

Welsh IG Toolkit for Health Boards and Trusts

Scoring Matrix				L1	L2	L3		Response	Compliance Score
2. Business Responsibilities				PERCENTAGE %					
2.1 Information Governance Management				Input	Core	Key	2800	2800	2780
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these								
	Please check to confirm								
1	Responsibility for driving improved information governance has been assigned to appropriate individuals within the organisation. This forms part of their job description and daily duties						100		
	Detail how information governance is reported up to Board level or equivalent, including any Groups or Committees						15		L1
	Name of appointed Senior Information Risk Owner (SIRO)						15		L1
	Senior Information Risk Owner has detailed responsibilities as part of their job role						5		L1
	Name of appointed Data Protection Officer (DPO)						20		L1
	Data Protection Officer/Service has detailed IG responsibility as part of their job role						5		L1
	Name of appointed Caldicott Guardian						15		L1
	Caldicott Guardian has detailed IG responsibilities as part of their job role						5		L1
	Detail the structure of the Information Governance team and how it fits into the organisation						10		L1
	Date of current 'fee' with the Information Commissioners Office (ICO)						10		L1
2	Responsible individuals have received appropriate training to take ownership of the information governance agenda and identified improvements from previous IG Toolkit(s). These have formally been documented to from an action plan/improvements plan							100	
	Appointed Senior Information Risk Owner (SIRO) has received appropriate training and is up to date							25	L2
	Appointed Data Protection Officer (DPO) has received appropriate training and is up to date							25	L2
	Appointed Caldicott Guardian has received appropriate training and is up to date							25	L2
	Improvements and targets have been documented to from an action/improvement plan as a working document and have been formally agreed							25	L2
3	IG arrangements and the progress against the IG Toolkit Improvement plan is regularly reviewed and reported to the Board/Committee/Management Team, as appropriate, by the DPO								100
	Progress and targets listed in the action/improvement plan are reported to the Board/Committee							50	L3
	Progression on the identified targets and IG arrangements are regularly monitored by the DPO along with performance reports to Board level, or equivalent							50	L3
2.2 Policies and Procedures									
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these								
	Please check to confirm								
1	The organisation has a number of policies and procedures in the context of IG. National policies such as Information Security, IG and Email Use policy have been adopted and made available to staff						100		
	National policies have been approved and adopted within the organisation						40		L1

Level 1	
Total Available	2800
Score Achieved	2780
Compliance Percentage	99%

2. Business Re	
Level 1	
Total Available	700
Score Achieved	680
Compliance Percentage	97%

3. Business N	
Level 1	
Total Available	200
Score Achieved	200
Compliance Percentage	100%

4. Individu	
Level 1	
Total Available	400
Score Achieved	400
Compliance Percentage	100%

5. Managing and	
Level 1	
Total Available	1000
Score Achieved	1000

	There are other organisational information governance related procedures and policies that are current and up to date and complement national policies				30			L1	yes	30
	All policies and procedures are made available to staff				30			L1	yes	30
2	There is a review process in place for all policies and procedures and any changes are communicated to staff					100				
	There is a review process in place for all local and national policies and procedures					50		L2	yes	50
	All updates and changes to all policies and procedures are effectively communicated to staff					50		L2	yes	50
3	Compliance with policies and procedures are regularly monitored to ensure they have been adopted in practice throughout the organisation						100			
	Spot checks/audits are made to ensure policies and procedures are being followed						100	L3	yes	100
2.3 Information Sharing										
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these									
	Please check to confirm									
1	Personal information is used and shared lawfully and relevant sharing principles of the Wales Accord on the Sharing of Personal Information (WASPI) and the common standards of the Welsh Control Standard for Electronic Health and Care Records have been adopted. All sharing is carried out in compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA)					100				
	The organisation has acknowledged and signed up to the Wales Accord on the Sharing of Personal Information (WASPI). The designated individual is current and the CEO details are up to date					35		L1	yes	35
	The organisation has acknowledged and signed up to the Welsh Control Standard for Electronic Health and Care Records and commits to the common standards and principles when sharing electronic health and care records					35		L1	yes	35
	There is a process in place for agreeing and approving ad-hoc sharing of personal data					30		L1	yes	30
2	Where appropriate Information Sharing Protocols (ISPs) or Data Disclosure Agreements are recorded in the form of an agreement register. National systems such as NIIAS and AC3 are used to demonstrate the adoption of the Welsh Control Standard for Electronic Health and Care Records						100			
	A register is in place to document existing information sharing agreements, their durations and who is party to them						50	L2	yes	50
	National systems have been deployed to demonstrate compliance with the Welsh Control Standard for Electronic Health and Care Records						50	L2	yes	50
3	There is a review process in place to ensure agreements are kept up to date. Any changes or updates are reflected in the Information Sharing Register									
	There is a process in place to ensure the review of all Information Sharing Agreements and the Information Sharing Register is maintained in accordance with any changes/updates						50	L3	yes	50
	New and reviewed sharing agreements are regularly reported to relevant Board/Committee/Management Team, etc						50	L3	yes	50
2.4 Contracts and Agreements										
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these									
	Please check to confirm									
1	Data protection and IG contracts and agreements are in place with all suppliers, contractors, third parties and staff, who have access to/process personal data, which include data protection /IG requirements					100				
	There are processes to ensure robust contracts are in place for all suppliers, contractors, data processors and third parties					25		L1	yes	25
	Standard contracts/clauses have been developed and made available where required for all suppliers, contractors, data processors and third parties					25		L1	yes	25
	There is a robust process to ensure confidentiality clauses/agreements are included in permanent staff contracts					25		L1	yes	25
	There is a robust process to ensure confidentiality clauses/agreements are included in staff contracts for temporary staff, agency staff and locum workers					25		L1	yes	25
2	All contracts and agreements are documented to allow easier assessment of current contracts/agreements already in place and due diligence checks are carried out on all potential suppliers, contractors, data processors and third parties						100			
	Due diligence has been conducted by the organisation to ensure third parties are compliant with data protection legislation, industry standards and relevant Welsh Health Circulars						70	L2	yes	70
	All contracts and agreements are documented to form a Register of Agreements						30	L2	yes	30

