# Data Protection Impact Assessment (DPIA)

This DPIA is provided by **Instruxo Limited** regarding the information governance relating to CQC Ready – a quality assurance platform designed to help General Practices.

See **cqc-ready.org**

Please note **CQC Ready** is not a clinical system and no patient identifiable information should be added as per the terms and conditions.

It does not integrate with other systems.

## Table of contents

# Data Protection Impact Assessment (DPIA)

## SECTION 1 – Screening questions

**1. Do you need to do a DPIA?**

| **1.a) Provide an overview of the initiative, programme, project or process, and describe what is being planned.** |
|---|
| CQC Ready is an online platform designed to help General Practices with quality assurance. It is not a clinical system. Practices are able to have a licence and as part of this give logins to key staff members.<br><br>CQC Ready enables<br><br>● coordinated team working,<br>● translates every day practice functions into CQC regulatory categories,<br>● provides a self-assessment,<br>● facilitates prioritisation,<br>● provides an indicative overall rating,<br>● task management and alignment of evidence<br><br>Practice documents relating to evidence can be uploaded and viewed by<br><br>● Staff who have logins<br>● Following provision by the practice of an access link: The CQC<br>● Following authorisation / consent by the practice: Other CQC Ready users who are<br> ○ in the practice PCN<br> ○ in other practices |
| **1.b) Provide a summary of how data will be used and shared.** |
| Personal data is in the form of staff name + email<br><br>It is used for staff to log on to the platform securely and for colleagues form the same practice to coordinate on the platform<br><br>Practices can upload evidence. This relates to their own narrative and documentation.<br><br>Practices can consent to share their evidence with other practices within their PCN or across the CQC Ready platform to facilitate collaboration. This is optional. The default is not to share with other licence holders.<br><br>No patient identifiable data should be placed on the platform<br><br>Staff details are not shared with anyone apart from the other users registered by the superuser responsible for that practice. |

Put an ☒ next to all that apply.

| | Type of data | |
|---|---|---|
| ☒ | Personal data | Individuals can be identified directly. |
| ☐ | Personal data | Individuals can be identified indirectly |
| ☐ | Special Categories - sensitive personal data | This could be about patients, staff, the general public, etc. |
| ☐ | Pseudonymised data | Someone for this initiative, programme, project or process, holds the 'key' and can re-identify individuals. |
| | Pseudonymised data | The 'key' to re-identify individuals is not accessible to the those managing this initiative, programme, project or process. |
| ☐ | Anonymous data | Not identifiable data, for example trends or statistics. |

**1.c) Description of the data**

**Staff name + email**
This is only available to the users from the same General Practice and CQC Ready support team to help with user support.

**Practice evidence**

As per practice submission

This may be in narrative form, a link to evidence elsewhere or a document that demonstrates that evidence.

# SECTION 2 – Why do you need the data?

**2. What are the purposes for using or sharing the data?**

Personal data is used for access and authentication.

Sharing evidence, protocols and proformas can help other practices save time by not having to generate these from scratch.

Practices that are struggling can also see how well performing practices function and can learn from their evidence.

As stated above, evidence that is shared is only via consent by the practice

The CQC will, by invite, be able to view restricted content – ie evidence aligned to quality statements but not staff details, tasks or self-assessments.

This can enable a more streamlined and effective presentation of evidence, reducing stress at inspection and enabling the CQC to find evidence quickly. This in turn is likely to enable a more positive CQC inspection.

**3. What are the benefits of using or sharing the data?**

See above

# SECTION 3 – What data do you want to use or share?

**4. Can you use anonymous data for your purposes? If not, explain why.**

Staff emails cannot be anonymous to the system or they cannot log on

Put an ☒ next to the one that applies.

| | |
|---|---|
| ☐ | Yes |
| ☒ | No |
| ☐ | Unsure |

**5. Which types of personal data do you need to use and why?**

Put an ☒ next to all that apply.

