KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

Version Control

Version	Date	Notes	Author
V1 – v3.1	June 2020	Initial Draft	Emma Cooper, Kafico Ltd
V3.2	July 2020	Added to Risk Mitigations and identified Customer Responsible elements Amended Data Quality in relation to use of patient demographics	Emma Cooper. Kafico Ltd

1. Project Context

Tekihealth Solutions Ltd LTD (TSL) has designed a telemedicine service that can directly help customer organisations support provision of care to patients remotely.

The service is unique since it not only connects GPs in surgery or at home (if they chose to work remotely) to patients in care homes or at home but also enables the GP to conduct a full clinical assessment through the use of tele-diagnostic equipment provided to the care home. This equipment allows the doctor to examine the chest (through a digital stethoscope), look into the patient's ears and throat and examine the skin for rashes and moles (through the use of camera). The doctor can communicate directly with the patient and care home staff via a video conferencing platform.

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

Abbreviations and Definitions

HCO: *Healthcare Organisation.* This is the customer that has purchased the product to provide telehealth services to their patient population.

RHCP: *Remote Health or Care Professional.* This is the individual who is present with the patient and taking the physical readings with the Tekihealth devices. It could be a HCA from the practice that is undertaking home visits or it could be a care home staff member as nominated by the HPO.

RC: *Remote Clinician*. This is the clinician who is logging in to the software remotely and reviewing readings obtained by the RHCP.

TSL: *Tekihealth Solutions Ltd*. Designers and facilitators of the telehealth service which employs the physical scopes and devices provided by Tytocare as well as servers that are hosted by Tytocare as a sub processor. TSL will provide user management services and management of issued devices.

Tytocare: Providers of the physical products and devices and scopes and providers of hosted storage for the data collected.

The process and data flows are identified below.

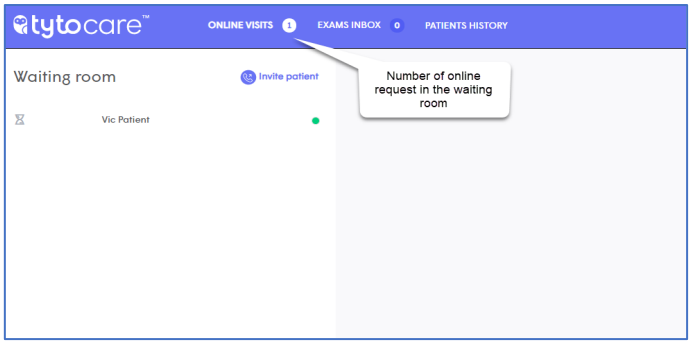
Onboarding

1. The Tekihealth iPad is provided and the HCO will log as an information asset within the organisation
2. The Tekihealth iPad comes with Tytocare App downloaded

3. Tekihealth will provide a single practice RHCP user profile for the Tytocare App on the iPad
4. Tekihealth will provide a single practice RC user profile for the Tyto Web App
5. The HCO will determine that a patient would benefit from a telehealth consultation
6. The parties make arrangements to be available at a particular time and both log into the software. For example;

    If the GP plans to undertake regular weekly ward rounds, they can agree a day and time slot beforehand when they will be logged in to see patients. Alternatively, the home can request an urgent assessment of a patient. They will first contact the GP surgery via telephone. The GP will then triage the patient as per GMC guidelines and decide if a virtual consultation is needed or appropriate. If they deem that it is appropriate for a virtual consultation, they will agree a suitable time to see the patient online.