Compliance Percentage	100%
------------------------------	-------------

6. Technical, Physical and	
	Level 1
Total Available	400
Score Achieved	400
Compliance Percentage	100%

8. Information Governan	
	Level 1
Total Available	100
Score Achieved	100
Compliance Percentage	100%

3	A review process is in place to ensure that all contracts and agreements are regularly reviewed and any changes are communicated appropriately					100		
	There is a review process to ensure contracts and agreements remain up to date for all suppliers, contractors, data processors and third parties					60	L3	
	Where changes are made to permanent staff contracts, staff are engaged with, and these are communicated appropriately					20	L3	
	Where changes are made to temporary, agency or locum staff contracts, staff are engaged with, and these are communicated appropriately					20	L3	
2.5 Data Protection Impact Assessments								
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these							
Please check to confirm								
1	A process to facilitate completion of Data Protection Impact Assessments (DPIAs) is in place to highlight potential risks for new projects/services. All DPIAs are collated to form a register and this is regularly maintained					100		
	There is a clear process for the completion of DPIAs, in advance of the processing of personal data commencing, when considering changes to existing or new projects, services, or systems					40	L1	
	DPIAs are used to inform and assist in the development of privacy information to meet specific needs of the project/service					30	L1	
	There is a comprehensive register maintained for all completed and ongoing DPIAs and this is updated regularly to reflect progress					30	L1	
2	A DPIA process is recognised and embedded throughout the organisation for existing processing of personal data and is formally signed off by the organisation's nominated officer					100		
	The DPIA process is embedded throughout the organisation for the processing of personal data					35	L2	
	All DPIAs are signed off by the organisation's nominated person					35	L2	
	Where the DPIA process identifies any residual high risks, the ICO should be consulted prior to processing commencing					30	L2	
3	DPIA documentation is regularly reviewed and compliance with the process is reported to the Board/Committee					100		
	The DPIA documentation is regularly reviewed to ensure it remains relevant and up to date					60	L3	
	DPIA figures are made available/visible via KPI reports to the Board/Committee					40	L3	
2.6 Freedom of Information Act and Environment Information Regulations								
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these							
Please check to confirm								
1	There are documented policies and procedures for the Freedom of Information Act (FOIA) 2000 compliance and for the Environmental Information Regulations (EIR) 2004 which sets out clear responsibilities for responding and dealing with information requests efficiently and in accordance with the law. Requests are documented and the organisation has adopted the ICO Model Publication Scheme. Procedures and Policies are made available to staff					100		
	There are Freedom of Information Act and Environmental Information Regulations related procedures and relevant guidance outlining high level responsibilities					20	L1	
	All staff responsible for dealing with FOI and EIR requests are aware of their responsibilities and are appropriately trained including coordinating responses as well as dealing with complaints, appeals and internal reviews					20	L1	
	Staff know where to direct any requests they may receive and understand the importance of doing so promptly due to the strict time constraints					20	L1	
	The ICO Model publication scheme has been adopted, this has been made available to members of the public via the organisation's webpage					20	L1	
	There is an FOI and EIR disclosure log which is regularly maintained and up to date					20	L1	
2	The organisation proactively publishes additional information as good practice and this is communicated to and is easily accessible by members of the public					100		
	Clear communication points are indicated on the organisation's website indicating where further/additional information can be found					50	L2	
	Website content is regularly reviewed in relation to the ICO model publication scheme, with data proactively published where appropriate					50	L2	

yes	60
yes	20
yes	20
yes	40
yes	30
yes	30
yes	35
yes	35
yes	30
yes	60
yes	40
yes	20
yes	20
yes	20
yes	20
yes	50
yes	50

