KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

Data Protection Officer Newsletter

July 2021

Minor Amendment to Norwich Social Prescribing Information Sharing Protocol

The previous Information Sharing Protocol for the Norwich Social Prescribing project described how information is shared with the component members of the Social Prescribing Consortium. Recently, it has been agreed that Age UK will also be a recipient of social prescribing referrals. The Protocol has been amended to reflect that and we have also added in the NCAN referral system. Please ensure that the relevant staff members are provided with the updated Protocol.

MyDpo

Most of you will be familiar with MyDPO as the Kafico website area just for our customers. The space allows us to share key documents with you such as policies and recorded training sessions.

We have recently updated this part of our site and wanted to welcome you to the new MYDPO! Simply go to www.kafico.co.uk and select MyDPO in the top menu. The new password is Mydpo21 (this log in is shared across the customer base since there is no personal data and no requirement to audit access) and we would ask that you do not share with non-customers.

The site allows you to do a number of tasks directly;

- Contact us about training.
- Report incidents.
- Obtain branded policies directly.
- Complete your Processing Activities Log (Beast).
- Create a practice systems list.

• Complete your annual audit.

• Read recent newsletters.

We welcome any feedback or items you would like to see added.

Inappropriate Staff Access

There has been a spike in the number of inappropriate access incidents being reported to us.

We understand that staff are overwhelmed and that mistakes are made, however, these incidents are highlighting an upward trend in this type of activity involving staff.

We would advise ensuring that innapropriate access discussed at the next practice staff meeting and that staff are reminded that they do not have permission to access practice information (including patient records) for any purpose that falls outside the scope of their employment and is against both the Data Protection Act 2018 and the Computer Misuse Act 1990.

Furthermore, that access to their own or family / friends / colleagues is not permitted unless the access is necessary and approved by the practice (not the patient).

New Starter Data Protection and Security Induction

The new MyDpo includes a link that creates an email for your new starter and attaches a link or copies of your practice Data Protection and Security Policies, the DPO contact details, the employee Privacy Notice and basic information governance advice. When you have a new starter, visit MyDpo and go to Employee Compliance to use this link!

Compliance Review Started for COVID-19 Risk Assessment Tool

This project implements a tool designed by QCovid which enables an informed conversation between the medically trained professional and their patient about the nature and extent of their health risks in relation to coronavirus infection, this is done via a evidence based risk prediction model.

The outcome for patients is that their clinician may gain a better understanding of their risks of infection and potential consequences for them of infection with coronavirus and the clinician is better able to advise the patient of their risks through a clinical consultation.

This may include advice on shielding, weight management and other health and lifestyle considerations. This can potentially could enable the country to better manage patient safety in light of the pandemic and potentially prevent further restrictions like national lockdowns.

Kafico have started the compliance review and will update practices in due course.

The Risks Around Shared Logins

We are having reports that staff are sharing NHS Mail accounts and logging into EMIS / S1 with generic accounts.

There are huge risks around the use of staff sharing a user account on a computer. Some of these are security risks, others are legal/liability risks. Using stories from the media we will explore some of these risks and examine how to avoid them.

Firstly, we must recognise why this might be happening in the first place. Some organisations may consider the time and expense associated with maintaining individual accounts for each employee as “not worth it”. Maybe, it is simply easier to

have a shared user account when all employees need access to the same important files. Companies may be waiting on IT or a manager to improve logins – giving shared logins until this is done. Or perhaps it's simply that "That's the way it's always been". Despite the perceived cost saving or the convenience associated with these reasons, the amount of security and compliance risk that this practice poses to your organisation cannot be stressed enough.

Now, let us now explore the main risk areas in more detail:

Accountability

When any person signs on as the shared user account, there is no way for the audit log to be able to determine which member of staff carried out a particular action. This makes the audit trail effectively useless. If there was an investigation into the actions of a particular user, especially in a medical environment, you would not be compliant with best practice or potentially the law, which will expose your organisation to litigation and costs associated with forensic investigations.

Security

The shared system's password is protecting unauthorised people from accessing its contents and the network. Constant thought needs to be put into who has access to the password, how those people are getting that password told to them, and most importantly, are people who no longer need access to that account, such as an ex-employee, still able to log in? If one account gets compromised then this could have a butterfly effect on other user accounts, especially if it is an administrator account which can affect other users.

An example of this is The Comodo Breach. Comodo is a company which specialises in cybersecurity solutions and aims to help their clients prevent cybersecurity breaches. However, even the experts can get it wrong through carelessness and not putting thought into the risk posed around shared logins.

So, what happened? Comodo used one account for its Microsoft cloud services, meaning that a single set of credentials was shared between multiple employees. The Microsoft account also lacked multi-factor authentication, meaning that any

employee (or hacker) with the right credentials could retrieve Comodo's confidential internal documents without further verifying their identity. A software developer at Comodo with access to the shared account inadvertently uploaded the credentials to a public GitHub repository, exposing Comodo to third party actors.

This demonstrates how shared logins are a single point of failure, which severely compromise accountability and can lead to exposure of you and your organisation resulting in devastating cybersecurity costs, fines and potential litigation.

Please contact Kafico if your organisation would like further guidance and support on moving away from using shared logins. Do put your hand up at your organisation and identify this risk as it may prevent massive issues down the road.

Kafico Awards

2021 will see the inaugural year of the Kafico awards. Each award represents an element of our company core values which are: "Inspire Confidence, Not Panic Bring Solutions, Not Problems. Challenge Yourself Support Each Other" Help us to recognise our team for their awesomeness! If one of our team embodies any of our values in their work with you – feel free to Nominate them! (Submissions are anonymous).