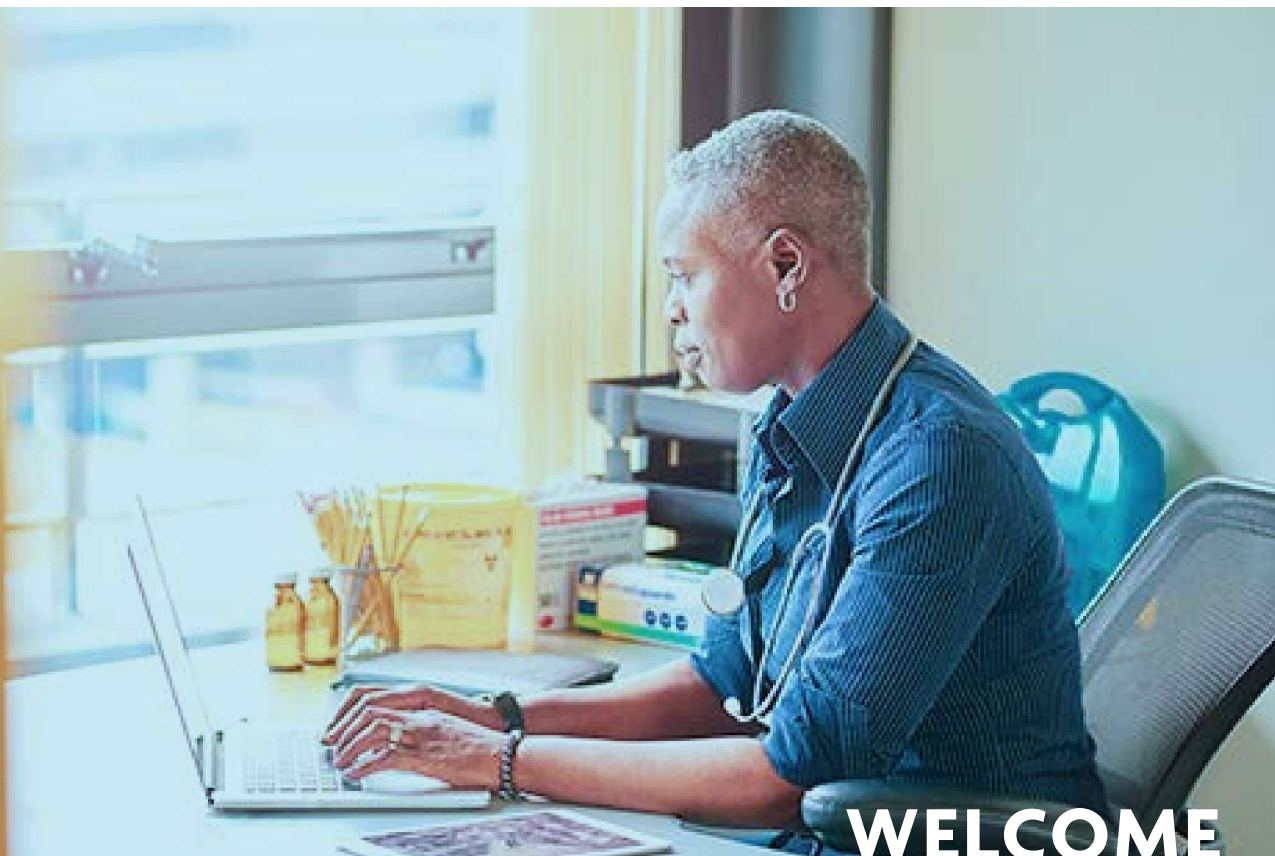




CYMORTH LLYWODRAETHU GWYBODAETH AR GYFER GOFAL SYLFAENOL
INFORMATION GOVERNANCE SUPPORT FOR PRIMARY CARE



WELCOME

to the November 2023 edition of the IG Support Service for Primary Care Newsletter

As you will be aware we publish these newsletters on a bi-monthly basis. Our newsletters aim to provide you with updates on support and guidance developed by the Primary Care Support Service, progress and developments with the Welsh IG Toolkit and relevant IG training and resources.

Medical Examiner Service

NHS Wales Shared Services Partnership (NWSSP) is responsible for setting up the Medical Examiners service (MES) within Wales. The service provides independent scrutiny of non-coronial deaths both in hospitals and in the community. Medical Examiners are senior doctors from a range of specialities including general practice, who review relevant information and provide independent scrutiny of deaths not taken for coroner investigation.