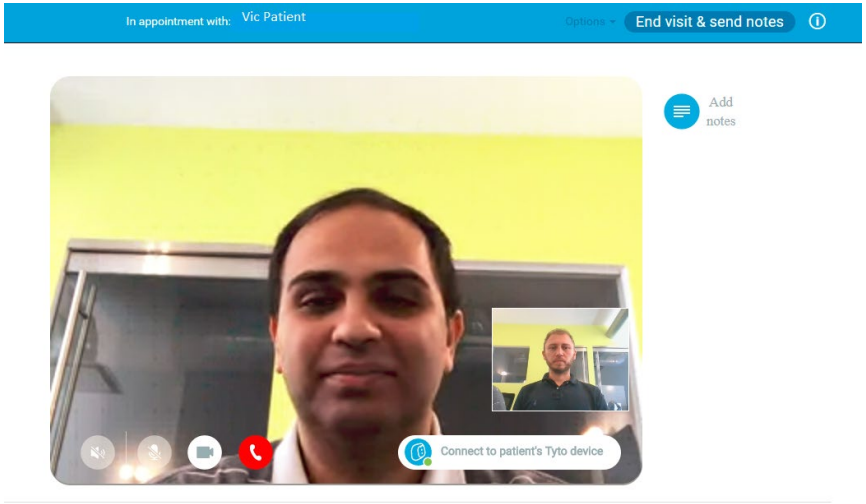
7. The care home / RHCP will then be visible in the waiting room as pictured below under the RHCP / care home name and this can be combined with a patient NHS Number in order to identify the patient in attendance. It can also be set up so that no patient demographics are entered into the system and the patient is identified according to the professional user or care home account; for example, Victoria Care Home might be visible in the waiting room as below;



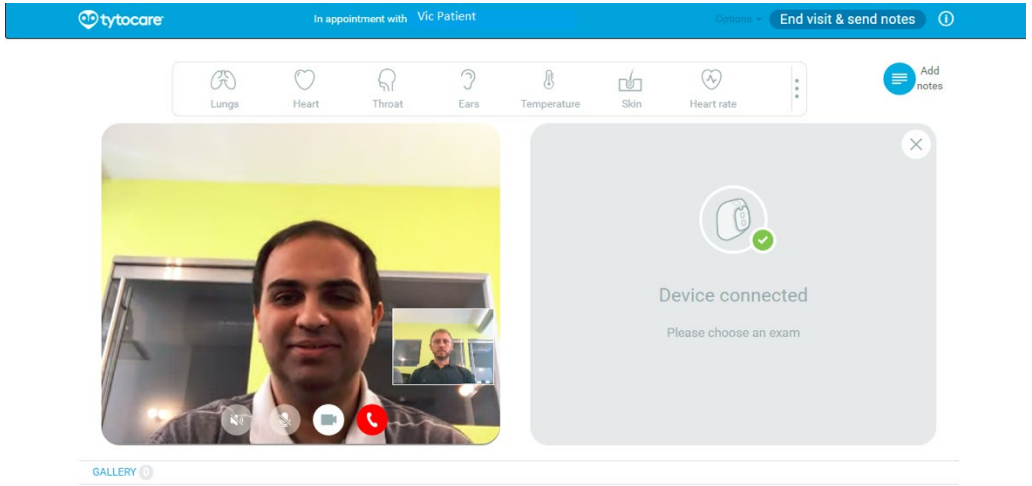
8. Having validated that they are accessing the session that has been agreed in advance with the RHCP, the RC will click ‘start the online visit’
9. This will then open up the telehealth consultation and the clinician will see the video being streamed from the RHCP iPad. This will likely show the RHCP in the first instance and the RHCP will make the introduction to each patient as the appointment progresses.

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY



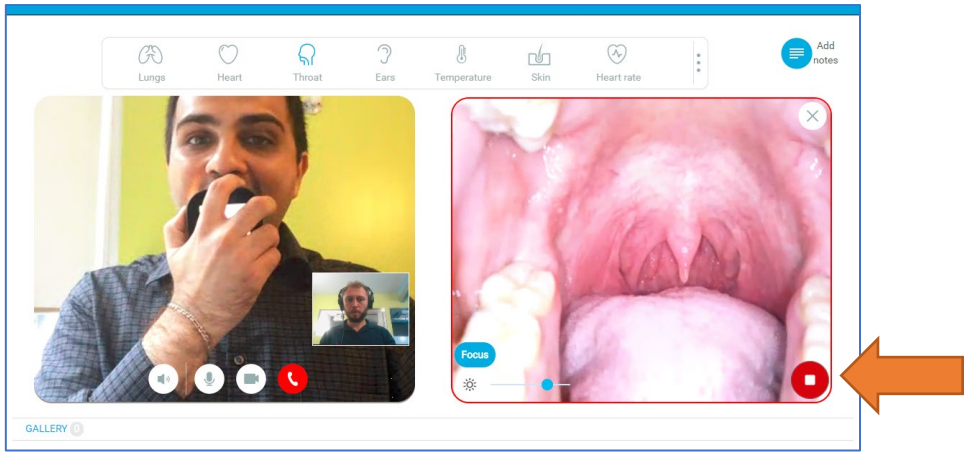
10. The streaming video of the patient and RHCP itself does not come with an option to record
11. The RC can then click on ‘Connect to patient’s Tyto device’
12. This will provide a menu of the various devices and allow the RC to direct the activities of the RHCP in terms of which readings are required using the available devices as below.