| | | | | | |
|---|---|---|---|---|---|
| ☒ | Forename | ☐ | Physical description, for example height | ☐ | Photograph / picture of people |
| ☒ | Surname | ☐ | Phone number | ☐ ☒ ☐ | Location data e.g.<br>● IP address<br>● Other |

| | | | | | |
|---|---|---|---|---|---|
| ☐ | Address | ☒ | Email address | ☐ | Audio recordings |
| ☐ | Postcode full | ☐ | GP details | ☐ | Video recordings |
| ☐ | Postcode partial | ☐ | Legal representative name (personal representative) | ☐ | Other |
| ☐ | Date of birth | ☐ | NHS number | ☐ | None |
| ☐ | Age | ☐ | National insurance number | | |
| ☐ | Gender | ☐ | Another numerical identifier | | |

| **State below why you need this personal data and embed a description of the dataset if available.** |
|---|
| So users are able to log on to the platform and be identifiable to one another on the platform. This is essential to enable teamwork. <br><br> So the platform can respond to users who forget their login details. <br><br> IPs are collected for security and performance analysis. |

6. **Data protection laws mean that some data is considered particularly sensitive. This is called special category data. Data that relates to criminal offences is also considered particularly sensitive. Which types of sensitive data do you need to use or share?**

    Put an ☒ next to all that apply and provide a reason why the data is needed.

| Type of data | | Reason why this is needed (leave blank if not applicable) |
|---|---|---|
| ☐ | Information relating to an individual's physical or mental health or condition, for example information from health and care records | |
| ☐ | Biometric information in order to uniquely identify an individual, for example facial recognition | |
| ☐ | Genetic data, for example details about a DNA sample taken as part of a genetic clinical service | |

| | | |
|---|---|---|
| ☐ | Information relating to an individual's sexual life or sexual orientation | |
| ☐ | Racial or ethnic origin | |
| ☐ | Political opinions | |
| ☐ | Religious or philosophical beliefs | |
| ☐ | Trade union membership | |
| ☐ | Information relating to criminal or suspected criminal offences | |
| ☐ | None of the above | |

| |
|---|
| **Embed a description of the dataset if available, unless special category data is covered in your embedded description in response to question 5** |
| Not applicable |

## 7. Who are the individuals that can be identified from the data?

Put an ☒ next to all that apply.

| | |
|---|---|
| ☐ | Patients or service users |
| ☐ | Carers |
| ☒ | Staff |
| ☐ | Wider workforce |
| ☐ | Visitors |
| ☐ | Members of the public |
| ☐ | Other |

## 8. Where will your data come from?

The submission by staff relating to that practice.

If a staff member is registered on the platform, other staff members in that organisation will be able to see their colleagues name and email.

The platform is empty of data apart from the primary registrants name and email when initially purchased.

All evidence is submitted by the practice as such they consent to upload the evidence.

9. **Will you be linking any data together?**

Put an ⊠ next to the one that applies.

| | |
|---|---|
| ☐ | Yes |
| ⊠ | No |
| ☐ | Unsure |

   a. **Will it become possible, as a result of linking data, to be able to identify individuals who were not already identifiable from the original dataset?**

   Put an ⊠ next to the one that applies.

| | |
|---|---|
| ☐ | Yes |
| ⊠ | No |
| ☐ | Unsure |

# SECTION 4 – Where will data flow?

10. **Describe the flows of data.**

| Data flow name | Going from | Going to | Data description |
|---|---|---|---|
| Collaborative evidence | Practice (A) that has consented to share their evidence on CQC Ready with respective other practice | Practice (B) who has paid for a premium subscription to view collaborative evidence can view on CQC Ready | Collaborative evidence e.g. protocol, policy etc |

11. **Confirm that your organisation's Information Asset Register (IAR), Record of Processing Activities (ROPA) or your combined information assets and flows register (IAFR) has been updated with the flows described above.**

Put an ⊠ next to the one that applies.

| | |
|---|---|
| ☒ | Yes |
| ☐ | No |
| ☐ | Unsure |

**12. Will any data be shared outside of the UK?**

Put an ☒ next to the one that applies.

| | |
|---|---|
| ☐ | Yes |
| ☒ | No The data centre is located in the UK |
| ☐ | Unsure |

> **a. If yes, give details, including any safeguards or measures put in place to protect the data whilst outside of the UK.**

## SECTION 5 – Is the intended use of the data lawful?

**13. Under Article 6 of the UK General Data Protection Regulation (UK GDPR) what is your lawful basis for processing personal data?**

| | |
|---|---|
| ☒ | (a) **We have consent** |
| ☒ | (b) **We have a contractual obligation** |
| ☐ | (c) **We have a legal obligation** |
| ☐ | (e) **We need it to perform a public task** |
| ☐ | (f) **We have a legitimate interest** |
| ☐ | **Other** |

