COVID-19 NHS Wales Information Governance Joint Statement

Information governance is about how we manage and share information appropriately.

The health and social care system faces significant pressures due to the COVID-19 outbreak and, in the current circumstances, it could be more harmful not to share health and care information than to share it. The Information Commissioner has confirmed that she cannot envisage a situation where she would take action against a health and care professional clearly trying to deliver care. You can read the statement from the Information Commissioner's Office, alongside their Q&A resource. Health regulators have also published a joint statement.

We are all responsible for looking after personal information and the important thing, as always, is to consider what type of information we are sharing and with whom. During this period, where clinical need demands it, we may need to work in different ways from usual. Our focus should be on **what** information we need share and **who** we share it with, rather than **how** we share it. We should always limit the use of personal or confidential patient/service user information to the minimum required to meet the specific purpose. Use approved processes, systems and applications where it is effective to do so.

This advice has been developed by the NHS Wales Information Governance Management Advisory Group and is endorsed by the Information Commissioner's Office and Welsh Government. It sets out some of the tools that can be used to support individual care, share information and communicate with colleagues during this exceptional time. Appendix A provides some further practical tips.

Mobile Messaging

Mobile messaging can be used to communicate with colleagues, patients and service users. Commercial, off-the-shelf applications can be used **where there is no practical alternative** and the benefits outweigh the risks; for example, you would not otherwise be able to communicate with, or provide timely advice to, patients or colleagues. NHS Wales endorses the use of Hospify available via https://www.nhs.uk/apps-library/hospify/ for professional to professional messaging containing personal identifiable information / clinical pictures.

Although they are not designed for business purposes, and are not recommend for this purpose, in the current crisis situation off the shelf consumer applications, such as

WhatsApp, can be considered where you urgently need to contact colleagues, staff members or patients if no practical alternative is available. You should avoid messages containing personal identifiable information in apps that have not been officially assessed and approved for this purpose.

Be mindful that communicating from device to device using consumer applications is likely to expose the details of that device (such as the telephone number) to patients and colleagues. Try to utilise devices provided by your employer or, if the technology allows, mask the device or personal details. Remember that using your personal device could present risks to the security of that device and your personal data.

Further detail on possible messaging solutions will be provided in due course.

Videoconferencing

The use of videoconferencing to carry out consultations with patients and service users could help to reduce the spread of COVID 19 and may be useful in some clinical scenarios. Make the most of any existing applications, such as Skype, made available by your employer. Work is ongoing to appraise and, where appropriate, roll out commercial products, such as AttendAnywhere, AcuuRx and other software designed specifically for this purpose. Further information will be provided in due course.

Although they are not designed for business purposes, and are not recommend for this purpose, in the current situation consumer applications, such as Face time and WhatsApp, can be considered where you urgently need to have a video consultation with a patient during this crisis period only, and if alternative channels are not available.

Consider the clinical risk of not conducting the consultation against any potential risk of using these types of consumer-focused services. Please be aware of the considerations, described above, regarding the visibility of your device details, such as telephone number, and your personal information.

Please remember that any information you collect during this type of consultation MUST be placed in the appropriate care record.

Also please be mindful that, although the organisation will not be recording the consultation, the patient may be doing so (the patient does not need our consent to do this for their private use).

Homeworking

You may well need to work from home - for example, to reduce potential contact or when self-isolating without symptoms.

Where available, use work devices and associated security measures.

If using your own equipment, check that your internet access is secure and that any security features are in use. If possible, use a Virtual Private Network (VPN) and avoid the use of unsecure networks, such as, public wi-fi.

When travelling or at home, ensure the security of any physical documents that contain personal or confidential patient information, service user or staff information. Please refer to your own organisation's policy and guidance, where available, for further advice. See Appendix A for practical hints and tips.

Using Your Own Device

You may have to use your own device to support video conferencing for consultations, mobile messaging and home working where there is no alternative; i.e. you can't access your normal work device(s) because you are unable to access your normal place of work. Note the previous comments regarding exposure of device and personal details.

Reasonable steps to ensure your device is safe to use for work purposes include, setting a strong password; using secure channels to communicate e.g. tools and apps that use encryption; not storing personal or confidential information on the device unless necessary and appropriate security is in place. Please refer to your own organisation's policy and guidance, where available, for further advice.

Agreements and risk assessments

The current environment in which we are working is fast moving and subject to change. As such, we believe efforts are best focused on finding practical solutions to ensure that appropriate care and treatment can be provided to those that need it. During this period of pressure, take a risk-based approach to the development of agreements and data protection impact assessments (DPIAs). You may need to prioritise the provision of care and treatment.

There is a clear lawful basis for the necessary disclosure and sharing of information between partners including GPs, Health Boards, Social Care Departments and Public Health Wales and the absence of agreements or DPIAs should not restrict the sharing or disclosure of data. It is good practice to keep a record of decisions you make (for example, save email strings) and to revisit assurance activity, such as agreements and DPIAs, if temporary ways of working develop into more permanent arrangements.

Arrangements involving third party suppliers processing personal data on your behalf need to be underpinned by a legal agreement. You will need to seek advice from your Data Protection Officer or Information Governance lead before entering into any such arrangement.

Record keeping

For all video or teleconference consultations, please ensure that ALL information is recorded in the appropriate care record (as you would normally do). Ensure any personal information stored on your own device, or obtained through a video or telephone conversation, is safely

transferred to the appropriate health and care record as soon as it is practical to do so. Delete any personal information, including back-up data, from your own device – being mindful of automatic backups that might be enabled. Apply your own relevant professional standards, as you would normally. Also remember that data protection rights and rules apply to any personal data stored on your personal device.

Further help

Speak to your own Information Governance lead or Data Protection Officer if you require assistance or have any queries about this advice.

Appendix A - tips for digital communication with patients and using your own device

Wherever possible, use approved processes, systems and applications in your dealings with colleagues and patients. Where the current situation means that you need to work differently, consider the following hints and tips.

- Ensure you are communicating with the correct person or group before sending a message or commencing a video or telephone consultation.
- When using emails or group messages to communicate, be careful when 'replying to all' and consider using 'bcc' when sending group emails.
- Take care when selecting the membership of any group set up to deliver mobile or electronic messages and review the membership regularly.
- Do not allow anyone else to use a device you use for work purposes unless there is no alternative.
- Before using your own device for work purposes, set a passcode and a time-out / screen lock after a short period of inactivity.
- Disable message notifications on your device's lock screen so that message content cannot be viewed when your device is locked.
- Enable the remote-wipe feature in case your device is lost or stolen.
- Limit the amount of personal data sent in messages – think about the purpose of the message and use the minimum amount of personal data required.
- If you receive or take any photos of patients, review these as soon as possible and delete when no longer required. Ensure such data is deleted from any back-up facility.
- Do not click on any images or files that you were not expecting to receive, report these to your IT Service Desk.
- If using your own device, think about how you can refer the patient back to central points of contact, such as 111 or a general enquiry line, for further communication.
- Physical documents documents containing personal, or confidential information, should be securely transported in a closed bag or case and remain on your person at all times while you are travelling. Documents should also be stored securely in your home and not accessible to anyone else but you. Under no circumstances should documents be left in a vehicle while you are not in that vehicle.