13. Each time a device is used, the RC can select to record the readings from that device. For example, recording the video from the device exploring the throat as below.

KAFICO®

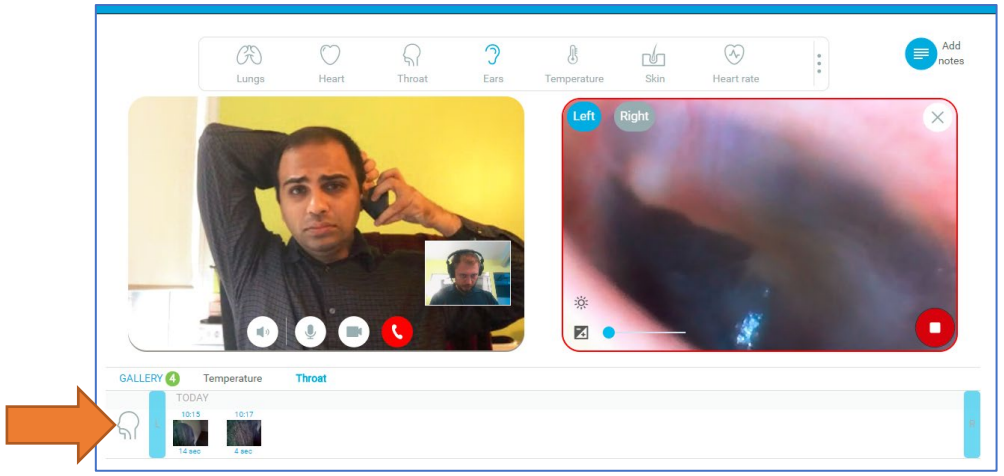
INFORMATION · GOVERNANCE · CONSULTANCY



14. Each time a device is used, and a recording created, they will appear as a thumbnail in the gallery at the bottom of the RC screen as below.

