Good Practice Guide Appendices Appendix 20

ICT and Information Systems

For effective cluster working, the need to draw together a broad range of professionals and coordinate care across a range of previously distinct services will be assisted through the better and more widespread use of existing and emerging technologies. Teams will need to identify the mechanisms available to access relevant information and use of different technologies to transform the delivery of care.

The importance of good infrastructure for immediate and future technologies cannot be over-emphasised to support staff and patient expectations and the delivery of high quality care. Appropriate stakeholder engagement is crucial to the success of any ICT development and implementation; each cluster will be included in the discussions and decisions for the procurement of ICT technology and systems to ensure understanding and consistency of decisions.

ICT Infrastructure

As well as embedding technologies such as tele-care and tele-health, the services must be supported by investment in the fundamental technical infrastructure that allows safe, reliable and accessible information providing better coordination and management of services. Information systems will need the functionality to 'speak with each other' and ensure information flows are seamless between organisations within the cluster, across clusters and to care partners. Across the care provider service, many providers are struggling because key information systems are not connected impacting on their ability to provide seamless and at times safe care.

In order to provide adequate and appropriate access to information systems for the user community we must ensure that we provide an appropriate level of access to computing devices, a consistent, fast, and reliable network and hardware that is matched to the optimum requirements of the applications software rather than the minimum. In addition the infrastructure must have improved capability, usability and good response times.

We must provide efficient mobile capabilities both on site and in the field within all the community settings and as such there needs to be a focus on getting the infrastructure correct and at a level that allows a reasonable degree of growth through sufficient capacity and a smoother adoption of future improvement through planned funding.

The capability and capacity of the hardware and the software must be sufficient to support effective working, and it needs to be kept up to date in order to optimise the productivity of staff and service delivery to patients. We also need to address areas that currently have no ICT access, either due to networking or absence of computing devices.

Information Governance

Information Governance (IG) concerns the way in which we manage the confidentiality, integrity and availability of information (CIA) about patients, families, staff, and about the organisation itself. As part of the cluster's overall governance framework, alongside Clinical, Financial and Corporate Governance, a robust Information Governance framework is one of the keystones to support the delivery of services whilst reducing risks to people, through effective management of information and records.

Drivers to providing effective IG include compliance with the various legislation (including the Data Protection Act 2018, General Data Protection Regulation, Network & Infrastructure Directive, Freedom of Information Act), regulatory requirements, measures and advisory standards (such as Standards for Health Services, Caldicott Report, Wales Accord on the Sharing of Personal Information etc.). Effective IG will not only help to provide assurances that the clusters will comply with the legislation and standards, but it supports the delivery of patient centred services, improves quality and makes better use of resources.

It is recognised that the delivery of services across organisational and service boundaries means that in order to provide complete health and well-being benefits to the individual, it is as much about partnership working and trust between care partners as it is about maintaining the individual patient-clinician relationship. Effective IG will empower staff to make the right choices and increase the confidence of our service users, the public, and partners that we are able to deliver effective services.

New Legislation

Data Protection Act 2018, General Data Protection Regulations (GDPR), Network & Infrastructure Directive (NISD), Digital Economy Act, etc.

The new Data Protection Act 2018 and General Data Protection Regulation (GDPR) are the biggest change in data protection laws for 20 years. These changes have been created due to the technical advances and the widespread availability of personal information. New technology brings new threats. These changes obviously have an impact on clusters, in the way information is managed and the way that clusters support patients, service users and staff.

The Information Commissioner's Office (ICO) guide on GDPR provides for the ability for NHS and Social Care to collect, use and share information by using different legal conditions without the reliance on consent. This will better enable the appropriate use of personal and sensitive information within and across clusters to improve the care of patients and families.

Each organisation within the cluster is classed as a Data Controller (as defined in GDPR). When a cluster becomes a legal entity, it also becomes a Data Controller in its own right.

Legal Requirements for Clusters

Each organisation within the cluster must comply with the legislation and standards.

Each organisation must nominate a Data Protection Officer [DPO] (as defined in the GDPR). For smaller organisation e.g. a primary practice, this need not be within the organisation but can be to a different body, e.g. with the Health Board. Where this is outside of the organisation then this will be formalised through a contract defining terms and conditions.

Each cluster (and organisations within the cluster) will have appropriate IG and technical security policies and procedures in place that are consistent across all clusters. Where new information systems are to be implemented then a Data Protection Impact Assessment (DPIA) will be undertaken by the lead organisation. The DPO can advise on the correct use and procedures of a DPIA.

Each organisation must have an incident and breach management policy and process to comply with the legislative reporting requirement where serious incidents must be reported to the ICO within 72 hours. The DPO must be informed of all breaches in order to advise on the way forward.

Each organisation (as a Data Controller) within the cluster will have procedures to deal with Subject Access Requests across the cluster and beyond. This is especially significant where primary care organisations forward on care to a different organisation within the cluster or to another cluster.

The GDPR requires that each organisation must understand what information is held and how it is used and shared. Each organisation will create and maintain an Information Asset Register, which describes the information system, the information held, the owner and administrator. The owner of each system within each primary care organisation will be the Lead Practitioner and the administrator will be the Practice Manager (or equivalent).

Each cluster must inform people what it does with their information, its security arrangements and their rights around this information (Privacy Notices). A layered approach will be used, whereby the a generic high level (organisational) notice can be provided (as poster and on internet sites) and then more detailed service specific notices can be layered under this e.g. about Frailty services, or primary care mental health services. Most of these can be provided on the clusters internet sites and complemented with posters and leaflets and use of social media and other mechanisms. Children will need to be considered separately from adults and child friendly notices will be developed.

All information systems used must have a facility to audit or check use, access to records and information, changes to data, identifying who did what and when.

Each organisation and people within the organisation are accountable for their compliance actions.

Each organisation or cluster will ensure that all staff are appropriately trained regarding IG and trained on each system that they use.

Contractual Implications

For the purposes of data protection and IG, staff working within the cluster or across the cluster are considered employees of the organisation with whom they hold their employment contract. Where there are joint funded posts the individual is considered an employee of the organisation with whom they have an employment contract. [This is important for accountability, training and concerns procedures].

Information Sharing

The improvement in people's health and well-being is not achievable by each organisation within a cluster or each cluster working on its own and each will share information to partners where it's appropriate to do so. The default will be that we will share information with others rather than securing data to the extent that it becomes difficult to share. Aversion to the risk of data exposure should not override the need to align that risk against the safety and benefit to the patients' health. Sharing between partners will be based on the Wales
Accord on the Sharing of Personal Information (WASPI) framework and supported by the appropriate Information Sharing Protocols (ISP's).
Each organisation within the cluster will sign up to the WASPI framework (signing the Accord) and participate in the development of appropriate ISP's to share information between sector partners. When procuring or designing information systems we must consider the entire patient pathway including that beyond the boundary of the cluster and include other partners that may be involved in the care and support of the patient. The design, functionality, implementation and rollout of information systems must be such that it supports the effective and efficient sharing of patients' digital data across boundaries, subject to appropriate IG protocols and benefit assessment.

Freedom of Information

Each cluster and organisation within the cluster will comply with the relevant requirements of the Freedom of Information Act, based on openness and transparency in all actions. Official documents will be made available through the organisations publication schemes. The cluster will determine the appropriate publication scheme (such as the Health Board) by which to publish its official documents. This will apply if a cluster becomes a legal entity in its own right.