Information Governance (IG) Handbook

Visit the IG Intranet Pages for More Information

Report all IG Breaches onto Datix within 24 hours as there is a legal requirement for this. Failure to do so may result in a fine to SB UHB of £22 million. DO NOT DELAY!!

1. General:

- Follow the "Information Governance Policy" and "Information Security Policy" (available on the Intranet or contact the IG Dept).
- Always ensure that health records, staff records and any other personal/confidential information are secure when you leave the office/nurses' station etc.
- Lock rooms or cupboards where personal (staff and patient) data is stored when an area is unmanned.
- Ensure personal data cannot be seen through windows, in reception areas, in consulting rooms, etc.
- Do not access clinical systems for reasons not directly work related: This breaches Policy and could result in your dismissal. This includes your own records and those of colleagues, family and friends, even with their consent. The only exception to this is if you are involved in their care, including admin staff involved in arranging care.
- Treat personal information as if it is your own.
- Never leave records, sensitive information or electronic devices unattended and in view in a vehicle.
- Do not post online comments that are offensive or breach confidentiality on social networking sites.
- Remove any confidential information from printers and fax machines once printed/sent/received.
- Ensure papers containing personal information are destroyed appropriately – shred or use confidential waste sacks/bins.
- Let your patients know how we use and manage their information: Posters and leaflets are available to download on the IG intranet pages (IT Informatics tab on Intranet front page, then Information Governance).
- Tell the IG Department if you have your own departmental information that you give patients (unless they are purely clinical which we do not need to review) or staff, including leaflets, letters, posters or newsletters so we can review them for legal compliance.
- Follow the Decommissioning Policy if you are moving offices, buildings or disposing of old equipment or furniture. Ensure no personal data is left in unexpected places, e.g. piece of paper under a mattress.
- If you share personal data externally with a non-NHS organisation regularly, please advise the IG Dept
- If you share patient information externally, please note this in the patient record – what/why/when/who with.
- Do not enter into local contracts without Procurement support – they may not be legally compliant.
- If you are responsible for a new project, or a major new information flow, there is a legal requirement to complete a Data Protection Impact Assessment – email sbu.confidentialityissues@wales.nhs.uk for details.
- Use your IGB Lead as your first point of contact for IG queries (see contacts section for details).
- Contact your IGB Lead if you identify any area of IG risk so they can add it to the relevant Risk Register.
- Ensure the Information Asset Register (IAR) includes details of all information held on databases, spreadsheets, documents, paper records stored offsite, locally in filing cabinets, etc – anything necessary for your department's business to take place needs to be logged. Email the IG Dept or your IGB Lead for details.

2. Telephone and face-to-face good practice:

- Speak discretely at all times – in consulting rooms, on the wards, in the corridors etc.
- Only share personal information via telephone when you have confirmed the caller is authorised to receive it.
- Remember the Caldicott Principles and the 'need to know' principle when discussing patients.
- Don't gossip.
- Be careful of how much information you leave on answering machines or voicemail.

3. Communication with the Police:

- Unless this is a regular part of your job, contact the IG Department for further advice. There are procedures available for release of information to the Police (ask the IG Department or visit the IG pages on the Intranet).

4. PC good practice:

- Follow the "Information Security Policy", "E-mail Use Policy" and "Internet Use Policy" (available on the Intranet or contact the IG Department).
- No personal IT equipment is allowed to connect to the Health Board network. However, you may connect your own equipment to the free WIFI service provided by Sky in your own time, and use Mobile Iron to access work data.
- Always save work to a secure network drive and not to the c: drive or the desktop.
- Lock or log out of workstations when unattended (Ctrl+Alt+Delete, then the enter key OR Window key+L**)**.
- Do not share or pass on your password - keep it private.

5. Sending of Mail:

- Please double check the address you are using with the most up-to-date information available. If you notice a discrepancy please don't guess - find out which is the correct address and organise to have the incorrect address(es) updated immediately.
- If you are handwriting an envelope, write neatly and clearly and include the recipient's full name and address.
- If you are using a window envelope, ensure that only the name and address of the recipient is visible through the envelope when sealed (shake it if necessary to check the letter doesn't shift position).
- Consider the use of "Private and Confidential" on the envelope – departments should make their own decisions, weighing up the risk of flagging the envelope as containing potentially sensitive information to those other than the recipient, versus the benefit of stating the envelope is private. You may choose to mark the envelope as "For addressee only" instead.
- Use two envelopes if sending anything heavy or bulky.
- Ensure all envelopes are fully sealed, but do not use any Sellotape on an envelope as this can lead to it sticking to a letter to be sent to someone different by mistake (this has happened and the Information Commissioner's Office recommended no Sellotape use).
- If hand delivering a letter, ensure that the envelope has still been fully addressed with the recipient's name and address, and ensure that it is handed over to the recipient only or posted through the correct secure letterbox.
- Consider the need to use a courier service, or tracking and/or 'signed for' services through Royal Mail, to ensure confidentiality and audit of the delivery and receipt of the letter/package.