3	There is a review process in place for FOIA and EIR processes and compliance with the procedures is regularly monitored					100	
	There is a process in place to monitor FOI and EIR compliance with policies and procedures					35	L3
	There is a process in place to audit the operation of the FOI and EIR procedure					35	L3
	FOI and EIR performance figures are regularly reported to the Board/Committee/Management Team, as appropriate					30	L3
2.7 Privacy Electronic Communications Regulations							
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these						
	Please check to confirm						
1	There are documented policies and procedures for the Privacy Electronic Communications Regulations (PECR) for all electronic marketing messages (by phone, email, text, etc.) and for the management of websites. The policies and procedures set out clear responsibilities and these are made available to staff					100	
	There are Privacy and Electronic Communications Regulations related policies and procedures outlining high level responsibilities. Policies cover relevance of PECR to health promotion / health service promotion messages, as well as to website cookies					60	L1
	All staff responsible for managing websites and public electronic communications are aware of their PECR responsibilities					20	L1
	All staff are aware of where to seek advice in relation to electronic marketing, including health promotional messages					20	L1
2	Consent processes for electronic marketing and cookies are actively managed. Policies and procedures are regularly reviewed, and any changes communicated to staff					100	
	There are policies and procedures in place to ensure cookie consent and consent to receive electronic marketing is up to date and withdrawn consent is effectively managed					50	L2
	Appropriate privacy notice information is provided about website cookies					50	L2
3	Compliance with PECR policies and procedures is regularly reviewed and reported as appropriate to the relevant Board / Committee					100	
	Checks are made to ensure PECR processes and requirements are followed: the management of consent for electronic marketing is documented and the use of website cookies is transparent and - where appropriate - optional					60	L3
	There is a process in place to report the organisation's compliance with PECR processes and requirements to the Board/Committee, etc					40	L3
3. Business Management							
3.1 Business Continuity Plan - This should be assessed in the organisation's individual							
3.2 IG Risk Register							
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these						
	Please check to confirm						
1	The organisation analyses IG risks regularly and documents in a formal IG risk register					100	
	IG risk assessments are routinely conducted					35	L1
	There is a clear process to manage identified IG risks					30	L1
	Risks are documented in an IG risk register and mitigating actions are identified					35	L1
2	There is a clear understanding and management of the identified IG risks					100	
	Where IG risks have been identified, mitigating measures are implemented and shared throughout the organisation where necessary					50	L2
	All high level unmitigated IG risks are reported to Board level, Committee or Management Team, etc as and when required					50	L2
3	Regular review of processes and the IG risk register are undertaken to ensure they remain up to date, with mitigations regularly checked to ensure they remain effective					100	
	Review of processes and IG risk register is regularly conducted, with mitigations regularly checked to ensure they remain effective					50	L3
	There is a process in place to report any actions required from the review of the IG risk register to the Board/Committee/Management Team, etc					50	L3
3.3 Auditing							
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these						
	Please check to confirm						
1	Organisations have audit processes in place to oversee all aspects of the Information Governance agenda					100	
	Auditing processes are in place					100	L1

yes	35
yes	35
yes	30
yes	60
no	0
yes	20
yes	50
yes	50
no	0
no	0
yes	35
yes	30
yes	35
yes	50
yes	50
yes	50
yes	50
yes	100

