CYMORTH LLYWODRAETHU GWYBODAETH AR GYFER GOFAL SYLFAENOL

INFORMATION GOVERNANCE SUPPORT FOR PRIMARY CARE

IG Guidance on

Printing within NHS Wales Applications for Community Pharmacies

Introduction

Information Governance (IG) is a framework which supports how organisations and individuals manage the way information is handled. It applies to sensitive and personal information of employees, patients, and service users. It is about setting a high standard for the management of all information and giving organisations the tools to achieve that standard.

Applications within community pharmacy which print through Citrix (via the Community Pharmacy Gateway – CPG) or via Multi Factor Authentication (MFA) include Choose Pharmacy, the Welsh Immunisation System and NHS Wales Email Service.

- Citrix access – only possible via the pharmacy N3/HSCN connection (on-site)
- MFA access – enables access either onsite via a non-N3/HSCN connection or off-site

When printing through Citrix the data file is converted to a pdf which is downloaded as a temporary file onto the device prior to printing. An IG risk arises when this contains sensitive or personal information as the information can be accessed by anyone with access to the device, with no audit history, allowing for potential inappropriate access. The information would also be accessible if the device was ever lost or stolen, or if secure destruction methods were not followed, increasing the risk of a potential personal data breach.

This guidance aims to support community pharmacies in mitigating the IG risks when printing personal information through Citrix and via MFA.

Personal Data and Special Category Personal Data

The organisation has a responsibility to process personal data with an appropriate level of security. Personal data is any information relating to an identified or directly or indirectly identifiable individual, this includes an identifier (i.e. name), identification number, location data, online identifiers, and factors specific to the individual which could identify them.

Special category personal data must be processed with an additional level of security, it is sometimes referred to as sensitive information. Special category personal data is information which reveals an individual's racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, and data concerning an individual's sex life or sexual orientation.

Examples of documents that would include personal data include, but not limited to:

- Prescriptions sent via email to the pharmacy in an emergency situation;
- Choose Pharmacy consultation records;
- Emails/attachments that include personal information relating to staff or patients.

Actions to mitigate IG risks when accessing NHS applications via Citrix

Pharmacy users should only print those documents where there is legitimate need to do so. Where printing is necessary, the following actions must be taken:

1. Use of Appropriate Devices

Only organisational owned devices should be used when printing through Citrix. Controls have been put in place within the Choose Pharmacy application to disable remote printing, devices must now be connected to N3/HSCN to print through the application. Users must not connect personal devices to N3/HSCN.

2. Deleting Temporary Files

After printing, the downloaded pdf must be deleted from the device. The process for removing the downloaded pdf or 'temporary file' from the device varies depending on the internet browser used within the organisation. The preferred option is for the browser settings to be set to automatically clear temporary files on exit, alternatively users can manually clear the temporary files as required.

Please see the link below for step by step guidance on clearing temporary files for each browser:

Details on how to clear the browser cache (temporary internet files) - Digital Health and Care Wales

Actions to mitigate IG risks when accessing NHS Wales applications via MFA

Pharmacy users accessing NHS Wales applications via MFA must receive organisational approval prior to using personal devices for this purpose.

The need for pharmacy users to access NHS Wales applications offsite is limited and staff should only do so where there is a need to access information to provide immediate patient care. This means that:

- Community pharmacy employees must not download Outlook or any other Microsoft applications linked to their NHS accounts to personal devices without explicit approval from their community pharmacy employer. Where approval is granted, pharmacy users must ensure that any access is in accordance with the NHS Wales Microsoft 365 Acceptable Use Policy for Primary Care Service Providers, the NHS Wales Email Use Policy for Primary Care Service Providers and the relevant organisation policies relating to the use of personal devices, information governance, information security and remote working;
- Community pharmacy employees must not access NHS clinical systems via MFA unless they are providing immediate patient care via an NHS service remotely. This must be authorised by the Health Board.

When accessing NHS Wales applications via MFA, access should be on a read-only basis, pharmacy users must not:

- Save any documents/emails to the device;
- Print any documents/emails;
- Forward any documents/emails from or to non-NHS email addresses.

Locum pharmacists who work on a contractual basis should not access any applications intended to be used by a specific pharmacy remotely under any circumstances. This includes accessing:

- NHS email shared mailboxes (where access has been granted);
- NHS clinical applications (e.g. WIS, Choose Pharmacy) unless the locum pharmacist is providing direct patient care via an NHS commissioned service (which has been authorised by the Health Board).