ig

CYMORTH LLYWODRAETHU GWYBODAETH AR GYFER GOFAL SYLFAENOL

**INFORMATION GOVERNANCE SUPPORT FOR PRIMARY CARE**

WELCOME

to the August 2022 edition of the
IG Support Service for Primary Care
Newsletter

We publish these newsletters on a bi-monthly basis, providing you with updates on support and guidance developed by the Support Service, progress and developments with the IG Toolkit for GMPs, and related IG training and resources which will include 'Lessons Learnt' scenarios.

CYMORTH LLYWODRAETHU GWYBODAETH AR GYFER GOFAL SYLFAENOL

INFORMATION GOVERNANCE SUPPORT FOR PRIMARY CARE

UPDATE! Frequently Asked Questions

The set of **Frequently Asked Questions** maintained on the IG Website have recently been reviewed to incorporate questions received during the Caldicott Guardian training sessions. Areas covered within the FAQs include:

FAQs
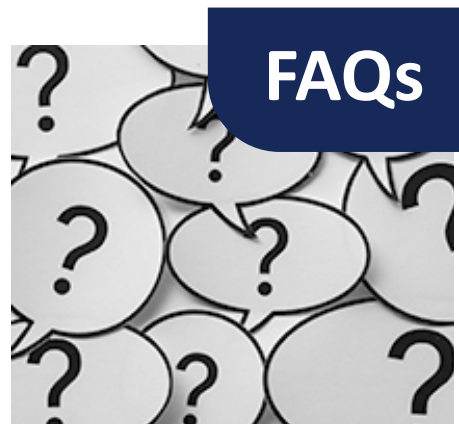
- Auditing
- Breaches
- Caldicott Guardian Documentation
- Children's Rights
- Communications, including email, text messages and telephone
- Contracts and Agreements
- Data Protection Impact Assessments (DPIA)
- Data Protection Officer (DPO)
- GP Data Extraction
- Information Commissioner's Office (ICO)
- Information Sharing
- Media, including Clinical Images

- Patient Rights
- Police and Courts
- Prescriptions
- Privacy Information
- Records Management
- Requests from Solicitors and Insurance Companies
- Review and Redaction
- Subject Access Requests (SAR)
- Systems
- Training
- Websites
- Welsh IG Toolkit
- Welsh Immunisation System (WIS)

UPDATE! Records Management Code of Practice for Health and Care 2022

Welsh Government have issued a **Welsh Health Circular – WHC (2022) 008** notifying all organisations within the NHS in Wales, that with effect from May 2022, they should use the new **Code of Practice**.

This new circular and Code of Practice supersedes the previous WHC 2000 (71): For the record – Managing Records in NHS Trusts and Health Authorities.

Contact the Information Governance Support Service for Primary Care via **dhcwinformationgovernance@wales.nhs.uk**

PECYN CYMORTH LLYWODRAETHU GWYBODAETH CYMRU
WELSH INFORMATION GOVERNANCE TOOLKIT

Welsh Information Governance Toolkit

The current edition of the IG Toolkit is available via the Information Governance Website.

The website hosts a specific section designed to support GMPs in completing the IG Toolkit, including detailed information on each of the requirements. The **Support and Resources** section continues to be developed and includes detailed information on each of the requirements set out in the Toolkit along with guidance on how to reach each attainment level. The supporting resources section includes the **IG Toolkit User Guide**, a set of **Frequently Asked Questions**, Guidance on **How do I delete evidence?** and **Guidance on carrying over evidence from previous submissions**, together with several templates and exemplars. As more resources are developed the pages will be updated.
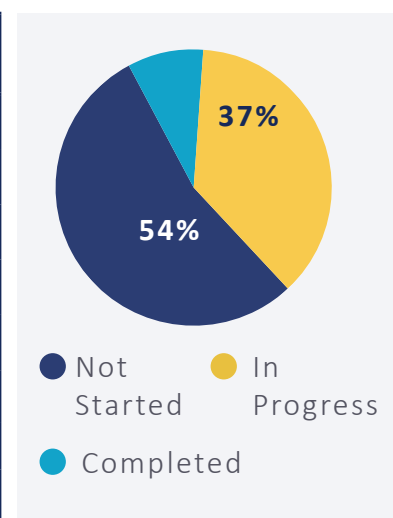
IG Toolkit Progress

We would like to remind practices that the current toolkit requires submission on or by 30th September 2022.

The toolkit has now been live for eight months. A total of 37% of practices have started their annual assessment, and an additional 9% of practices have completed and submitted their assessment.

Toolkit Stats

Health Boards	Not Started	In Progress	Complete	Total
Aneurin Bevan	35	32	6	73
Betsi Cadwaladr	59	28	10	97
Cardiff & Vale	35	21	4	60
Cwm Taf Morgannwg	24	23	1	48
Hywel Dda	26	15	6	47
Powys	4	6	6	16
Swansea Bay	29	17	3	49
All Wales	212	142	36	390

New IG Toolkit Platform

Great progress continues with the development for the new bespoke platform to host the IG Toolkit.
Thank you for those who have offered to take part in the platform user testing in the Autumn. We will be arranging some short 'Pre-testing sessions' nearer the time. We plan to contact the group in September with further details.

There are still spaces for the user testing, therefore if you are interested in taking part or have any questions for the Information Governance Toolkit Team, please contact us via **WelshIGToolkit@wales.nhs.uk**

Information Governance Training

The Information Commissioner's Office recently published their three-year strategic plan – **ICO25**. ICO25 describes the ICOs purpose, objectives and values and the shift in approach the ICO aim to achieve.