6. Faxes

- Follow the Fax Policy (available on the Intranet or contact the IG Department).
- Make sure you have the correct fax number and that there is an appropriate person ready to receive the fax at the other end.
- Emailing within policy is preferable, followed by the Secure File Sharing Portal, MoveIT or CJSM (ask the Information Security Manager for details), then Royal Mail or internal mail; fax as a last resort only.
- Check and check again.

7. <u>Transfer of personal data – patient and/or staff – via e-mail</u>

Personal data is information relating to an individual, including their image or voice, which enables them to be uniquely identified from that information on its own, or from that and / or other information available. Personal data refers to patient or staff information. The transfer of personal data via e-mail should be controlled as follows:

- **Within NHS Wale (addresses ending in wales.nhs.uk) -** Personal data can be sent anywhere within the Welsh NHS network (wales.nhs.uk) without password protection or encryption. This includes GPs at their wales.nhs.uk address, as long as the process has been agreed with them first.
- **Within Public Sector in Wales -** Following work undertaken by a number of Welsh public sector organisations and NHS Wales, e-mails will be automatically encrypted in transit between ourselves and the organisations listed on next page.

Regarding the security of e-mail between NHS Wales and a number of other public bodies, it is now as safe to send mail between ourselves and these organisations as it is to other NHS Wales e-mail addresses.

Please see if the address you want to email Person Identifiable Details ends with following domain, @:

NHS Wales
wales.nhs.uk
secure.nhs.uk
nhsbt.nhs.uk

Welsh Government

Blaenau Gwent
blaenau-gwent.gov.uk
Bridgend
bridgend.gov.uk
Caerphilly
caerphilly.gov.uk
caerffili.gov.uk

socialservicesblaenau-gwent.caerphilly.gov.uk

Carmarthenshire
carmarthenshire.gov.uk
sirgar.gov.uk
Ceredigion
Ceredigion.gov.uk
Ceredigion.llyw.cymru
Swansea
swansea.gov.uk
Cardiff
cardiff.gov.uk
caerdydd.gov.uk

Conwy
conwy.gov.uk

Denbighshire
denbighshire.gov.uk
sirddinbych.gov.uk
Gcar-cgc.org.uk

Flintshire
Flintshire.gov.uk
Siryfflint.gov.uk
Gwynedd
gwynedd.gov.uk
gwynedd.llyw.cymru
Anglesey
anglesey.gov.uk
ynysmon.gov.uk
Merthyr
merthyr.gov.uk
Monmouthshire
monmouthshire.gov.uk
Neath-Port Talbot
npt.gov.uk
neath-porttalbot.gov.uk
Newport
newport.gov.uk
Pembrokeshire
pembrokeshire.gov.uk
Powys
powys.gov.uk

Rhondda Cynon Taf
rctcbc.gov.uk
rhondda-cynon-taff.gov.uk
rhondda-cynon-taf.gov.uk
cscjes.org.uk
links.cscjes.org.uk
rctpensions.org.uk
Torfaen
torfaen.gov.uk
Vale of Glamorgan
valeofglamorgan.gov.uk
bromorgannwg.gov.uk
Wrexham
wrexham.gov.uk
wrecsam.gov.uk

Welsh Government Departments

assembly.wales
senedd.cymru
gov.wales
wra.gov.wales
llyw.cymru
wlga.gov.uk
gcsx.gov.uk
gse.gov.uk
gsi.gov.uk
gsx.gov.uk
hscic.gov.uk
mod.gov.uk

And:

