



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

APR 2022



WELCOME

**to the April 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

Celebrating one year of the IGSPC Newsletter!

It has been one year since we released the first edition of the IGSPC Newsletter, and we would like your feedback. What do you find beneficial about the newsletter? What could be improved? We look forward to hearing from you!

Please contact the Team via DHCWInformationGovernance@wales.nhs.uk

NEW! Important information about e-mail between Wales and England NHS accounts

Digital Health and Care Wales have been working with NHS Digital colleagues in England to enable improved security and accredited connection for e-mail between @Wales.nhs.uk and @NHS.net accounts.

Email communications between Wales and England NHS accounts can now occur without the need for additional encryption to be applied. NHS Wales email solution now meets with NHS Digital's accreditation standard in order to transfer personal and confidential information between organisations.

This means that both the @Wales.nhs.uk email domain and Microsoft O365 platform have been accredited to the secure email standard for health and care. In addition, both have passed the required clinical safety elements (SCCI 0160 and SCC0129) and achieved the ISB1596/SCCI1596 accreditation. More information on NHS Digital standards is available on the [NHS Digital E-mail standards website](#).



SENDING SECURE E-MAILS - QUESTIONS AND ANSWERS

Do I still need to use additional encryption for sending confidential information to e-mail addresses outside of @Wales.nhs.uk and @nhs.net ?

Yes, you will need to use secure file sharing ([MoveIT](#)) for sending confidential information to email addresses outside of @Wales.nhs.uk and @nhs.net

When does this change come into effect?

The improved security and accreditation was enabled in March 2022. No additional encryption is now needed between @Wales.nhs.uk and @nhs.net.

How is NHS Wales meeting the secure e-mail standard?

The @Wales.nhs.uk email domain has been accredited and has met all the requirements of [secure e-mail standards](#).

Who can I contact if I encounter any issues with e-mail security?

Please contact the [NHS Wales ServiceDesk](#).

NEW! Records Management Code of Practice for Health and Social Care

Welsh Government have recently published an updated [Records Management Code of Practice for Health and Social Care](#). The Code is relevant to all organisations working within, or under contract to, the NHS in Wales, as well as local authorities in Wales who commission or deliver adult social care and public health functions.

It is anticipated that a Welsh Health Circular (WHC) will be published replacing the previous guidance issued in WHC 2000 (71): For the record - Managing Records in NHS Trusts and Health Authorities.

When we have updates on this, we will make them available on the [IG Website News page](#).

Communicating Urgent Prescriptions

The IG Support for Primary Care team have recently updated the previous edition of the '[Communicating Emergency Prescriptions between Prescribers and Community Pharmacies](#)'.

The guidance has been updated to reflect the use of the NHS Wales Email Network as the best and preferred option for all Prescribers, regardless of their organisation, when communicating emergency prescriptions with community pharmacies.

The guidance also references emailing addresses in NHS England ending in nhs.net and the use of fax machines being actively discouraged.

All Wales Policies for Primary Care Service Providers

The set of All Wales policies have been reviewed and updated and are now available on the [IG Website](#), including the NHS Wales Email Use Policy and the Acceptable Use Policy for NHS Wales Office 365 applications.

DVLA – Emailing Patient Information

The IG Support Service have recently been informed that the DVLA's email system does not accept encrypted emails, this includes information sent via the MoveIT secure file sharing portal. At present, the DVLA are not a TLS enabled organisation, therefore unencrypted emails are not secure. Practices are advised that it is not appropriate and in breach of the [NHS Wales Email Use Policy for Primary Care Service Providers](#) to send patient information via unsecure email. DHCW hope to engage with the DVLA to come up with an appropriate solution to resolve the issue, however in the meantime practices are advised that patient information should be sent via other means, such as post.

NEW! IG Guidance for Safe Haven Faxing

The IG Support Service have reviewed the former guidance on the use of Safe Haven Faxing. Although we actively discourage the use of faxing any personal information, we also appreciate that this does, on occasions, happen. Therefore, we have updated the guidance on this to provide support when it is considered absolutely necessary to fax such information.

