



GIG
CYMRU
NHS
WALES

Iechyd a Gofal
Digidol Cymru
Digital Health
and Care Wales



Cefnogiir gan
Lywodraeth Cymru
Supported by
Welsh Government



Cytundeb Rhannu Gwybodaeth
Bersonol Cymru
Wales Accord on the
Sharing of Personal Information

Code of **Conduct Consultation Report**

OVERVIEW

This document provides a summary of the responses to the consultation on the Wales Accord on the Sharing of Personal Information (WASPI) proposal to become an approved Code of Conduct.

ACTION REQUIRED

This document is for information only. Further information and related documents, large print, Braille and alternative language versions of this document are available on request.

CONTACT DETAILS

FOR FURTHER INFORMATION:

Dave Parsons
WASPI Code Manager
Digital Health & Care Wales
Information Governance
Tŷ Glan-yr-Afon
21 Cowbridge Road East
Cardiff CF11 9AD
Email: Dave.Parsons@wales.nhs.uk

This document is also available in [Welsh](#)

CONTENTS

INTRODUCTION AND BACKGROUND	4
CONSULTATION DETAILS	5
GLOSSARY	6
ANALYSIS METHODOLOGY	7
SUMMARY OF RESPONDENTS	8
SUMMARY OF RESPONSES BY QUESTION	9
CONCLUSION/ NEXT STEPS	27



Introduction and Background

Sharing of personal data is an essential element of delivering effective services to citizens.

The existing Wales Accord on the Sharing of Personal Information (WASPI) is a framework for those organisations that hold information about living individuals (personal data) and who consider it appropriate or necessary to share it with others.

The WASPI framework will build upon the existing framework with the intention of applying to become an approved Information Commissioner's Office (ICO) Code of Conduct under the provisions of article 40 of the UK General Data Protection Regulation. Offering members and their stakeholders, including the public, additional assurance around organisational practices of data sharing.

The code can provide an approved assurance model for organisations to confidently document the lawful sharing of personal and sensitive data across multiple sectors.

In order to fulfil the Welsh Ministers' commitment to engage with stakeholders and the requirements of the Information Commissioner's Office (ICO) when developing the proposal for the WASPI Code of Conduct, we embarked on an ambitious engagement process, involving stakeholder workshops and focus sessions.

Many professional representatives from Local Authorities, Health Boards and Trusts, Police, Fire and Rescue and Third Sector organisations provided feedback, which has guided and assisted us in preparing the proposals which will be taken to the ICO for determination.

We believe the successful implementation of WASPI as a Code of Conduct approved by the ICO will encourage better decision making and ultimately deliver better outcomes and transparency for citizens through ensuring data sharing takes place in a controlled, consistent, and regularly reviewed manner.



Consultation Details

The WASPI Code of Code public consultation ran from 20th February to 28th April 2023.

Responses were received in numerous ways:

- **Online via the survey consultation form**
- **Completing the easy read consultation document and submitting via email**
- **Verbal feedback via consultation launch event held on 2nd March 2023 and through attendance at regional and national forums.**

The consultation sought views on:

- **whether the proposed code was clear and enhanced the existing WASPI framework.**
- **whether the requirements of prospective code members, which are necessary to make the code compliant with the Information Commissioner's Office code of conduct expectations, were clear.**
- **whether organisations would intend to sign up to become a code member.**

All consultation documents are available on the following page: [Wales Accord on the Sharing of Personal Information \(WASPI\) Code of Conduct | GOV.WALES](#) and a list has been provided below:

WASPI Code of Conduct Consultation document

- **WASPI Code of Conduct**
- **Governance & Information Risk Assurance Procedure**
- **WASPI Code of Conduct Audit Strategy**
- **Complaint/Appeal Handling Procedure**

Glossary

Quality Assurance Process is the process through which Information Sharing Protocols are checked for consistent use of the WASPI templates and appropriate application of the data protection legislation. The process involves five regional Quality Assurance groups across Wales overseeing the process.

WASPI Accord is a common set of principles and standards which support the sharing of personal information to deliver services to the people of Wales. Signing the Accord allows an organisation to become a “WASPI member” and demonstrates a commitment to apply the principles within the Code. WASPI membership is separate to Code Membership and is therefore not detailed within this Code. However, organisations looking to attain Code Membership are encouraged to sign up to the Accord before submitting their application. Further detail on WASPI membership can be found via the WASPI website.

Monitoring Body means a legal entity, or a defined part of a legal entity such that it is legally responsible for its monitoring activities. The monitoring body shall agree to be responsible for its monitoring role and therefore responsible for a fine under UK GDPR Article 83(4)(c) and S.155 DPA 2018.

Code Owner means associations or other bodies representing categories of controllers or processors who have responsibility of the code, ensures the code is periodically reviewed, and that capacity and tools are provided to the monitoring body to discharge their responsibilities.