To enable Medical Examiner review of relevant medical records, practices may be asked to share or provide access to the medical records of the deceased. Currently the MES is not a statutory service, and the legislation requires an update. Once an update to the Access to Health Records Act 1990 occurs this will give medical examiners the statutory right to access medical records of the deceased patients from the holders of those records, including GMPs. The relevant legislation is expected to be in place by April 2024.

For the period before the statutory medical examiner service commences, following an application by NWSSP to the Confidentiality Advisory Group (CAG, which is an independent body that provides expert advice and guidance on the use of confidential patient information), an approval has been provided to use confidential patient information for the purposes of the non-statutory medical examiners service. This will be under Section 251 of the National Health Service Act 2006 and Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002.

Section 251 support is in place until September 2024 and enables GMPs to share medical records of the deceased patients with medical examiners. The approved application can be found on the [Health Research Authority's website](#) (ref: 23/CAG/0095). Once the statutory legislation is in place this support will no longer be required.

Medical Records of the deceased patients are outside the scope of UK GDPR, however GMPs may be asked to share contact details of a deceased patients next of kin. The legal basis for sharing contact details only of the next of kin, will be Article 6(1)(e) of UK GDPR, in that the processing is necessary for the exercise of a public task. The Medical Examiners Service is based within NWSSP, an NHS Wales organisation, who will hold and process personal data in accordance with all applicable legislation.

Practices should ensure that their privacy notices are up to date and include reference to sharing with the MES.

Further information on the National Medical Examiner System for England and Wales

can be found [here](#). Specific Information relating to the Wales Medical Examiner service can be found [here](#).

The NWSSP Medical Examiners Service will be circulating an updated information sharing agreement which includes the updated legal basis to practices shortly.

Should you have any questions or queries, please do not hesitate to contact us:

DHCWInformationGovernance@wales.nhs.uk

PECYN CYMORTH LLYWODRAETHU GWYBODAETH CYMRU WELSH INFORMATION GOVERNANCE TOOLKIT



Welsh Information Governance Toolkit

Old IG Toolkit Platform – FormBuilder Two

As you will be aware, the IG Toolkit launched on a new platform this year. The [previous edition of the IG Toolkit](#) will continue to be available to practices to download previous evidence and create reports via the FormBuilder Two platform.

The Corporate Applications Team will be de-commissioning FormBuilder Two on the 2nd February 2024. We therefore encourage users to download copies of reports and information they require prior to this date.

New IG Toolkit Platform – Caforb

The [new IG Toolkit](#) was released on the 31st July 2023. In-line with the latest GP contract, General Practices have until the end of March

2024 to submit the Toolkit, although we do

encourage organisations to work through the assessment throughout the year, to avoid last minute pressures leading up to the submission date.



The new platform consists of just one IG Toolkit form for all its stakeholders. It is broken down into 'core' questions that target all organisations, with additional questions relevant to specific organisation types. Therefore, you will find some questions are written with terminology to encompass the wide range of users.

There are lots of new, exciting, and useful features to the Caforb platform, making the IG Toolkit more seamless to the user. The Toolkit will now be available all year round, closing on the submission date and re-opening the following day, giving organisations more time to populate/update the assessments.

A selection of some of the new features include:

- Individual logins rather than generic access – enables more than one user at a time to access and populate the assessments, with section locking if more than one user is logged in.
- A range of access permissions - Organisation Administrator, User or Read Only
- The ability to re-set your password using the system – you are no longer required to log a call with the Service Desk
- An 'Alert' facility - ability for Users to view messages from the IG Toolkit Team
- A 'Dashboard' - displaying organisation progress.
- An 'Action Plan' - ability for users to record required actions, update progress on actions and create reports.
- The introduction of Minimum Expectations and Expectations Exceeded rather than the previous three levels.

All answers and evidence will remain on the organisation's IG Toolkit form until users delete or update it. Therefore, in future years evidence from the previous year's submission will remain on the form to assist practices, enabling only a review to determine if any answers or evidence have changed. If evidence has changed, an update will be necessary. For example, deleting existing evidence and re-loading new.

If no updates are required only a simple click of the declaration control is required to confirm everything remains the same and is still current. The user can then move onto the next assessment section and repeat the process.

Version 4 of the toolkit was released in October. The Software Development team are currently working on Version 5, which focuses on reporting functionalities. We expect this to be released in the New Year.