**14. If you have indicated in question 6 that you are using special category data, what is your lawful basis under Article 9 of the UK GDPR?**

Not applicable
Put an ☒ next to the one that applies.

| | |
|---|---|
| ☐ | (b) **We need it to comply with our legal obligations for employment** |
| ☐ | (f) **We need it for legal claims, to seek legal advice or judicial acts** |

| | |
|---|---|
| ☐ | **(g) We need to comply with our legal obligations to provide information where there is a substantial public interest, as set out in this list** |
| ☐ | **(h) We need it to comply with our legal obligations to provide or manage health or social care services** |
| ☐ | **(i) We need it to comply with our legal obligations for public health** |
| ☐ | **(j) We need it for archiving, research and statistics where this is in the public interest** |
| ☐ | **Other** |
| ☒ | **Not applicable** [the use of special category data is not proposed] |

15. **What is your legal basis for using and sharing this health and care data under the common law duty of confidentiality?**

Put an ☒ next to the one that applies.

| | |
|---|---|
| ☐ | **Implied consent** [for individual care or local clinical or care audits. Skip to question 16] |
| ☐ | **Explicit consent** [a very clear and specific statement of consent. Go to question 15a] |
| ☐ | **Section 251 support** [this means you have support from the Secretary of State for Health and Care or the HRA following an application to the Confidentiality Advisory Group (CAG) CAG must be satisfied that it isn't possible or practical to seek consent. Go to question 15a] |
| ☐ | **Legal requirement** [this includes where NHS England has directed an organisation to share the data using its legal powers. State the legal requirement in the further information section. Go to question 15a] |
| ☐ | **Overriding public interest** [for example to prevent or detect a serious crime or to prevent serious harm to another person. The justification to disclose must be balanced against the public interest in maintaining public confidence in health and care services. Routine use of this is extremely rare in health and care, as it usually applies to individual cases where decisions are made to share data. Go to question 15a] |
| ☒ | **Not applicable** [you are not using identifiable health and care data. Skip to question 16] |

| **15 a) Please provide further information or evidence.** |
|---|
| CQC Ready is not a clinical platform engaged in processing personal clinical data or a data platform engaged in managing patient data. |

# SECTION 6 – How are you keeping the data secure?

**16. Are you collecting information?**

Put an ☒ next to the one that applies.

| | |
|---|---|
| ☒ | Yes [go to question 16a] |
| ☐ | No [skip to question 17] |
| | |

| **16 a) How is the data being collected?** |
|---|
| Input of users |

**17. Are you storing information?**

Put an ☒ next to the one that applies.

| | |
|---|---|
| ☒ | Yes [go to question 17a] |
| ☐ | No [skip to question 18] |

**a. How will information be stored?**

Put an ☒ next to all that apply and provide details.

| Storage location | | Details |
|---|---|---|
| ☐ | Physical storage, for example filing cabinets, archive rooms, etc. | |
| ☐ | Local organisation servers | |
| ☒ | Cloud storage | Tier 3 Data Centre in the UK |
| ☐ | Other | |

**18. Are you transferring information?**

Put an ☒ next to the one that applies.

| | |
|---|---|
| ☐ | Yes [go to question 18a] |
| ☒ | No [skip to question 19] |

| **18 a) How will information be transferred?** |
|---|
| |

**19. How will you ensure that information is safe and secure?**

Put an ☒ next to all that apply and provide details.

| | Security measure | Details (leave blank if not applicable) |
|---|---|---|
| ☒ | Encryption | All data is encrypted at rest and in transit. |
| ☒ | Password protection | Both user and administrative access is password protected. |
| ☒ | Role based access controls (RBAC) | All users are given specific roles and permission to data is granted only as required. |
| ☒ | Restricted physical access | The site is stored from a Tier 3 datacentre with restricted physical access. |
| ☒ | Business continuity plans | Backups and recovery plans are in place to ensure continuity. |
| ☐ | Security policies | |
| ☐ | Other | |

**20. How will you ensure the information will not be used for any other purposes beyond those set out in <u>question 2</u>?**

Specify the measures below which will be used to limit the purposes the data is used for.