DHCW means Digital Health and Care Wales. A Special Health Authority and statutory body established under statutory instrument 2020 No. 1451 (W.313), ‘The Digital Health and Care Wales (Establishment and Membership) Order 2020’.

Analysis Methodology

All consultation responses received online via Microsoft Forms were downloaded. The responses received via email, which consisted of letter responses and emails were uploaded into the downloaded sheet to ensure that a full data set with consistent formatting was available for analysis.

The initial quantitative analysis of each question provided the early opportunity to highlight areas that respondents indicated would need further consideration. Each of the comments provided by respondents throughout the consultation were collated, along with the respondent ID and whether the respondent answered 'yes/no' where applicable. There were occasions where respondents were not required to answer 'yes/no', but where responses to questions were provided. These were then grouped by question, analysed and themed to allow focus specific areas of interest.

Number of complete responses received

38

Number of comments received

103



Summary of Respondents

The WASPI Code of Conduct consultation generated a total of 38 complete responses.

The consultation did not require every question to be answered before submission however, for the 38 complete submissions there was an 100% completion rate.

Of the 38 completed responses, 37 respondents identified as a registered organisations, with 1 respondent providing a collective response on behalf of a professional group of data protection/information governance professionals. Within the list it is acknowledged that 24 respondents indicated they would like their name to remain anonymous from any consultation report, therefore names of organisations/groups only, who provided responses, have been published within this report.

The breakdown of respondents who submitted complete responses were:

- 9 NHS representative/organisations. e.g. Local Health boards, NHS Trusts and Special Health Authorities
- 11 Local Authorities
- 2 Police Forces
- 1 Fire and Rescue Service
- 3 Housing Associations
- 12 other organisations, including Welsh Government, Audit Wales, Welsh Local Government Association, National Resources Wales, Transport for Wales, citizens/service users and a collective number of local authorities providing a collaborative response.

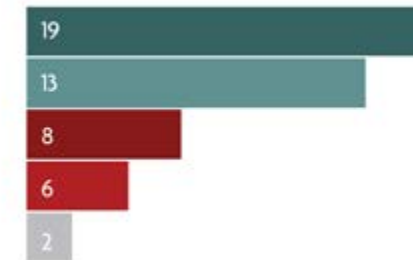
Summary of Responses by question



Theme

- Greater citizen reassurance
- Increased stakeholder & public trust
- Strengthen existing framework
- Benefits of code not clear
- No added benefits

Times Identified



Question 1: Please explain whether you believe the proposed code offers additional assurances on data sharing for citizens and what benefits you believe this can provide to your organisation if applicable.

Over 80% of respondents provided a positive response that they believed that the proposed code would offer assurances on data sharing for citizens.

The majority of respondents provided a clear positive indication that creating an enhanced WASPI framework would provide greater confidence to organisations on their approach to information sharing with this being likely to result in better / less risk averse approaches to sharing of personal data about Welsh citizens. By improving information sharing, this enables better service delivery,

allowing Welsh citizens to receive better service. A number of themes on benefits were identified from responses in respect of greater reassurance to citizens that data sharing activities were compliant and regularly reviewed, together with increasing stakeholder and public trust in organisational data sharing practices with the benefits to organisations of a WASPI code of conduct.

The code, once approved by the ICO, would help to build public trust in the use of data by those who sign up as well as increasing the confidence of public authorities to share data by following a process that they can be assured conforms to the Information Commissioners' Office (ICO) expectations.

Other themed responses included:

- the proposed code would offer additional assurances around data sharing. The enhanced monitoring and audit proposals, in particular, would provide assurance that Information Sharing Protocol (ISPs) are being reviewed, maintained, and, where appropriate, renewed.
- the ICO's approval of the WASPI code of conduct would enhance the framework's status - the public would be assured that the UK regulator considers the framework to be compliant with data protection legislation.

There was one respondent who questioned why the code only covered ISP's with another respondent querying why the code would not cover all elements of UK GDPR compliance.

WASPI Team response:

The proposed Code of Conduct is designed to support compliance and demonstrate to the ICO how organisations comply with data sharing activities, specifically that of legal basis of regular sharing of personal information between organisations and citizen transparency. It is not designed to cover the entire principles of the UK GDPR. An ICO Code of Conduct would generally be designed to support areas of compliance not to cover all the principles of data protection.

Two respondents did not believe that the proposed code would have any added benefits for citizens or their organisations. One respondent did not believe that the consultation proposal adequately articulated the specific benefits over and above the existing WASPI Accord, together with being unclear as to how this proposal will address some of the shortfalls with the current model, namely, out of date agreements relying on a lawful basis that may no longer be valid and the lack of a template to support joint controller data sharing.

WASPI Team response:

The benefits of the Code and how this will address some of the issues raised are set out within the proposal, including a requirement to ensure that organisations regularly review Information Sharing Protocols.