2	Audit processes are used to regularly monitor appropriate use of personal information					100	
	Audit processes are proactively used to identify risks and inappropriate use and access to information					50	L2
	Mechanisms are in place to follow up and review previous audit actions/recommendations					50	L2
3	There is a review process on all the auditing programmes the organisation undertakes to ensure it remains relevant and feedback is acted on					100	
	Regular checks are made to ensure audit processes are appropriate in accordance with the processing activities					50	L3
	There is a process in place to report audit activity and key findings to the Board/Committee/Management Team, etc					50	L3
4. Individuals Rights							
4.1 Right of Access							
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these						
	Please check to confirm						
1	There is a documented procedure and guidance in place for Subject Access Requests (SARs) that sets out clear responsibilities for responding to information requests efficiently and in accordance with the law					100	
	There are written procedure(s) to follow in respect of the processing of a subject access request					25	L1
	Staff are made aware of how to recognise a subject access request					25	L1
	There is a designated individual or department(s) responsible for dealing with SARs					25	L1
	Members of the public and staff are informed on how to submit a request (SAR) under the GDPR					25	L1
2	Staff members who manage requests have been appropriately trained. A register of requests is maintained					100	
	All SAR requests are documented and managed by a register(s) to log requests, timelines, actions and responses					50	L2
	Staff working in areas where requests are managed are appropriately trained					50	L2
3	There is a robust review process in place in the event of appeals, internal reviews and complaints. Performance figures in relation to SARs are regularly reported to the Board/Committee/Management Team, as appropriate					100	
	SAR performance figures are regularly reported to the Board/Committee/Management Team as appropriate					50	L3
	There is a process in place for dealing with complaints, appeals and internal reviews following a response to a SAR					50	L3
4.2 Right to be Informed							
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these						
	Please check to confirm						
1	The organisation has developed and made available privacy information to respect individuals rights to comply with the General Data Protection Regulation and the Data Protection Act					100	
	Privacy information is provided to individuals which is clear and informative and reflects all statutory requirements. A layered approach is used, with short notices containing key privacy information and additional layers of more detailed information					100	L1
2	Privacy information accommodates a diversity of individuals and is made available and accessible by varied means e.g. health board website etc.					100	
	Provide details of how privacy information is communicated to all individuals					30	L2
	Tools such as DPIAs, WASPI framework, Asset Register, etc. are used to inform and assist in the development of privacy information to meet specific needs of a particular service/project and the intended audience					30	L2
	Communication material is available in a range of formats, taking into consideration individuals with limited access to resources. All formats of communication material use clear, plain language, in particular for any information addressed specifically to a child					40	L2
3	All privacy information is regularly reviewed to ensure they remain fit for purpose to reflect the current nature of all the processing undertaken by the organisation Privacy information is approved by the relevant person with responsibility, IG team/department and documented and linked to the Information Asset Register					100	
	All privacy information is regularly reviewed by the IG team/department or similar to ensure statutory requirements are maintained, and where appropriate changes are made					60	L3
	The organisation can demonstrate that all processing on the Information Asset Register (IAR) is covered by privacy information					40	L3
4.3 Individual's right to object, to erasure, rectification and portability							
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these						
	Please check to confirm						

yes	50
yes	50
yes	50
yes	50
yes	50
yes	25
yes	25
yes	25
yes	25
yes	50
yes	50
yes	100
yes	30
yes	30
yes	40
yes	60
yes	40

1	There are documented procedures and guidance in place to manage objections and requests for rectification, erasure and portability that sets out clear responsibilities for responding to information requests efficiently and in accordance with the law				100					
	There are written procedure(s) to follow in the respect of individual's right to object to the processing, to the erasure, rectification and transfer of personal information				30			L1	yes	30
	Staff are made aware of how to recognise a request in relation to objection, rectification, erasure or portability				30			L1	yes	30
	There is a designated individual/department(s) responsible for dealing with individuals rights in respect of the right to object, to erasure, rectification and portability				20			L1	yes	20
	Members of the public and staff are informed on how to submit a request to object, to erasure, rectification and portability, under the GDPR				20			L1	yes	20
2	Procedures have been implemented by all staff members and those who manage requests have been appropriately trained. A register of requests is maintained					100				
	All request submissions are documented and managed by a register to log requests, timelines, actions and responses					50		L2	yes	50
	Staff working in areas where requests are managed are appropriately trained					50		L2	yes	50
3	There is a review process in place for all requests in relation to erasure, rectification, portability and the objection to processing including a robust process for internal reviews, complaints and appeals. Performance figures in relation to submitted requests are regularly reported to the Board/Committee/ Management team, as appropriate									
	There is a process in place for dealing with complaints, appeals and internal reviews resulting from submitted requests and responses in relation to erasure, rectification, portability and the objection to processing						50	L3	yes	50
	Performance figures for requests are regularly reported to the Board/Committee/Management Team as appropriate						50	L3	yes	50
4.4 Rights related to profiling and automated decision making that has a significant impact on the data subject										
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these									
	Please check to confirm									
1	The organisation has identified any solely or partly automated decision making / profiling that has a significant impact on data subjects and has relevant policies and procedures in place to protect data subject's rights in relation to that processing. Appropriate lawful bases have been identified and care is taken to ensure the rights of children and vulnerable people are protected				100					
	The organisation has a means to identify any solely or partly automated decision making /profiling that has a significant effect on data subjects				30			L1	yes	30
	No solely automated decision making / profiling with significant effect on data subjects takes place unless the lawful bases and additional rights specified in GDPR Article 22 are met				20			L1	yes	20
	The organisation has relevant policies and procedures in place to uphold data subjects' rights in relation to solely and partially automated decisions including right to be informed; right of subject access and where any decision making is solely automated, the right to request a human review of the outcome				30			L1	yes	30
	Checks are made to protect children and vulnerable groups subjects to automated decision making				20			L1	yes	20
2	Individuals are made aware that data protection rights apply to automated decision making. Staff involved in procuring, managing and operating relevant systems are appropriately trained in data protection. DPIAs have been undertaken on any automated decision making that has a significant impact on data subjects					100				
	Appropriate privacy information is provided to data subjects that specifically explains the automated decision making / profiling, its possible effects and their rights					30		L2	yes	30
	Staff are made aware that data protection rights apply to automated processing and they know where to seek advice					20		L2	yes	20
	Staff involved in procuring, managing and operating automated decision making systems are appropriately trained to identify and uphold data protection rights and responsibilities					20		L2	yes	20
	A DPIA has been undertaken on any automated decision making that has a significant impact on data subjects					30		L2	yes	30
3	Automated decision making systems are regularly reviewed, including for accuracy and bias. Identified staff are authorised to undertake reviews, investigate complaints and where necessary change decisions as a result of their findings. The use of all forms of automated decision making is overseen by the appropriate Board / Committee / Management Team, as appropriate									
	Solely automated decision making systems are regularly reviewed by identified staff for accuracy and bias						30	L3	yes	30
	In regard to any solely automated decision making specific staff are authorised and trained to review and where necessary change decisions including in response to complaints						30	L3	yes	30
	The use of automated decision making in the organisation is overseen by an appropriate Board / Committee /Management Team, as appropriate to ensure data protection rights and responsibilities are being upheld						40	L3	yes	40
5. Managing and Securing Records										
5.1 Management of Records										