The updated guidance is available under the '[Information Governance Support for Primary Care](#)' section of the IG Website.

For more information, contact the Information Governance Support Service for Primary Care Team via DHCWInformationGovernance@wales.nhs.uk

NEW! ICO Guidance on Video Surveillance

The Information Commissioner's Office (ICO) have released [new video surveillance guidance](#) that provides organisations with an updated resource, that addresses new applications of video surveillance technologies, and a more comprehensive description of how the UK GDPR and DPA 2018 applies.



NEW! ICO Guidance on Dealing with Vexatious FOI Requests

The ICO have updated their guidance for dealing with vexatious requests under Section 14 of the Freedom of Information Act. The detailed guidance is written for public authorities to provide a deeper understanding in applying section 14(1) in practice.

The [Guidance](#) can be found on the Information Commissioner's Office website and forms part of their [Guide to Freedom of Information](#).



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. The pages will be updated as more resources are made available.

IG Toolkit Progress

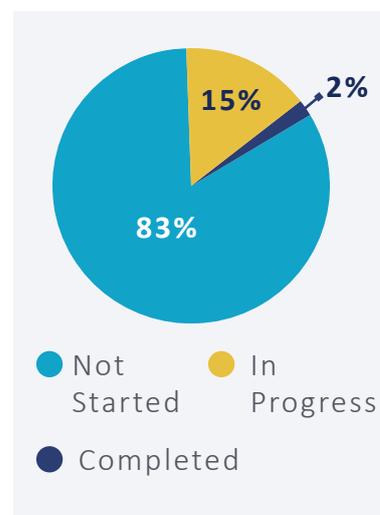
The 2021-22 edition of the IG Toolkit went live at the beginning of December 2021 with a submission date of 30th September 2022. We encourage practices to work through the Toolkit throughout the year to avoid last minute pressure leading up to the submission date.

The toolkit has now been live for five months. We are pleased to see that a total of 59 practices have started their annual IG Toolkit submission, and an additional 6 practices have completed and submitted their IG Toolkit.

To enable the IG Toolkit to be an extremely useful IG knowledge base and training resource, the toolkit should be followed appropriately and methodically. By working through the assessments in this way, whilst referring to the supporting resources on the IG Website and your Practice's IG Improvement Plan, will help

you determine the level of your IG compliance. If used as a 'Tick Box' exercise, the Practice will gain little from the process.

Health Boards	Not Started	In Progress	Complete	Total
Aneurin Bevan	57	16	0	73
Betsi Cadwaladr	81	15	1	97
Cardiff & Vale	51	8	1	60
Cwm Taf Morgannwg	45	4	0	49
Hywel Dda	40	7	0	47
Powys	11	2	3	16
Swansea Bay	41	7	1	49
All Wales	326	59	6	391



Should you have any further questions, comments or feedback about the IG Toolkit, please contact the Team via WelshIGToolkit@wales.nhs.uk

HYFFORDDIANT LLYWODRAETHU GWYBODAETH INFORMATION GOVERNANCE TRAINING



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, 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 Audits consistently lead to high information sharing recommendations for health organisations

Information Sharing Agreements (ISA), Data Sharing Agreements (DSA), and Information Sharing Protocols (ISP) are all terms different

organisations may use, this is acknowledged by the [ICO](#). In NHS Wales we generally use the term **Information Sharing Protocol (ISP)**, for ease and understanding we have amended the terminology used to refer to Information Sharing Protocols (ISP) throughout.

The Information Commissioner's Office (ICO) conducts audits of public and private companies, public authorities and government departments to provide an assessment of whether the organisation is following good data protection practice. The audits look at whether effective controls are in place alongside fit for purpose policies and procedures to support data protection obligations. They check if the organisation is following data protection legislation as it applies to them and produce a report which makes recommendations on how to improve.

Since November 2021 the ICO have conducted audits and published executive summaries of four NHS organisations, **all** of these audits resulted in **multiple high recommendations for information sharing**, identifying a common theme for health organisations.