Work is already progressing, as part of the existing WASPI Accord framework, to develop further national standard templates, including a joint data controller agreement which would be made available through the WASPI website.

We recognise that the ICO already has a Data Sharing Code of Practice, however this proposal is not a Code of Practice but rather a Code of Conduct approved by the ICO which would have to demonstrate actual benefits and compliance that any organisation signed up to WASPI would have to demonstrate, thus aiding an organisations compliance with data sharing practices.

One respondent questioned if the code is intended to provide greater assurance, what the success factors be and how would they be measured, with another respondent being unclear from examining the proposed changes whether they provide added value and safety for vulnerable older people in Wales and whether resources should be directed towards why information is not shared and towards multi agency engagement and training on the importance of sharing the right information in the right way and at the right time.

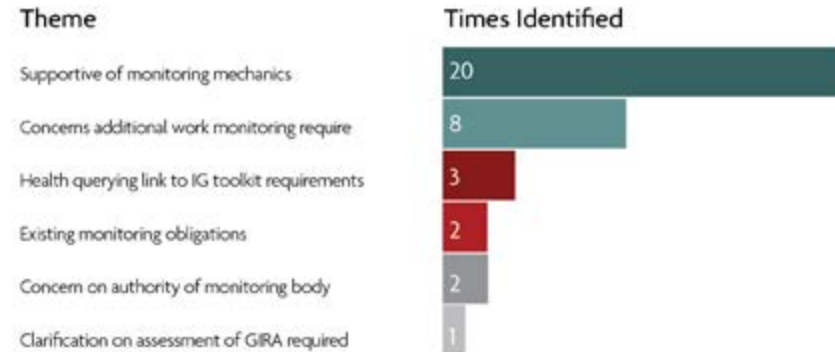
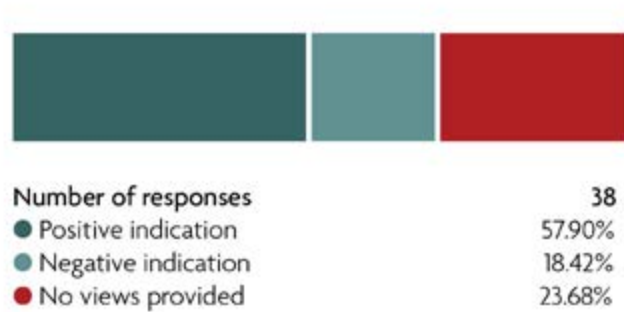
WASPI Team response:

The proposed code creates a compliance standard for data sharing arrangements.

There have been numerous examples of where lack of information sharing between agencies has resulted in neglect or death of individuals. One recent finding of a child practice review case in Wales set out how information sharing between agencies did not take place, resulting in a significant child practice review action plan being developed, which in part focuses on information sharing practices and the need for ensuring data sharing is effectively reviewed.

One of the significant risks and problems that the code of conduct will address will include the requirement of regular reviewing of Information Sharing Protocols. This will support actions from recent child practice reviews to ensure a committed review plan of regularly reviewing information sharing activities becomes embedded into public bodies.

The WASPI service will consider how training resources could be developed to support organisations with regards to data sharing standards and WASPI processes, however responsibility for adequate and appropriate information sharing practices is ultimately the responsibility for individual data controllers.



Question 2: The proposed code sets a number of monitoring mechanisms which will be implemented to ensure that a code member remains compliant. Do you have any views on the intended monitoring mechanisms or any related issues which we have not specifically addressed, please use this space to report them.

This question requested views in respect of the assurance and audit mechanisms associated with Code of Conduct membership. Most respondents either indicated a positive response to the proposed monitoring mechanisms or no views were provided in answer to the question. In some cases, organisations provided multiple views within their response, which is reflected within the breakdown of theme of the responses, indicating both opportunities for consideration with regards to the proposals and also offering supportive feedback to the approach to monitoring proposed.

The supportive feedback covering the monitoring mechanism typically covered the same theme with respondents feeling that the monitoring mechanisms were required and proportionate to ensure that member organisations maintain compliance to the assurances which the code seeks to address.

Most respondents who provided a positive comment also felt that monitoring would be expected for other standards and that ongoing compliance being maintained would provide greater credibility to the purposes which the code seeks to address.

One respondent questioned whether individual data controllers would be required to complete annual governance and assurance requirements, and what the requirements would be for organisations, such as schools, who may contract Data Protection Officer (DPO) services with a Local Authority or third party contractor.

WASPI Team response:

The Monitoring controls will apply to each data controller who will individually be required to demonstrate and provide evidence of standards expected. In instances where organisations may contract out elements of data protection support, the organisation who has signed up as a code member would be required to fulfil and demonstrate meeting the audit and assurance requirements and supply annual governance assurances.

Eight respondents were mindful that monitoring may involve additional work for Information Governance departments and resources. Two respondents questioned whether the proposed three-year governance and information risk procedure could supplement or replace any existing audit responsibilities to avoid duplication of effort, with one respondent suggesting a change from a three year to five-year audit programme.

