' website, ideally you should not have to save these papers to your device prior to printing. You can access the website, open the files you wish to print, and then print directly from there without the need to save the files before printing. If there is a reason that you are unable to print directly from opening the files from your member's account, you should save the files, print them, and then delete them immediately after this – also emptying your Recycle Bin to ensure files are removed completely. Case files will remain on your member's account until after the hearing date if you need to refer back to them. If you require to save documents to your device as you plan to view them on your device rather than printing them, then you must ensure that you delete the documents when the case has concluded – again also making sure to empty your Recycle Bin.

You should also routinely check your device to make sure files are not being stored anywhere unbeknownst to you. For example, when you open a file from the members' area, this file can sometimes be automatically saved to the 'Downloads' folder on your device. You should check your device for a 'Downloads' folder and ensure there are no MHTS files sitting there.

On top of the encryption software that your device should have, you should ensure that your device has up to date anti-virus software on it as well as making sure to keep other software on the device up to date – this includes the operating system, internet browsers and Adobe software. Ensuring all these are up to date will provide your device with a high level of protection at all times.

Separately from the website and downloading papers, it is worth providing a reminder to everyone that when taking part in a hearing by teleconference you should ensure you participate in hearings from a room where you are alone (and will not be overheard). More generally, we are all spending more time with laptops open, accessing sensitive personal data in our own homes. At all times, we must remain attentive to the need to protect the security of this information.

I will leave you with the following six points to keep in mind as you continue your work for the Tribunal over the next year and beyond.

- Do – ensure your device has the appropriate encryption software installed on it
- Do – routinely check your device for saved files that are no longer required
- Do – take the appropriate level of care when in possession of confidential data in a public setting
- Do – report any losses of data immediately to headquarters in Hamilton
- Do not – store or save any confidential files on a shared server
- Do not – retain any confidential data longer than is necessary

Scott Blythe
Tribunal Liaison Officer

Content of email referred to above – The use of encrypted personal devices

The Scottish Courts and Tribunals Service (SCTS) has recently undertaken a review of the advice given to members of the Mental Health Tribunal for Scotland (MHTS) regarding the use of encrypted personal devices to access and download case papers. As you will be aware your device must meet the required standard of encryption in order to use it to access Tribunal paperwork. Each of you will currently be using a device which meets the required level of encryption as prescribed by SCTS IT department.

Previously, SCTS recommended and provided MHTS members with access to Symantec Encryption Desktop software which allowed members to encrypt their (Windows) devices and ensure that sensitive case papers could be sent securely and electronically. However, it is recognised that Symantec Encryption Desktop software can be quite complicated to install. As Tribunal members' personal devices are not managed by SCTS, there is also a risk that issues may arise if the software is installed

incorrectly or is incompatible with other software already installed on the device – particularly other encryption software.

Going forward, if you decide to change to a new device which you intend to use to access your tribunal papers, we would ask you consider one of the following two options;

1. Buy an Apple device, like a MacBook. Apple devices come with a built in encryption called FileVault(2) that is very easy to activate and means you don't have to add any software to the device – it is simply a matter of activating FileVault(2) as it is not automatically switched on.
   or

2. Buy a Windows operated device that has Windows 10 **Professional** Operating System on it. With Windows 10 **Professional** you have built in encryption on the device called Bitlocker – it is simply a matter of activating Bitlocker as it is not automatically switched on. Again this means you wouldn't have to install additional software on to the device. Most devices won't come with the **Professional** version as standard, but you can request this to be added/upgraded from whoever you are buying the device from.

If you change to a new device which does not fall under one of the two options above, it will mean that you have to upgrade your new device to meet the required encryption specification, and this will come at a cost which will not be reimbursed by MHTS.

If you are considering getting a new device at some point in the future, please feel free to contact me and I can advise further where appropriate.

'Tribunal Members' Search' Function on the Website

Most of you will be aware that there is a function within the members' area of the website that allows you to search for other members. In doing this search you will be able to find other members' contact details, such as telephone number and email address, for when you require to contact them in relation to tribunal work.

We have had some queries recently from members unable to find the contact details of another member. So I thought it would be helpful to provide a short guide on using this search function.

Firstly, to get to the search function you should log in to your member's account and go to the section titled 'Tribunal Members' Search'. You will find this page in the sub menu on the left hand side of the page, as shown circled red below.

When you arrive at the 'Tribunal Members' Search' page, you will see two fields. One is a drop down called 'Using Member Type' which contains various options to search by, the other field called 'And / or Member name' which allows you to type in the name of the member you are looking for.

With regard to the drop down menu, there seems to be one common error that is preventing the successful search for members. The drop down menu will automatically be set at 'SELECT' (red arrow below). If you try searching for a member by typing in their surname with the drop down still set to 'SELECT', the search will provide no successful returns. The simplest thing to do is to choose 'ALL'

(blue arrow below) from the drop down menu, then type in the member's surname in the 'And / or Member name' box, then click search. You will find that your search is successful if you follow this guidance.

One point to note is that the effectiveness of this function relies heavily on each member ensuring that their contact details are kept up to date. Each member can update their own contact details on the 'Update Profile' (green arrow above). You can update your telephone number and email address in this area, and you can also change your password, if you wish.

Scott Blythe
Tribunal Liaison Officer