Please check to confirm												
1	There are processes and procedures for staff to follow for the creation, management, retention, and archiving of records				100							
	Name of the individual responsible for records management for corporate records				50					L1	yes	50
	There are records management related procedures and relevant guidance in place for corporate records				50					L1	yes	50
2	Procedures have been embedded within the organisation and all staff have been informed					100						
	Staff are made aware of their responsibilities through various channels including team meetings, awareness sessions, staff briefings and induction					50				L2	yes	50
	Responsibility for developing guidance/operating procedures has been assigned to an individual or group					50				L2	yes	50
3	Procedures are regularly reviewed and maintained and where available spot checks are made to ensure the procedures are enforced across the organisation							100				
	Policies and procedures are regularly reviewed							40		L3	yes	40
	Spot checks and monitoring are conducted to ensure procedures are followed across the organisation							30		L3	yes	30
	The management of acute health records is reported up to the relevant Board/Committee/Management Team, etc							30		L3	yes	30
5.2 Information Asset Register												
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these											
Please check to confirm												
1	The organisation has an extensive Information Asset Register (IAR)				100							
	The organisation holds an up to date information Asset Register that encompasses all types of records held by the organisation				50					L1	yes	50
	Name/department with responsibility for the management and upkeep of the IAR				50					L1	yes	50
2	There is a reporting procedure available to notify the responsible department of any new/changes with the processing activities and to highlight any areas of non compliance					100						
	Each information asset has a designated Information Asset Owner (IAO) who is responsible for any updates/changes required to the IAR					35				L2	yes	35
	The IAR is referenced in organisational policies and procedures and staff are made aware of their responsibilities					35				L2	yes	35
	There is a process in place for identifying areas of non compliance					30				L2	yes	30
3	The IAR is a working document and the reporting procedure is regularly reviewed to ensure it remains effective and up to date							100				
	The IAR remains as an ongoing working document that is reviewed and maintained regularly							50		L3	yes	50
	There is reporting on performance to the relevant Board/Committee/Management Team, etc							50		L3	yes	50
5.3 Data Accuracy												
5.3.1 Health Records												
5.3.1.1 Acute Records												
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these											
Please check to confirm												
1	The importance of data accuracy is recognised by the organisation and there is supporting guidance and procedures in place to ensure information is updated when necessary				100							
	There are processes in place to ensure that data accuracy checks are undertaken at every episode of patient contact				50					L1	yes	50
	Appropriate guidance is provided to ensure staff maintain accuracy of records				50					L1	yes	50
2	System validation processes exist within the organisation, active steps are taken to address any systems lacking validation					100						
	There are validation processes in place for systems to ensure information remains accurate and up to date					50				L2	yes	50
	There are processes to identify and address any systems where data is not validated on a regular basis					50				L2	yes	50
3	All procedures are regularly reviewed and where available spot checks are made to ensure the procedures are enforced across the organisation							100				
	Checks are made to ensure procedures are followed and these are regularly reviewed							50		L3	yes	50
	There is reporting on performance to the relevant Board/Committee/Management Team, etc							50		L3	yes	50
5.3.1.2 Community Records												
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these											
Please check to confirm												