Several NHS organisations queried within their response whether the annual assurance processes could replace or link with existing Welsh Information Governance Toolkit responsibilities which already exist across Health, as these already require Information Governance assurance evidence to be provided on an annual basis.

WASPI Team response:

Annual assurance and audit assessments will be streamlined to ensure that they minimise impacts on organisations. The WASPI team will look to utilise tools, such as the intended deployment of

the Information Sharing Gateway to support organisations through assurance and audit requirements where possible. Organisations would be able to liaise with any existing regulators/inspectors and use the assurance and audit evidence provided to as part of the code of conduct requirements to support existing obligations they may have.

It would be for each organisation to identify the relevant officers for completing assurance assessments, however we would expect this to typically involve Data Protection Officer, Senior Information Risk Owner's, Caldicott Leads within organisations. Auditing by external bodies would not cover the specific details associated with the proposed WASPI code of conduct, however it may be possible for information provided as part of evidence to existing audit/assurances to be permitted.

In developing the proposed Governance and Information Risk Assurance (GIRA) framework, the WASPI Team has considered existing audit requirements across key public services, taking into specific consideration assessments which already exist, for example those obligations set out within Information Assurance for Small and Medium Enterprises (IASME), Cyber Essentials, Governance and Information Risk Returns adopted across UK Police Forces and Information Governance Toolkit requirements across Health.

For Health Boards and Trusts, opportunities to align annual assessments will be considered to be linked into existing assurance requirements within the Welsh IG Toolkit, to support organisations with returning assurance assessments through one annual process.



Number of responses	
● Yes	38 92.11%
● No	2.63%
● Unsure	5.26%

Question 3: Does the code clearly set out the roles of the code owner and monitoring body.

This question focused on the intended roles of both the proposed code owner and monitoring body to be established. The majority of respondents indicated that the proposed code of conduct clearly set out the roles of the code owner and monitoring body.

Whilst the overarching position on the roles of the code owner and monitoring body appears from the responses received to be clear, there were a number of respondents who questioned the approach to Digital Health and Care Wales (DHCW) being both the code owner and monitoring body, and in particular, feedback was received over whether the proposed code could more clearly set out how the independence of the monitoring body from the code owner, who would also potentially be a signatory to the Code of Conduct, could be demonstrated.

One respondent did not believe the WASPI team, as code owners, were successfully able to demonstrate that the monitoring body is independent or impartial from code members, the profession, industry or sector to which the code applies, particularly as this could also include DHCW as a data sharing organisation.

WASPI Team response:

The UK GDPR sets out a framework for the type and structure of a monitoring body. A monitoring body can be an internal body as long as evidence can be provided of adequate procedures and rules that allow monitoring of compliance with a code independently and without undue pressure or influence from the code owner or the code members.

It is intended that legal and decision-making procedures will be established to enable the Monitoring Body to demonstrate that it will act independently in its choice and application of its actions and sanctions. This will be demonstrated through terms of reference, powers, and operation of committees or personnel that may be involved with the Monitoring Body.

DHCW as the proposed code owner will put forward proposals for their code monitoring body in accordance with Article 41(2) as part of formal ICO application requirements. This submission is in order to gain accreditation and demonstrate how independence in relation to the subject matter of the code, to the satisfaction of the ICO in accordance with A41(2)(a) UK GDPR, is intended to be met. This assessment will be considered by the ICO as part of decision-making processes to gain accreditation for the monitoring body.

One respondent questioned whether Welsh Government and the Wales Audit Office, who are set up within their constitution to undertake auditing roles such as these have been consulted on the proposals and whether there would be any conflict in work programmes and duplication of effort, with two respondents looking for further clarity on the roles and in particular independence of the monitoring body from its direct organisation.

WASPI Team response:

ICO codes of conduct are tools which enable sectors to identify and resolve key data protection challenges with assurance from ICO that the code, and its monitoring, is appropriate. The WASPI code of conduct proposal would enable detailed compliance, not commonly assured, or considered by existing audit/regularly functions to be monitored, providing assurance to organisations, the public and the ICO that appropriate data sharing controls are in place.

Both Welsh Government and Audit Wales have been consulted on the proposals and their feedback will be used to shape the final decisions on the code of conduct and monitoring body proposals.

One respondent queried whether it would be more appropriate for Welsh Government to be the code owner and for the monitoring body to be independent of any particular service sector, particularly so in relation to adoption of the code given that this evolution of WASPI recognises that the sharing of data goes beyond solely health data and covers information and stakeholders in areas such as education, safety, crime prevention and more generally well-being.

WASPI Team response:

Welsh Government have been consulted on the proposals and their feedback will be used to shape the final decisions on the code of conduct and monitoring body proposals.