Some of the findings included:

- There is **no Information Sharing Protocol (ISP) log** to record vital information pertaining to current ISPs which the organisation is party to;
- The organisation should **improve their information sharing documentation** by ensuring there are adequate policies and procedures in place outlining roles and responsibilities for staff involved with data sharing;
- The organisation's **Information Sharing Protocol (ISP) library is not up to date and not all routine data sharing activities are covered by a sufficiently detailed ISP** signed by the senior management of all sharing partners; and
- **Existing ISPs are not reviewed periodically**, in all cases, to provide assurance that each agreement continues to operate as intended and in line with legislative requirements.

information sharing being routine within General Practice, we can learn from such audits to consider whether similar findings may be present in practices across Wales. For example:

- Would your Practice benefit from a review of its processes?
- Does the Practice have an Information Sharing Protocol (ISP) log in place?
- Are your ISPs regularly reviewed?
- Has the Practice signed up to WASPI?

Wales Accord on the Sharing of Personal Information (WASPI)

The **'WASPI framework'** is a tool designed to help organisations share personal information



**Wales Accord on the
Sharing of Personal Information**

effectively and lawfully. It includes a common set of principles and standards which support the sharing of personal information to deliver services to the people of Wales.

The WASPI Framework provides a practical approach to sharing personal information, providing common standards and templates for developing Information Sharing Protocols (ISPs) and Data Disclosure Agreements (DDAs). Its overall aim is to help public service providers deliver effective services while complying with their legal obligations – namely the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

264 GMPs are currently signed up to WASPI.

The case study below from the ICO highlights good practice information sharing within General Practice, although the case study refers to NHS England, similar principles can also be applied in Wales.

ICO Case Study – Good practice information sharing within General Practice Sharing medical records of care home residents

Staff in a privately-owned care home did not have access to the recent medical history of residents. Instead, the home used to phone the GP practice or call out a GP every time they needed more information. This could be a risk, as the staff might need to check quickly what medicines residents were taking and at what dosages.

To make the process more efficient, the care home and the local GP practice signed up to a formal Information Sharing Protocol (ISP), so the care home staff would have access to their residents' electronic medical records when necessary.

The GP practice and local Clinical Commissioning Group made potential residents aware that if they were admitted to the care home there was a possibility that their medical record would be accessed. In addition, when patients were admitted to the care home, their explicit consent - or that of their representatives – was sought before their electronic medical record was accessed. Where consent was not provided, the former system of contacting a GP would continue to be used.

Other key features of the Information Sharing Protocol (ISP) were:

access to residents' records could only take place while they were under the care of the home;

- access was restricted to the clinical and professional nursing staff at the care home;
- access was only allowed where this was necessary to provide treatment and for residents' safety;

- access was restricted to information relevant to the provision of care to residents;
- access to the information was by secure means; and
- the information obtained was held securely and in accordance with good information management practice.

A formal Information Sharing Protocol (ISP) can put in place effective safeguards for residents and can ensure the various parties involved in data sharing are working to a common set of rules. An agreement can also help to deal with the ethical and confidentiality issues that can arise in health and social care.

Even if there is an Information Sharing Protocol (ISP) in place, organisations still need to make sure that individuals whose data may be shared are aware of what is taking place. This can be done through the privacy information they provide, using various methods. In the circumstances outlined here, it might be more effective to talk to individuals to explain the situation and to find out whether they agree to their information being shared. Their decision needs to be documented.



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 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 our 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.](#)

Please note: The ICO have created a new [Preference Centre](#) for existing subscribers to update their preferences in receiving the Newsletter, by answering *“Do you still want email updates from the ICO?”*. Within this section there is also an accompanying privacy notice, and you can also provide feedback on what subjects and sectors you are interested in hearing about. **Those who answer no or do not answer before July 2022 will be unsubscribed from the newsletter.**

If you have previously signed up to receive the ICO Newsletter, [please update your preferences here.](#)

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