1	The importance of data accuracy is recognised by the organisation and there is supporting guidance and procedures in place to ensure information is updated when necessary				100			
	There are processes in place to ensure that data accuracy checks are undertaken at every episode of patient contact				50		L1	yes 50
	Appropriate guidance is provided to ensure staff maintain accuracy of records				50		L1	yes 50
2	System validation processes exist within the organisation, active steps are taken to address any systems lacking validation					100		
	There are validation processes in place for systems to ensure information remains accurate and up to date					50	L2	no 0
	There are processes to identify and address any systems where data is not validated on a regular basis					50	L2	no 0
3	All procedures are regularly reviewed and where available spot checks are made to ensure the procedures are enforced across the organisation							100
	Checks are made to ensure procedures are followed and these are regularly reviewed						L3	no 0
	There is reporting on performance to the relevant Board/Committee/Management Team, etc						L3	no 0
5.3.1.3 Mental Health Records								
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these							
Please check to confirm								
1	The importance of data accuracy is recognised by the organisation and there is supporting guidance and procedures in place to ensure information is updated when necessary				100			
	There are processes in place to ensure that data accuracy checks are undertaken at every episode of patient contact				50		L1	yes 50
	Appropriate guidance is provided to ensure staff maintain accuracy of records				50		L1	yes 50
2	System validation processes exist within the organisation, active steps are taken to address any systems lacking validation					100		
	There are validation processes in place for systems to ensure information remains accurate and up to date					50	L2	no 0
	There are processes to identify and address any systems where data is not validated on a regular basis					50	L2	no 0
3	All procedures are regularly reviewed and where available spot checks are made to ensure the procedures are enforced across the organisation							100
	Checks are made to ensure procedures are followed and these are regularly reviewed						L3	no 0
	There is reporting on performance to the relevant Board/Committee/Management Team, etc						L3	no 0
5.3.2 Corporate Records								
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these							
Please check to confirm								
1	The importance of data accuracy is recognised by the organisation and there is supporting guidance and procedures in place to ensure information is updated when necessary				100			
	There are processes in place to ensure that data accuracy checks are undertaken for staff data at every opportunity				50		L1	yes 50
	Appropriate guidance is provided to ensure staff maintain accuracy of records				50		L1	yes 50
2	System validation processes exist within the organisation, active steps are taken to address any systems lacking validation					100		
	There are validation processes in place for systems to ensure information remains accurate and up to date					50	L2	yes 50
	There are processes to identify and address any systems where data is not validated on a regular basis					50	L2	yes 50
3	All procedures are regularly reviewed and where available spot checks are made to ensure the procedures are enforced across the organisation							100
	Checks are made to ensure procedures are followed and these are regularly reviewed						L3	yes 50
	There is reporting on performance to the relevant Board/Committee/Management Team, etc						L3	yes 50
5.4 Retention Schedules, Secure Destruction and Disposal								
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these							
Please check to confirm								
1	The organisation holds retention schedules for the processing and disposal of personal data which outline different retention periods dependent on the categories of personal information				100			
	The organisation holds up to date retention schedules for all organisational records				30		L1	yes 30
	There is a policy/procedure in place for the secure disposal of organisational records				30		L1	yes 30
	Facilities are in place to enable staff to comply with policies and procedures around the secure destruction of organisational records				20		L1	yes 20