Funding to deliver the WASPI framework is provided to Digital Health and Care Wales through Welsh Government and therefore as the service and staff who specialise in this area are within DHCW, we are satisfied that we would be the most appropriate organisation to take on responsibilities associated with the proposed code of conduct.

As the WASPI team are not part of any direct data sharing activities, we believe that we can successfully demonstrate how we act independently. In order to gain accreditation and demonstrate how independence in relation to the subject matter of the code, to the satisfaction of the ICO in accordance with A41(2)(a) UK GDPR, we would intend to evidence this as part of any future applications on both the code and monitoring body functions.



Question 4: How does your organisation feel being subject to monitoring mechanisms and evaluation, and the implications of not meeting requirements resulting in the potential for code membership to be revoked?

Over half of the respondents provided a positive indication of their organisation being subject to monitoring mechanisms, with 17 of these respondents providing additional statements of support welcoming or having no concerns with monitoring mechanisms being adopted which their organisations would be subject to.

Some respondents welcomed the proposals as a baseline to ensure that as a member they meet the requirements and have an ongoing commitment to demonstrating that they comply with data protection laws, with others welcoming this as a clear enhancement and agreeing that membership to the code should be something which is earned.

Some public bodies indicated that they were not concerned with monitoring, as in many cases their organisations are already subject to audit and regulatory scrutiny. These respondents therefore welcomed the additional audit assurance which would demonstrate to the ICO, their citizens and partner organisations their compliance with data sharing standards to the highest levels.

Several respondents highlighted concerns over additional workloads that monitoring requirements could potentially create, particularly for organisations who are already subject to internal audit and external regulatory assurances, with several health boards also questioning how the monitoring assurance controls fit into existing Welsh Information Governance Toolkit submission requirements which already exist across health.

WASPI Team response:

Annual assurance and audit monitoring will be streamlined to ensure that they minimise impacts on organisations. Whilst we realise that organisations may already have assurance and governance controls in place, the purpose of an ICO Code of Conduct is to provide assurance to the ICO that the specific commitments of the code are being continually met by a code member.

In creating the proposed monitoring processes, the WASPI Team have considered existing audit requirements across key public services, taking into specific consideration assessments which already exist, for example those obligations set out within IASME, Cyber Essentials, Governance and Information Risk Returns adopted across UK Police Forces and Information Governance Toolkit requirements across Health.

It is also intended that the monitoring mechanisms would be supported through tools currently being developed, such as the Information Sharing Gateway. Organisations would be able to liaise with any existing regulators/inspectors and use the assurance and audits provided through the WASPI Code of Conduct processes to support other existing obligations.

One respondent questioned DHCW's proposed role of the monitoring body, suggesting that DHCW, whose function is to build and design systems and services for health and care in Wales, would not be appropriate to conduct monitoring of organisations compliance, with another respondent questioning the benefits additional monitoring and assurance mechanism will bring that do not already exist.

WASPI Team response:

Monitoring mechanisms are vital in demonstrating the added value that the ICO would expect a Code of Conduct to provide and provide assurances to the regulator that members of a code are meeting requirements. There may be opportunities for organisations to align to existing governance assurances they may be already subject to, however as WASPI applies to all sectors, establishing something which could be specific for all sectors aligned to differing annual governance statements would not be practical.

The proposals would be for the WASPI Team, within Digital Health and Care Wales to be approved by the ICO to become a Monitoring Body. During this application process Digital Health and Care Wales are committed to ensuring that evidence is provided to the ICO which sets out how the service would act independently to the wider organisation in discharging these duties.

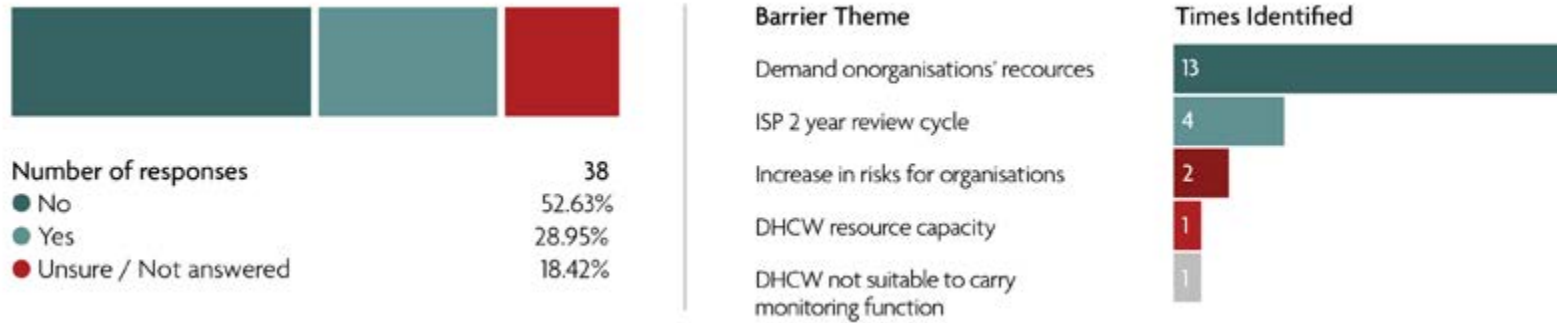
Observations were provided from one respondent in respect of the risks that monitoring, reporting and sanctions could potentially create, when signing up to the code would be voluntary. The observations provided also suggested that organisations may find themselves subject to sanction for a wide variety of reasons, many of which effectively impose requirements on organisations that would be impossible for many potential signatories to abide by on a practical level. For example, some national bodies refuse to accept data sharing agreements provided to them on WASPI templates, yet the code stipulates that the use by a code member of an agreement on a non-WASPI template is a matter for sanction.