The [Support and Resources](#) section has been updated to support the requirements in the new IG Toolkit. As more resources are developed the pages will be updated. A set of [Frequently Asked Questions](#) has also been developed.



A range of bitesize training videos and guides have been developed to support users in navigating the new platform. These are available on our [Supporting resources web page](#). A written [User Guide for the New Welsh IG Toolkit](#) is also available.

Following publication of the new platform, the team have planned several drop-in sessions, over lunchtime hours, where we will be on hand to answer your questions and guide you through the platform with a full demonstration.

These drop-in sessions will be held monthly. The link to the sessions will be made available via each future Newsletter, on the IG Website and within the IG Toolkit itself, on the new Alerts section.

The scheduled dates and links to join are detailed below:

Tuesday 21st November – 1-2pm – [Click here to join the meeting](#)

Thursday 14th December – 1-2pm - [Click here to join the meeting](#)

Authorised Requesters

We can confirm that the following number of Practices in the following Health Boards have not updated their Authorised User forms in the past 6 months.

ABUHB -	36
BCUHB -	38
CAVUHB -	19
CTMUHB -	18
HDUHB -	18
PTHB -	3
SBUHB -	23

It is recommended that each practice nominate four Authorised Requesters. These are usually made up of the Practice Manager, a GP Partner or senior member of staff, and two other staff members of choice.

DHCW maintain a record of the Authorised Requester's nominated by each practice. Only calls logged by those on the list, with the Service Desk will be actioned. If the practice has not updated their list in the last 12 months and wishes to make any changes, you can do so by completing the [Authorised Requester List](#) and forwarding it to the [DHCW Service Desk](#). Only those nominated members of staff can make changes to the list (add or remove staff members and their rights of authorisation).

Mail Marshal Breaches

All emails in and out of the NHS Wales email system pass through Mail Marshal. Emails are monitored to:

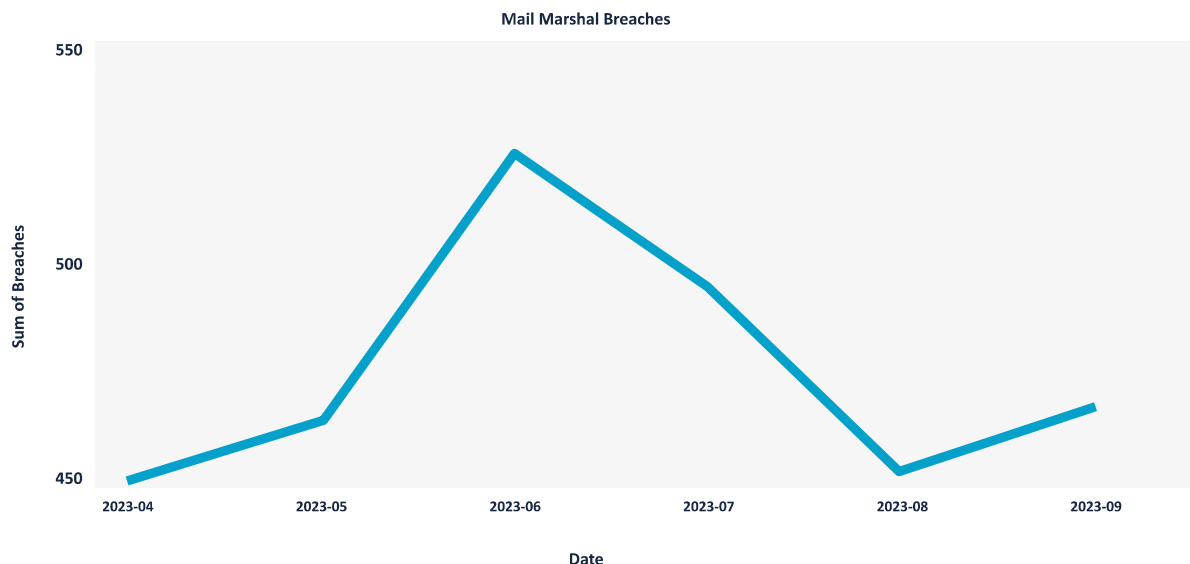
- reduce the risk of patient identifiable information being breached.
- reduce the risk of business sensitive information being breached.
- ensure that the language used by staff does not contain profanities.
- reduce the risks to NHS Wales organisations from malicious file attachments.



Below are the figures for Mail Marshall Breaches from April 2023 – September 2023.