Put an ☒ next to all that apply and provide details.

| | Security measure | Details (leave blank if not applicable) |
|---|---|---|
| ☒ | Contract | Terms and Conditions on subscription |
| ☐ | Data processing agreement | |
| ☐ | Data sharing agreement | |
| ☐ | Data sharing and processing agreement (DSPA) | |
| ☒ | Audit | |
| ☒ | Staff training | |
| ☒ | Other | Privacy Policy |

# SECTION 7 – How long are you keeping the data and what will happen to it after that time?

**21. How long are you planning to use the data for?**

We hold the data on behalf of the client while they have a licence and for 6 months after in case of need for file access and / or change in decision. After then it will be deleted

We process the data on behalf of the client

**22. How long do you intend to keep the data?**

Depends on the duration of a licence – see above

**23. What will happen to the data at the end of this period?**

After 6 months it will be deleted

Put an ☒ next to all that apply and provide details.

| Action | | Details (leave blank if not applicable) |
|---|---|---|
| ☐ | Secure destruction (for example by shredding paper records or wiping hard drives with evidence of a certificate of destruction) | |
| ☐ | Permanent preservation by transferring the data to a Place of Deposit run by the National Archives | |
| ☐ | Transfer to another organisation | |
| ☐ | Extension to retention period | |
| ☐ | It will be anonymised and kept | |
| ☐ | The controller(s) will manage as it is held by them | |
| ☒ | Other | After 6 months of cancelling the licence, the data will be deleted |

# SECTION 8 – How are people's rights and choices being met?

**24. How will you comply with the following individual rights (where they apply)?**

| Individual right | How you will comply (or state *not applicable* if the right does not apply) | |
|---|---|---|
| **The right to be informed**<br>The right to be informed about the collection and use of personal data. | We have assessed how we should inform individuals about the use of data for CQC Ready<br><br>Put an ☒ next to all that apply. | |
| | ☒ | Privacy notice(s) for all relevant organisations<br><br>https://cqc-ready.org/privacy-statement |
| | ☐ | Information leaflets |
| | ☐ | Posters |
| | ☐ | Letters |
| | ☒ | Emails |
| | ☐ | Texts |
| | ☐ | Social media campaign |
| | ☒ | DPIA published (best practice rather than requirement) |
| | ☐ | Other [please state] |
| | ☐ | Not applicable |
| **The right of access**<br>The right to access details of data use and receive a copy of their personal information - this is commonly referred to as a subject access request. | Licence users have full access to their data that they have submitted | |
| **The right to rectification**<br>The right to have inaccurate personal data rectified or completed if it is incomplete. | Licence users have full access to edit / rectify their data that they have submitted | |
| **The right to erasure** | | |

| The right to have personal data erased, if applicable. | Licence users have full access to delete their data that they have submitted |
|---|---|
| **The right to restrict processing**<br>The right to limit how their data is used, if applicable. | Licence users sign up to enabling CQC Ready to process their evidence. This is part of the product. As such restricting processing would mean not gaining from the product.<br><br>CQC Ready will never share personal details (name + email) with anyone. |
| **The right to data portability**<br>The right to obtain and re-use their personal data, if applicable. | Not applicable – personal data is not portable from this platform |
| **The right to object**<br>The right to object to the use and sharing of personal data, if applicable. | Sharing of personal data is not applicable as it is not shared. |

25. **Will the national data opt-out need to be applied?**

No this is not applicable

Put an ☒ next to the one that applies.

| ☐ | Yes |
|---|---|
| ☒ | No – CQC Ready is not a clinical system processing patient information. This is not applicable |
| ☐ | Unsure |

26. **Will any decisions be made in a purely automated way without any human involvement (automated decision making)?**

Put an ☒ next to the one that applies.

| ☐ | Yes [go to question 26a] |
|---|---|
| ☒ | No [skip to question 27] |
| ☐ | Unsure [add as a risk in section 10 with an action to find out] |

| **26 a) Where the effect of the automated decision on the individual is substantial, how will you uphold an individual's right not to be subjected to a decision solely made by automated means)?** |
|---|
| |

**26 b) Are you using any special category data as part of automated decision making?**

| | |
|---|---|
| ☐ | Yes |
| ☐ | No |

27. **Detail any stakeholder consultation that has taken place (if applicable).**

   CQC Ready has been developed by GPs in close engagement with GPs. Local practices were engaged and provided free licences

# SECTION 9 – Which organisations are involved?

28. **List the organisation(s) that will decide why and how the data is being used and shared (controllers).**

   Instruxo Limited (owner of CQC Ready) + Licensee (respective General Practice who hold the licence)

29. **List the organisation(s) that are being instructed to use or share the data (processors).**