WASPI Team response:

Whilst joining as a code member is voluntary, upon committing the organisation will be bound by the requirements of the code. The code is a form of enabling organisations to demonstrate how they comply with elements of the UK GDPR which relate to data sharing. Failure to demonstrate controls in place could result in sanctions as such failures would be considered breaches of the ICO code requirements. However, these, as outlined within the proposal will always be a last resort and the monitoring body would be committed to working with any member organisation to avoid such sanctions being applied. Ultimately it is a decision for each organisation to make as to whether to sign up and commit to the code.

WASPI, its principles and controls which would be subject to assurance are focused on data sharing between organisations in Wales. We recognise that WASPI templates are not always used outside of Wales to support data sharing activities with Welsh organisations, therefore such agreements will not be focused on during assurance and audits, which will solely focus on WASPI template information sharing activities or data sharing commitments where use of WASPI and the ISP template would be applicable.

Question 5: Are there any barriers which may prevent your organisation from signing up to become a code member and would your organisation be intended to become a code member?



The breakdown of responses in respect of whether there are any barriers which may prevent organisations from signing up to become a code member are outlined below:



Just over half of the respondents indicated that there were no barriers which may prevent their organisations from signing up to the code as proposed, with just over a quarter of respondents indicating some barriers which may prevent sign up, with many of these having a similar theme.

Whilst the majority of responses indicated that there were no current barriers is really positive in respect of the proposals, focusing on those who have indicated some potential barriers and/or concerns is a key part of the consultation. These responses allow the WASPI

service to review and consider any alterations which could be made to the code to alleviate concerns raised, and increase the confidence in organisational uptake in the proposed code.

Almost half of respondents indicated that they wished to become a code member, with only a small number of respondents indicating that they did not or that it would not be applicable for their organisation.

A common theme in the feedback received indicated concerns over resources for organisations who may wish to sign up. Several respondents outlined concerns over limited information governance/data protection/data sharing resources within their organisations and concern over the need to have to comply with annual governance assurance and three year audit schedules potentially being unsustainable within their limited resource capacity.

Four respondents specifically indicated a resource concern linked into the requirements that organisations would be required to continually achieve maintaining Information Sharing Protocols in line with the proposed two year review cycle, with suggestions to potentially review the two year review period which could make complying with the standards achievable and alleviate some challenges to maintaining information sharing protocols.

WASPI Team response:

The annual assurance proposals will be used to assess specifically whether a code member organisation is meeting the requirements specific to the ICO approved Code of Conduct. This is vital in demonstrating the added value that the ICO would expect a Code of Conduct to provide and provide assurances to the regulator that members of a code are meeting expectations.

There may be opportunities for organisations to align annual assurances they provide to their own specific annual governance

statements. However, as WASPI applies to all sectors, establishing something which could be specific for all sectors aligned to differing annual governance statements would not be practical. Most public sector organisations will already be subject to annual governance assessments so there may be some duplication to existing processes in regard to some question sets, and where this is the case minimal additional work is created.

For Health Boards and Trusts opportunities to align annual assessments could be linked into existing assurance activities such as the Welsh IG Toolkit which is required to be provided on an annual basis. It would be envisaged that adding of the additional question sets associated with WASPI Code of Conduct compliance would make this achievable for Health Boards, Trusts, Special Health Authorities and anyone else completing the Welsh IG Toolkit to maintain.

The WASPI team will look to utilise tools, such as the creation of the Information Sharing Gateway platform to support organisations through assurance and audit requirements where possible.

We believe that the three year audit programme is balanced and in many cases where organisations are already subject to audit scrutiny, engagement with a three year audit should be easily achieved. The proposed controls can support organisations with assurance they provide to other regulators or audit assurance processes and will ultimately provide citizens with increased confidence and trust that data sharing activities are regularly reviewed, further enhancing controls that ensure appropriate information is shared with the

correct agencies to deliver the best possible services.

The response from one public body further emphasised concerns with mandating the use of WASPI agreements for all reciprocal personal data sharing operations, combined with the further requirement to keep these updated with a minimum frequency of two years, advising that this would be potentially prohibitive in terms of available information governance resource.