Please see below the link for further information regarding Mail Marshall Breaches along with Cyber Security Training videos and other useful resources. [Mail Marshal](#)

The NHS Wales Secure File Sharing Portal (SFSP) or MOVEit both provide an alternative and safe way to send personal and business sensitive information to third parties. Utilising SFSP or MOVEit is a safe and quick way of avoiding Mail Marshal breaches when the practice is required to share documents containing personal information via email. Further information is available via the below link: [NHS Wales Secure File Share Service \(MoveIT\) \(sharepoint.com\)](#)



Lessons Learnt

Sometimes things go wrong; when this happens, it is important that lessons are learnt. In each edition of the newsletter, we look at a real-life scenario either an incident or audit finding and reflect to see if this could happen in your organisation or if there are lessons which can be learnt, including any changes which can be implemented in your organisation to prevent a similar situation occurring.

ICO enforcement action

A social worker sent copies of a Child and Family Assessment report to the mother and her two ex-partners: each the father of one of her two children. The report contained sensitive personal data which should have been redacted from the copies sent to the partners.

The material disclosed related to previous domestic violence enacted on the mother and the two children. This disclosure put the mother and the two children at risk of actual physical harm and created a volatile and dangerous situation between the parties.

A reprimand has therefore been issued to Nottinghamshire County Council in relation to an infringement of Article 32(1) of the UK General Data Protection Regulation (UK GDPR).

In their investigation, the ICO found:

- Lack of robust procedures
- Lack of training and guidance on redaction
- Previous incidents of a similar nature had occurred
- Severity of breach was serious and put people at risk of harm

Your organisation will need to be mindful of family structures becoming increasingly complicated when dealing with requests for information. As family circumstances change, sometimes quickly, responding to requests is not always a straightforward task. However, if this is not done correctly, it can have devastating consequences to families and lead to incidents occurring.

Breaches can occur for several reasons, the most common being human error. This highlights the importance of staff being thorough when undertaking tasks such as responding to requests and always double checking the final response before sending. Another key factor when responding to requests is taking time to ensure the recipient it is sent to is correct and that it is sent via secure method, such as secure email software or tracked postage.





Having robust policies and procedures in place for all staff to follow is essential. This will help staff to carry out their roles effectively and understand what is expected of them. It also helps the organisation to demonstrate their accountability and that they have mitigated against potential risks.

Organisations must also ensure staff receive relevant Information Governance training that is suited for their role. For example, if staff are responding to subject access requests (SARs) or releasing personal data, they will need to undertake enhanced training that specifically covers matters such as redaction. Undertaking training will also help to improve staff understanding of how to deal with these types of data incidents appropriately.

You should consider whether you have the following in place to help you mitigate any potential risks regarding releasing data:

- Does your organisation have an up-to-date SAR and Information Sharing procedure, including guidance on where to seek further advice?
- Do your procedure include guidance on redaction, particularly surrounding third party information?
- Are staff members with allocated responsibility for responding to SARs and third-party requests for personal data appropriately trained?
- Do you have a process in place for documenting SARs and third-party requests? This should also note any advice that was sought, why decisions were made to redact information e.g., relevant exemptions.



e-newyddion wythnosol weekly e-alert



GIG
CYMRU
NHS
WALES

Iechyd a Gofal
Digidol Cymru
Digital Health
and Care Wales

IG eAlert

The Digital Health and Care Wales (DHCW) IG Department produce a weekly **eAlert** intended for staff who have an interest in information governance issues that affect the NHS in Wales. These eAlert's include news items from around the world on topics such as data breaches, IG related news articles and fines issued by the Information Commissioners Office.

If you have any articles which you feel would also be useful to colleagues, please feel free to forward them for inclusion in the next edition.

Historic editions of the [eAlert](#) can be accessed through the IG Website.

If you would like to receive the weekly eAlert direct to your inbox, please contact DHCWInformationGovernance@wales.nhs.uk

ICO Newsletter

The Information Commissioner's Office (ICO) publish an e-newsletter at least once a month which provides an overview of their work. They bring you the latest news and events, information about enforcement, latest developments, blogs, guidance, codes of practice, etc. in a range of legislation such as data protection, freedom of information and electronic communications and marketing, to name but a few.

To sign up to receive the e-newsletter, [please complete the form.](#)

[The Latest news from the ICO](#) is now available to view. Previous editions of the ICO newsletter can be found using the following [Previous newsletters | ICO](#)

If you do not wish to receive further editions of the newsletter, please email DHCWInformationGovernance@wales.nhs.uk