Please check to confirm						
1	Information Governance training has been provided to staff in line with the core skills framework. Processes are in place to ensure temporary staff, volunteers and students have received appropriate IG Training				100	
	The organisation is able to meet 50% compliance of mandatory IG training for staff [NOTE - Figures should be taken as of 1st January]				30	L1
	The organisation regularly identifies individuals who have received IG training and those who haven't				20	L1
	A local IG training programme has been developed for employees and made mandatory for induction and refresher IG training				20	L1
	There is a process and/or contractual measures in place to ensure temporary staff, volunteers and students have received IG training				20	L1
	Compliance levels are regularly reported to the appropriate forum				10	L1
2	The organisation has increasing compliance with IG mandatory training. There is a training strategy in place to identify the need and provision of specialist IG training				100	
	The organisation is able to meet 70% target for compliance on mandatory IG training for staff as a minimum [NOTE - Figures should be taken as of 1st January]				40	L2
	A training needs analysis approach is in place to identify any new IG training requirements by staff groups				20	L2
	IG Leads and SMEs (subject matter experts) receive appropriate specialist training to carry out their role				20	L2
	Compliance reports are used to identify areas of low compliance and these areas are targeted for improvement				20	L2
3	The organisation has a high level of mandatory IG training compliance. Training content is regularly reviewed and updated. Feedback is requested where appropriate				100	
	The organisation meets the national target compliance of 85% for mandatory IG training [NOTE - Figures should be taken as of 1st January]				50	L3
	The local IG training programme and associated materials are regularly reviewed and agreed by the IG Team				25	L3
	There is a process in place for feedback on training to be provided by staff where appropriate				25	L3
6.4 Mobile Working and Remote Access - This should be assessed in						
6.5 Secure Destruction and Disposal of IT equipment - This should						
6.6 Surveillance Systems						
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these					
Please check to confirm						
1	The organisation has defined policies and procedures around the use of surveillance systems in use, including CCTV on the premises, body worn recording devices and any other surveillance systems in use within the organisation				100	
	The organisation knows and has a record of what surveillance systems it uses				10	L1
	The organisation has up to date policies and procedures for the use and authorisation of surveillance systems				10	L1
	There is a designated individual responsible for the development and operation of each surveillance system				20	L1
	DPIAs are carried out prior to deployment of any new surveillance system, any risks are identified and recorded with appropriate mitigations implemented prior to use				20	L1
	The organisation has identified a clear purpose and lawful basis for the operation of each surveillance system				20	L1
	Appropriate fair processing notices are clearly displayed where surveillance systems are in use				20	L1
2	Training has been provided to all staff who manage or operate recording devices. Identified risks are highlighted with current and new recording equipment				100	
	Staff who manage or operate recording devices have the necessary level of awareness and understanding of how surveillance fits in with the organisation's data protection requirements				40	L2
	DPIAs have been undertaken for pre-existing systems to assess the privacy and proportionality implications of the use of these devices, and appropriate mitigations are implemented				30	L2
	Retention periods are the minimum required for the stated purpose and are clearly documented. All information and images are securely disposed/deleted once their purpose has been discharged				30	L2
3	There is an effective review process and audit mechanisms are in place to ensure legal requirements, policies and standards are complied with in practice. Compliance reports and issues of concern are reported to the appropriate forum				100	
	Spot checks/internal audits are conducted to ensure compliance with policies and procedures				30	L3
	The organisation reviews the continued use of surveillance systems on a regular basis, at least annually, to ensure they remain necessary, proportionate and effective in meeting its stated purpose for deployment				40	L3
	Compliance reports or issues of concern are raised with the appropriate forum and escalated to the designated responsible individual and DPO as necessary				30	L3
7. Cyber Security - This should be						
8. Information Governance Incident						

yes	30
yes	20
yes	20
yes	20
yes	10
yes	40
yes	20
yes	20
yes	20
yes	50
yes	25
yes	25
yes	10
yes	10
yes	20
yes	20
yes	20
yes	40
yes	30
yes	30
yes	30
yes	30
yes	40
yes	30

8.1 Reporting Data Breaches						
0	The organisation has considered the requirements necessary to progress and confirm action is being taken to working towards these Please check to confirm					
1	There are supporting policies and procedures available to inform individuals of the reporting structure of any Information Governance related incidents. Such policies and procedures also detail the requirements around the reporting of data breaches to the ICO, data subjects and Welsh Government (when required). These are made easily available to staff so they are aware of their responsibilities			100		
	The organisation holds supporting policies and procedures around the internal reporting of Information Governance (IG) related incidents			40		L1
	Policies and procedures are in place that set out who, when, how and what to include when reporting a breach to the ICO, data subject and Welsh Government in line with the National Breach Reporting Guidance (when available)			30		L1
	Staff are made aware of their responsibility to report IG incidents			30		L1
2	A confidential system for reporting security breaches internally is actively used and appropriate communication is had with external contacts by the IG Leads/Team to manage the effects of data breaches. IG incidents and near misses are appropriately documented and managed				100	
	All IG related incidents and near misses are reported and documented internally through the incident management system and escalated to the DPO when appropriate. Any trends are identified				40	L2
	There is an investigation process in place to follow up on specific IG incidents and trends				30	L2
	Staff who implement measures to manage damage control are appropriately trained				30	L2
3	Improvements are made to reduce the chance of re-occurrence and are reported to the Board. A review process is in place to ensure the notification procedure remains relevant and works in practice					100
	Lessons learnt and investigation outcomes are effectively communicated to the relevant Board/Committee via reports such as KPIs					40
	Lessons learnt and outcomes are communicated to staff					30
	Checks are made to ensure procedures are followed and these are regularly reviewed					30

yes	40
yes	30
yes	30
yes	40
yes	30
yes	30
yes	40
yes	30
yes	30

Total		
Level 2	Level 3	Overall
2800	2780	8380
2600	2480	7860
93%	89%	94%

Responsibilities	
Level 2	Level 3
700	700
700	600
100%	86%

2.1 Information Governance Management			
	Level 1	Level 2	Level 3
Total Available	100	100	100
Score Achieved	100	100	100
Compliance Percentage	100%	100%	100%

2.2 Policies and Procedures		
	Level 1	Level 2
Total Available	100	100
Score Achieved	100	100
Compliance Percentage	100%	100%