WASPI Team response:

The WASPI team has considered both comments and feedback provided as part of this consultation and as part of ongoing service delivery with the existing WASPI framework on the effectiveness of the current best practice two year review periods for information sharing protocols.

As a result of feedback and a review of processes of how reviews currently take place within the existing framework, the WASPI team have determined the current two year review proposals could be changed to a three year review within the proposed code of conduct, as well as implementing the same changes to processes as part of the existing WASPI framework standards.

There were two specific comments raised through the consultation in respect of whether creating a code of conduct and mandating standards which are currently best practice, actually creates a risk for organisations to sign up to, and therefore could be a potentially seen as a barrier to organisations signing up. There was one further comment from a respondent who did not believe that Digital Health

and Care Wales would be suitable to hold monitoring body functions.

WASPI Team response:

It would ultimately be a consideration for each organisation to determine their commitment to signing up to the code of conduct.

The proposed code is designed to demonstrate how an organisation is compliant with data protection practices associated with data sharing, we would therefore be of the view that signing up to the code of conduct approved by the ICO, would be added value to an organisation in demonstrating controls in place to mitigate against risks. We would see an organisation holding an ICO approved accredited code membership being something which is significantly advantageous and increases public confidence and trust.

During this application process for the monitoring body accreditation Digital Health and Care Wales are committed to ensuring that evidence is provided to the ICO which sets out how the service will act independently to the wider organisation in discharging such duties. As the organisation that has successfully implemented WASPI to a UK wide recognised standard, and as a provider of digital solutions as opposed to direct public facing service provider, we believe that we are best positioned to deliver the proposed code and its monitoring body requirements.



Question 6: Code membership will be subject to annual Governance & Information Risk Assurance (GIRA) and a committed 3-year audit requirement. Are there any barriers to the intended GIRA or any standards which you feel could be implemented to assist your organisation with demonstrating meeting the requirements of code membership?

Over half of the respondents indicated that there were no barriers which may prevent their organisations to committing to the Governance & Information Risk Assurance (GIRA) and three year audit requirements associated with the code, with the themes from respondents similar to those provided in answer to question 5.

Several respondents were welcoming that there was no intended 'membership' fee proposed at this time for signing up to the code. Respondents also recognised the assurance and audit processes being beneficial for organisations to be

operating on the same standards across all Welsh public sectors with being badged to a standard demonstrating commitment to the highest data protection standards.

Once again the main theme in the feedback received indicated concerns over resources for organisations to fulfil the requirements of the annual governance assurance and three year audit within their limited resources, however additionally there were a number of respondents who indicated that they were unsure of whether there would be any barriers to the assurance processes without understanding more about what the requirements of the three year audit on their organisation would entail, with one response suggesting that if the code were enacted as presently set out, an exhaustive audit on such a frequency might inadvertently serve to be a deterrent to joining the code, which is obviously not the WASPI team's intention.

WASPI Team response:

Becoming an ICO approved code of conduct would provide assurance that the code and its monitoring is appropriate and will help organisations to apply the UK GDPR effectively and consistently.

A code of conduct is required to describe the appropriate monitoring mechanisms in place that code members are required to achieved. The proposed code is designed to demonstrate how an organisation is compliant with data protection practices associated with data sharing with the Governance & Information Risk Assurance (GIRA) and audit activities proposed being vital in demonstrating the added value that the ICO would expect a code of conduct to provide and ensure assurances to the regulator that members of a code are meeting expectations.

We believe that the three year audit programme is balanced and in many cases where organisations are already subject to audit scrutiny, engagement with the three year audit should be easily achieved.

The WASPI Team intend to provide further details as part of continued development of the code of conduct and monitoring

arrangements, detailing what the three year audit for organisations would entail, this is planned to be based around controls and assurances already provided by organisations as part of their annual GIRA. However, this would be developed further if the outcome of the consultation is positive and if there is support for creating WASPI as an approved ICO code of conduct.

One respondent indicated the need for a vision for Wales associated with the Information Governance strategies and frameworks with a concern that the development of WASPI as an approved ICO code of conduct could potentially become the start of many other potential codes covering the wider information governance framework, with this seen as something which could cause a burden on resources for organisations..

One further respondent indicated that they felt that the audit and assurance processes were unnecessary and not constructive.

WASPI Team response:

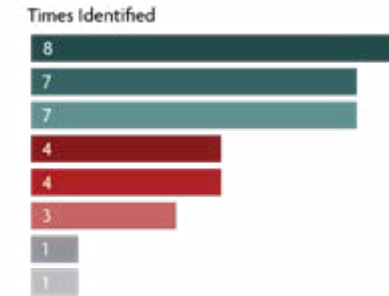
The proposed Code of Conduct with the ICO is specifically designed to align to data sharing responsibilities/accountabilities. Codes of conduct enable a sector to own and resolve key data protection challenges and are not expected to be developed to covering all areas of data protection responsibilities.