As part of ICO25 the Information Commissioner committed to publishing the ICO's internal data protection and freedom of information training materials on their website for reuse by the organisations they regulate.

The information governance and legislation training modules are now available on the **ICO website** and cover topics including:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 – Parts 3 (law enforcement authorities) and 4 (intelligence services)
- Privacy and Electronic Communications Regulations (PECR)
- Freedom of Information Act (FOIA) and Environmental Information Regulations (EIR)

As this training is designed for ICO staff some individuals and organisations may find it too high level and in depth for their needs. However, you should still find the content useful in the key points of the relevant legislation, particularly for those with IG responsibilities, regardless of the organisation.

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 issues NHS Trust with fine following Outlook incident

The Information Commissioner's Office has issued the Tavistock and Portman NHS Foundation Trust with a **penalty notice** following an incident in which an email communication was sent to a total of 1,781 patients whereby the email addresses were entered into the 'To' field instead of the 'Blind Carbon Copy (BCC)' field. The penalty notice imposed an administrative fine of **£78,400** on the Trust.

This is the second administrative fine the ICO have issued in the past nine months for an incident in which the BCC email field was not used appropriately. The fine issued to HIV Scotland, along with guidance on the use of 'To', 'CC' and 'BCC' was detailed within our **November 2021 newsletter**.

Within the penalty notice the ICO detail the factors relevant to whether a penalty is appropriate, and if so the amount of the penalty, this includes both mitigating and aggravating factors.

MITIGATING FACTORS

- The incident was not intentional or deliberate

- The staff member who sent the emails noticed the error immediately and attempted, albeit unsuccessfully, to recall the emails

- The Trust notified both the Commissioner and the affected data subjects promptly

- The Trust apologised to the recipients and has taken remedial action following the incident

- The Trust commenced an internal investigation into the incident

- The Trust fully co-operated with the Commissioner

- The Trust had established customs and practices surrounding public and patient involvement activities

- At the time of the incident the Trust had a suite of policies, including the 'Email, Text and Internet use procedure' which states: "To avoid inadvertently sharing other people's email addresses, recipients should be selected in the 'Bcc' box, not the 'To' box". 'Email Safety Top Tips/ Guidance' includes mention of double-checking email addresses and what to do if an email is sent in error.

- The Trust has published a new standard operating procedure for staff communicating with patients

- The Trust had measures to ensure all staff undertook data security and protection training at the commencement of their employment and routinely thereafter which covered information governance and data security, including the requirement to use the "Bcc" function" in any multi-patient communication

- The staff member who sent the email had received this training

- Consent was considered prior to sending the email and some consents were in place.

- An appointed Caldicott Guardian and IG Lead were available for advice

AGGRAVATING FACTORS

- The inadvertent use of the "To" rather than "Bcc" field in Outlook to insert email addresses for bulk communications has, for some time, been a known security risk

- The Trust should have recognised the inherent risks in relying upon Outlook and "Bcc" for bulk communications involving special category data and/or high-risk groups of patients and should have used an alternative and more appropriate method of sending the emails

- The Trust had access to a technology solution in relation to marketing material which has the capability of addressing bulk emails to individual email accounts

- At the time of the incident the Trust's email server did not have a maximum recipient limitation policy applied to Outlook

- The Trust failed to share the learning from two previous incidents in 2017 or change the processes within similar services

- The consent booklet did not clearly show personal data may be used for this purpose

- The infringement was likely to cause distress to service users

- The Trust could have taken reasonable steps to prevent the contravention

- The majority of the email addresses had either the first name or last name or initials in some way identifiable

- By virtue of the content of the email it can be inferred that the other recipients were also users of the service and thus an inference as to gender status can be drawn. In these circumstances the email addresses are special category data.

- Whilst measures were in place prior to the personal data breach, they were insufficient in the circumstances, and particularly when the Trust was sending bulk emails that contained special category data and/or involved a high-risk group of patients

Consider the mitigating and aggravating factors detailed on the previous page, if this incident occurred in your Practice would all of the mitigations be present?

- Does the Practice have a suite of appropriate policies in place, including an Email Use Policy?   Note: **NHS Wales Email Use Policy for Primary Care Service Providers** must be implemented where staff have been given access to the NHS Wales Email Service.

- Does the Practice have measures in place to ensure all staff complete IG Training on induction and every two years thereafter?

- Does the Practice have an appropriate policy, procedure or guidance in place detailing the action to be taken following a data breach? This should include notification to the ICO, notification to the data subject and investigation process. Note: Information relating to the categorisation and reporting of breaches can be found within the **NHS Wales Guidance on the Categorisation and Notification of Personal Data Breaches** developed by the Information Governance Management Advisory Group (IGMAG).

- Does the Practice have an appointed IG Lead and Caldicott Guardian?

- Are all staff members aware of the action they need to take if an email is sent in error?

- Has guidance been made available to staff on the use of the 'BCC' field? Note: Guidance on the use of 'To', 'CC' and 'BCC' was detailed within our **November 2021 newsletter**.

- Does the Practice have a process in place to ensure lessons are learnt from previous incidents and that these lessons are shared across the organisation?

Further information on any available IG training can be found on the IG website.

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 edition of the ICO e-newsletter** is now available to view. **Previous editions of the ICO newsletter** can be found on the ICO website.

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