Home Office

biometricscommissioner.org.uk
cluster2security.gov.uk
dbs.gov.uk
dmip.independent.gov.uk
expertpanel.gov.uk

extremismcommission.independent.gov.uk

forensicscienceregulator.gov.uk
gla.gov.uk
hmicfrs.gov.uk
iasc.independent.gov.uk
icibi.gov.uk
iicsa.independent.gov.uk
ipco.org.uk
ipt.independent.gov.uk

modernslaveryactreview.independent.gov.uk

sccommissioner.gov.uk

Police

North Wales
nthwales.pnn.police.uk

Dyfed Powys
dyfed-powys.pnn.police.uk

Gwent
gwent.pnn.police.uk
South Wales
south-wales.pnn.police.uk

Fire Service

South wales
southwales-fire.gov.uk
decymru-tan.gov.uk
Bridgend
firecontrol-bridgend.pnn.gov.uk

rheolitan-penybontarogwr.pnn.gov.uk

Mid and West Wales
mawwfire.gov.uk
tancgc.gov.uk

National Parks

Beacons
beacons-npa.gov.uk

Pembrokeshire coast
pembrokeshirecoast.org.uk
arfordirpenfro.org.uk

Misc

Nwc-reps.org.uk
srswales.com
adoptcymru.com
cccpartners.org.uk
crcv.org.uk
hah.co.uk
mariecurie.org.uk
amgen-cymru.com
westernbayadoption.org
Flintshirefostering.org.uk
cardiffcreditunion.com
cardiffcreditunion.co.uk
cardiffcu.com
cardiffcu.co
taffhousing.co.uk
careerswales.com
gyrfacymru.com
saferwales.com
cardiffwomensaid.org.uk
ewc.wales
wwha.co.uk
unitedwelsh.com
hafod.org.uk

This means that we can now send identifiable and confidential information securely between ourselves and these public sector organisations. Please remember that we must still be vigilant and ensure the e-mail address we are sending the information to is correct and that we have a legal reason for sharing this information under the Data Protection Act 2018 (GDPR). For further information please contact the Information Security Manager, ext. 43650.

- **Outside Public Sector in Wales** - The transfer of personal data via e-mail outside of the Public Sector in Wales is not permitted **unless** it is contained within an encrypted attachment/document. This would include e-mail to such recipients as English NHS organisations. However, if personal data must be sent to these recipients then please contact the Information Security Manager for advice, ext. 43650.

Data Protection Officer: sbu.dpo@wales.nhs.uk

General IG queries: sbu.confidentialityissues@wales.nhs.uk

Head of Information Governance:

- Becky Wadley at HQ, x43336, 01639 683336, becky.wadley@wales.nhs.uk

Information Governance Manager:

- Jessica Hiscock at HQ, x44346, 01639 484346, jessica.hiscock@wales.nhs.uk
- Andy Lock at HQ, x43651, 01639 683651, andy.lock@wales.nhs.uk
- Claire Parsons at HQ, x43749, 01639 683749, claire.parsons@wales.nhs.uk

Information Governance Support Officer:

- Ania Dobek at HQ, x44347, 01639 684347, ania.dobek@wales.nhs.uk **(Training Lead)**

Information Governance Support Officer:

Nicola Williams at HQ, x44345, 01639 684345, nicola.williams43@wales.nhs.uk

IG Dept

Information Security Manager:

- Chris Phillips at HQ, x43650, 01639 683650, chris.phillips@wales.nhs.uk

Freedom of Information Act queries:

- Corporate Administration Dept at HQ, x43312, 01639 683312

IGB Leads:

Find your local IGB Lead by visiting the IG Intranet pages (IT Informatics tab on Intranet front page, then Information Governance). You need to work with them when managing an IG breach, or when completing the Information Asset Register. They support the drive for compliance with IG mandatory training and data protection legislation in general. They represent your SDU/Corporate Dept at the bimonthly meetings of the Information Governance Board, which is chaired by the Director of Corporate Governance in their role as SIRO (Senior Information Risk Owner).

Training is mandatory and must be updated once every 2 years. Training is available through general Health Board sessions advertised via the Intranet and e-mail, or (in exceptional circumstances) by Departmental visits by a member of the IG Department. Contact Training Lead for details. There is e-learning available (details available on the Intranet site – go to the IT Informatics tab, then Information Governance), but we strongly recommend you attend a face-to-face session at least every other refresher, i.e. every 4 years.

Short term placements such as students or agency staff should attend a face to face session if possible, but if not, then they MUST read the IG Intranet Pages and sign the confidentiality agreement via the link on the IG intranet pages to be kept on file by the relevant department.

IG Incident Flowchart