WASPI covers all sectors, and the proposed code of conduct is designed to reflect the requirements of different processing sectors and considering specific needs of small and medium size organisations.

We believe that the proposed assurance controls are balanced, proportionate, and required, and will be streamlined and supported through digital solutions to allow organisations who sign up as members to be able to achieve and demonstrate continued compliance, which in turn will provide appropriate assurances to the ICO.



Theme	Times Identified
Strengthen the current framework	8
Support of monitoring and structure of accountability	7
Provides greater reassurance to citizens	7
ICO recognition will enhance status of WASPI	4
Supportive of code of conduct intention	4
Provide greater consistency between partners	3
Concern the code does not cover all of GDPR	1
Resource should be used to support other IG ideas	1



Question 7: Do you agree with the proposal to create WASPI as an approved ICO code of conduct? Please explain your reasoning.

This question of the consultation asked respondents for their views on whether they agreed with the proposal to create WASPI as an approved ICO code of conduct and to provide some comments in support of their answer.

There was an overwhelming response supporting the proposals, and a common set of themes provided further explaining why support was being provided.

Many respondents comments reflected themes that the development of WASPI as an approved code of conduct by the UK regulatory for data protection would strengthen the already effective framework in place supporting organisations across Wales. The introduction of structure and monitoring to the framework for organisations signed up as code members offers greater reassurances to the public that data sharing activities were not only in place, but regularly reviewed to ensure, appropriateness and proportionality was continually maintained, and opportunities for review of information sharing practices mandated.

Several responses also commenting on the code allowing those organisations to displaying the WASPI Code of Conduct member badge, demonstrating that they met the standards of the code of conduct. By displaying the badge, this would increase public confidence and visibility that an organisation with who they may hold personal data upholds the highest levels of data sharing standards, recognised and supported by the Information Commissioner’s Office.

Some suggestions were made by respondents that a programme of training and educational awareness would be beneficial to support organisations with their obligations both under the existing WASPI framework and the introduction of the potential code of conduct.

One respondent raised concern that the proposed code did not cover compliance against the whole of the UK GDPR requirements, with another respondent indicating that resources should be considered to support other elements of information governance compliance as opposed to developing the existing WASPI framework as an approved ICO code.

WASPI Team response:

It is encouraging to see an overwhelming response indicating support to develop WASPI as an approved ICO Code of Conduct, ICO Codes of Conduct should be specifically designed to align to areas of data protection responsibilities/accountabilities and are not designed to cover compliance with the whole of the UK GDPR.

The responses to the consultation are consistent with our views that enhancing the existing WASPI framework into a formal ICO Code would be a naturally progression and enhance the existing framework which is embedded across Wales, building upon the successes to date and providing additional assurances for organisations and citizens.

If a successful application is submitted to the ICO, the WASPI Team will consider digital solutions and training support which would be made available to support organisations with meeting the obligations set out within the Code.

Conclusion/ Next Steps

Following the consultation, Digital Health and Care Wales intends to make some slight modifications to the proposed code of conduct to reflect comments provided from respondents to the consultation.

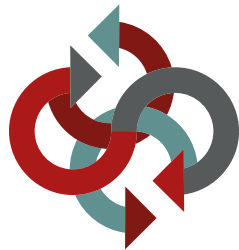
These changes will reflect:

- adding additional confidence around the establishment of the Monitoring Body arrangements and how these would be compliant article 4(1) of the UK GDPR,
- clarification on complaint handling procedures and the role of the Monitoring Body as well as the role of the Information Commissioner's Office in respect of the complaint handling,
- clarification on the requirements and timeframes for returning annual Governance and Information Risk Assurance (GIRA) assessments,
- updating the requirements for review of Information Sharing Protocols (ISPs) from a requirement of review every two years to three years, and
- adding clarification on the scope of Information Sharing Agreements which would be subject to the annual Governance and Information Risk Assurance processes.

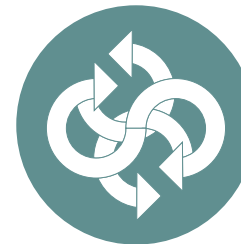
These changes will be made and reflected within an updated WASPI code of conduct which will be submitted for consideration to the Information Commissioner's Office as part of their formal application and decision-making process.

In addition to this application, Digital Health and Care Wales will begin to finalise evidence to support a further application to the Information Commissioner's Office in respect of the proposed monitoring body to maintain and support the proposed code of conduct.

Further updates on the WASPI framework and the development of the WASPI code of conduct will be provided through the WASPI website: www.waspi.gov.wales



Cytundeb Rhannu Gwybodaeth
Bersonol Cymru
Wales Accord on the
Sharing of Personal Information



AELOD COD YMDYGIAD
CODE OF CONDUCT MEMBER

Cytundeb Rhannu Gwybodaeth
Bersonol Cymru
Wales Accord on the
Sharing of Personal Information