Management	
Level 2	Level 3
200	200
200	200
100%	100%

3.2 IG Risk Register			
	Level 1	Level 2	Level 3
Total Available	100	100	100
Score Achieved	100	100	100
Compliance Percentage	100%	100%	100%

3.3 Auditing		
	Level 1	Level 2
Total Available	100	100
Score Achieved	100	100
Compliance Percentage	100%	100%

Equal Rights	
Level 2	Level 3
400	400
400	400
100%	100%

4.1 Right of Access			
	Level 1	Level 2	Level 3
Total Available	100	100	100
Score Achieved	100	100	100
Compliance Percentage	100%	100%	100%

4.2 Right to be Informed		
	Level 1	Level 2
Total Available	100	100
Score Achieved	100	100
Compliance Percentage	100%	100%

Securing Records	
Level 2	Level 3
1000	980
800	780

5.1 Record Management Procedures - 5.1.1 Health Records			
	Level 1	Level 2	Level 3
Total Available	300	300	300
Score Achieved	300	300	300

5.1 Record Management Procedures - 5.1.2 Corpo		
	Level 1	Level 2
Total Available	100	100
Score Achieved	100	100

80%	80%
-----	-----

Organisational Measures	
Level 2	Level 3
400	400
400	400
100%	100%

ce Incident Management	
Level 2	Level 3
100	100
100	100
100%	100%

Compliance Percentage	100%	100%	100%
-----------------------	------	------	------

6.1 Physical Security Measures			
	Level 1	Level 2	Level 3
Total Available	100	100	100
Score Achieved	100	100	100
Compliance Percentage	100%	100%	100%

8.1 Reporting Data Breaches			
	Level 1	Level 2	Level 3
Total Available	100	100	100
Score Achieved	100	100	100
Compliance Percentage	100%	100%	100%

Compliance Percentage	100%	100%
-----------------------	------	------

6.2 Technical Security Measures		
	Level 1	Level 2
Total Available	100	100
Score Achieved	100	100
Compliance Percentage	100%	100%

Level 3
100
100
100%

2.3 Information Sharing			
	Level 1	Level 2	Level 3
Total Available	100	100	100
Score Achieved	100	100	100
Compliance Percentage	100%	100%	100%

2.4 Contracts and Agreements			
	Level 1	Level 2	Level 3
Total Available	100	100	100
Score Achieved	100	100	100
Compliance Percentage	100%	100%	100%

Level 3
100
100
100%

4.3 Individual's right to object, to erasure, to rectification and to portability			
	Level 1	Level 2	Level 3
Total Available	100	100	100
Score Achieved	100	100	100
Compliance Percentage	100%	100%	100%

4.4 Rights related to profiling and automated decision making			
	Level 1	Level 2	Level 3
Total Available	100	100	100
Score Achieved	100	100	100
Compliance Percentage	100%	100%	100%

rate Records
Level 3
100
100

5.2 Information Asset Register			
	Level 1	Level 2	Level 3
Total Available	100	100	100
Score Achieved	100	100	100

5.3 Data Accuracy - 5.3.1 Health Records			
	Level 1	Level 2	Level 3
Total Available	300	300	300
Score Achieved	300	100	100

100%

Level 3
100
100
100%

Compliance Percentage	100%	100%	100%
-----------------------	------	------	------

6.3 Organisational Measures (Training and Awareness)			
	Level 1	Level 2	Level 3
Total Available	100	100	100
Score Achieved	100	100	100
Compliance Percentage	100%	100%	100%

Compliance Percentage	100%	33%	33%
-----------------------	------	-----	-----

6.6 Surveillance Systems			
	Level 1	Level 2	Level 3
Total Available	100	100	100
Score Achieved	100	100	100
Compliance Percentage	100%	100%	100%

2.5 Data Protection Impact Assessments			
	Level 1	Level 2	Level 3
Total Available	100	100	100
Score Achieved	100	100	100
Compliance Percentage	100%	100%	100%

2.6 Freedom of Information Act and Environment Information Regulation			
	Level 1	Level 2	Level 3
Total Available	100	100	100
Score Achieved	100	100	100
Compliance Percentage	100%	100%	100%

2.7 Privacy Electronic Con	
	Level 1
Total Available	100
Score Achieved	80
Compliance Percentage	80%

5.3 Data Accuracy - 5.3.2 Corporate Records			
	Level 1	Level 2	Level 3
Total Available	100	100	100
Score Achieved	100	100	100

5.4 Retention Schedules, Secure Destruction and Disposal			
	Level 1	Level 2	Level 3
Total Available	100	100	80
Score Achieved	100	100	80

Compliance Percentage	100%	100%	100%
------------------------------	-------------	-------------	-------------

Compliance Percentage	100%	100%	100%
------------------------------	-------------	-------------	-------------

Communications Regulations	
Level 2	Level 3
100	100
100	0
100%	0%