   General Practices who sign up to use the platform may consent to sharing their own data. No one is instructed or required to share anything

30. **List any organisations that have been subcontracted by your processor to handle data**

   FreelyGive Limited - This is the Informatics arm of Instruxo Limited

31. **Explain the relationship between the organisations set out in <u>questions 28</u>, <u>29</u> and <u>30</u> and what activities they do**

   - The General Practice is the customer
   - Instruxo Limited is the supplier
   - FreelyGive Limited part owns Instruxo Limited and provides Informatics Support

32. **What due diligence measures and checks have or are being carried out on any processors used?**

   Put an ☒ next to all that apply .
   Where multiple processors are used, indicate which option applies to which processor.

| Due diligence measures | | Details (leave blank if not applicable) |
|---|---|---|
| ☐ | **Data Security and Protection Toolkit (DSPT) compliance** | |

| | | |
|---|---|---|
| ☒ | **Registered with the Information Commissioner's Office (ICO)** | |
| ☐ | **Digital Technology Assessment Criteria (DTAC) assessment** | |
| ☒ | **Stated accreditations** | ISO 27001 in progress |
| ☐ | **Cyber Essentials or any other cyber security certification** | |
| ☐ | **Other checks** | |

## SECTION 10 – What data protections are there and what mitigations will you put in place?

33. **Complete the <u>risk assessment table</u>. Use the <u>risk scoring table</u> to decide on the risk score.**

**Risk assessment table**

| Risk ref no. | Description | Risk score* (L x I) | Mitigations | Risk score* with mitigations applied |
|---|---|---|---|---|
| 01 | There is a problem at the datacentre which could lead to a loss of service or data or both. This could be caused by power failure, connectivity problems or cyber attack. | 3*2=6 | Freelygive provides hosting services using professional datacentres which are appropriately certified and with whom they have a successful track record. Such datacentres will have power back up options and will look to avoid single point of failure connectivity. The datacentre will have a level of cyber attack protection. Freelygive provides a maintenance service which keeps the core software of the CQC-Ready System, Drupal, up to date with Security patches to avoid cyber attacks. Back-ups of both code and data are stored in different | 2*1=2 |

| | | | datacentres and the system could be moved to a different data centre in the highly unlikely event of a long term datacentre outage.  The CQC-Ready system is neither short-term mission critical nor highly volatile.  Therefore some outage or temporary loss of data is unlikely to harm practices unduly. | |
|---|---|---|---|---|
| 02 | Theft of data through hacking | 3*2=6 | Freelygive provides a maintenance service which keeps the core software of the CQC-Ready System, Drupal, up to date with security patches to avoid hacking.  Back-ups of both code and data are stored in different datacentres. The CQC-Ready system does not store sensitive personal data, so the theft of data is unlikely to damage practices, especially as the data is backed up. | 2*1=2 |
| 03 | Blocking of access through hacking | 2*2=4 | Mitigation for this risk is outlined in risks 01 and 02 | 2*1=2 |
| 04 | Cyber attack / fire / natural disaster on an individual practice | 2*2=4 | Access to the CQC-Ready system is via the internet and is not dependent on any other practice systems.  While such events may be critical for the practice involved, it would not be through loss of service or data on the CQC-Ready system | 2*2=4 |
| 05 | Periodic updates of software introduce bugs, which could corrupt data, limit access to the system or stop the system from working properly | 3*2=6 | Apart from the mitigations already mentioned FreelyGive adopt a proven development process to minimise the number of such bugs that are introduced through software development.  In addition Instruxo has adopted a culture of thorough testing which further reduces the | 2*1=2 |

| | | likelihood of significant disruption to the use of the system | |
|---|---|---|---|
| | | | |

**\*Risk scoring table**

| | | Impact (I) | | | | |
|---|---|---|---|---|---|---|
| | | Negligible (1) | Low (2) | Moderate (3) | Significant (4) | Catastrophic (5) |
| **Likelihood (L)** | Rare (1) | 1 | 2 | 3 | 4 | 5 |
| | Unlikely (2) | 2 | 4 | 6 | 8 | 10 |
| | Possible (3) | 3 | 6 | 9 | 12 | 15 |
| | Likely (4) | 4 | 8 | 12 | 16 | 20 |
| | Almost certain (5) | 5 | 10 | 15 | 20 | 25 |

**CQC Ready**
**Instruxo Limited**