KAFICO®

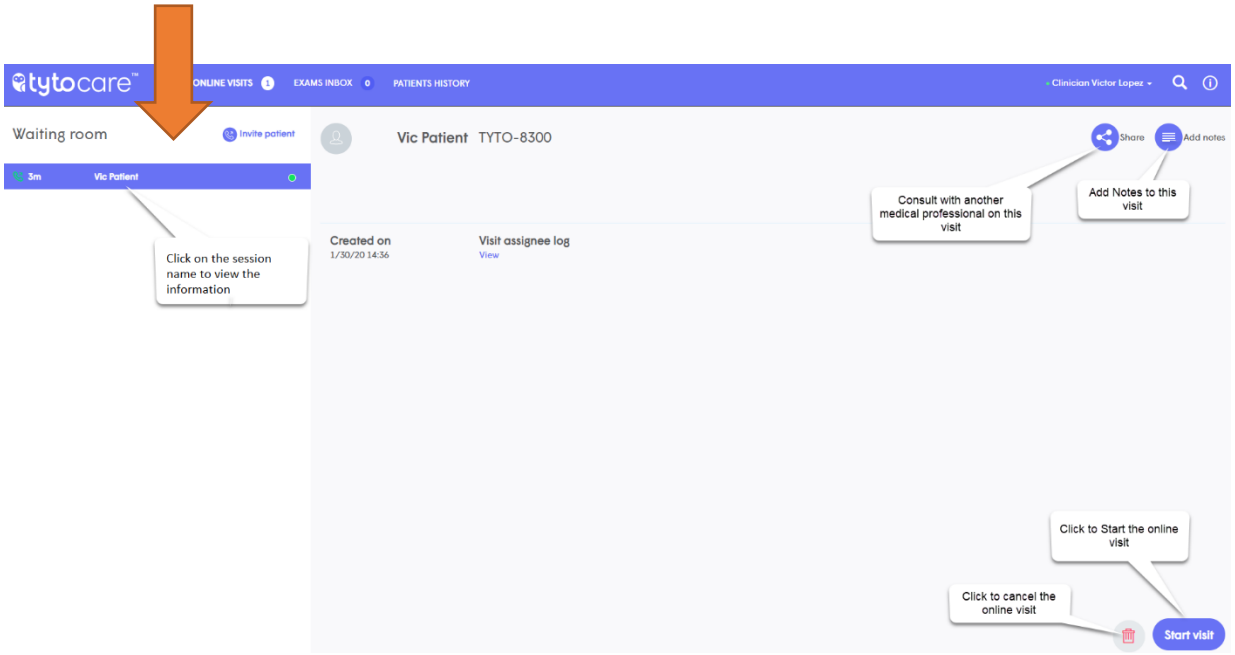
INFORMATION · GOVERNANCE · CONSULTANCY



15. Depending on the nature of the examination, the media being collected will differ. For example, a heart exam will record the sounds of the heart and a throat examination will record the visual of the throat.
16. At the end of the telehealth visit, the RC clicks ‘end visit and send notes’ and the recordings from the session will appear in the Exams Inbox within the Web App interface as below.

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY



17. Clicking the Exams Inbox allows the RC to retrieve previous recordings through the Web App
18. The exams are listed by the name of the RCHP and the date of the session is provided. This allows the RC to link the recordings with the entry into the clinical system appointment book.

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

Tekihealth customers should be aware that this DPIA relates to the software application provided to deliver the remote consultation service. Where other branded devices are provided as part of the bundle, no assurances are provided by Tekihealth around the data protection compliance of these devices and customers are advised to undertake due diligence before logging in to any non Tekihealth app or service.

2. Controllers and Processors

The aim of this section is to identify the data protection responsibilities for the project and identify any gaps or risks therein.

Sources

Data Protection Act 2018 (DPA)

General Data Protection Regulations (EU) 2016/679 (GDPR)

Information Commissioner – Guide to the General Data Protection Regulations (ICO Guide)

ICO Guidance - Data Controllers

European Data Protection Board (EDPB) Opinion 00264/10/En Wp 169 (WP29O)

Integrated Digital Care Records: Data Controller Issues - IGA

GDPR Lawful Processing - IGA

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

Definitions / Context

- ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
- ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
- Controller responsibility lies with a professional service provider because it determines what information to obtain and process in order to do the work and because it is answerable itself for the content.
- Controller should exercise control over the content, manner and purpose for collection of personal data
- The Controller will define the information to be collected and will often exercise professional judgement
- Controller will have the ability to give effect to the rights of individuals
- Any party which makes use of data for its own purposes will be a data controller for those purposes.
- “Where the same personal data is processed by a series of parties in sequence, each using the data for a different purpose then they will remain separate controllers but where they have an element of common purpose they will be joint controllers.” 1
- "for a single processing operation, a number of parties may jointly determine the purposes and means of processing to be carried out" and therefore the parties would be "jointly" acting as controllers; where the determination is exercised by acting together.
- It is strongly recommended that each shared record community should establish an Information Governance Steering Group to establish effective IG arrangements for the shared record.

1 European Data Protection Board (EDPB) Opinion 00264/10/En Wp 169 (WP29O)

- Where there is plurality of control, each controller may be accountable, and therefore liable for the processing at different stages and to differing degrees.

The Controller in this instance remains the healthcare provider since that party retains control over the purpose and manner of processing throughout.

Whilst Tekihealth / Tytocare provide the software and make autonomous decisions about its development and design, they are not able to collect personal data autonomously and shall not be processing personal data for any reason other than to provide services to the Controller customer and satisfy their own legal obligations.

This then makes Tekihealth a Data Processor and so they must be engaged, by the Controller customer via a legally enforceable Data Processing Contract that is compliant with Article 28.

All customers must sign the Tekihealth Data Processing Contract at the point of engagement with the service.

Tekihealth uses Tytocare as a software, hardware and hosted storage provider. Tytocare are contractually bound to process data only as described below;

1. Once collected Tytocare will transmit and store the readings from the scopes (which are not directly identified to particular patients) in AWS EU hosted servers (Ireland) and make available to Tekihealth customers and end users

2. The transferred and stored data shall be accessed for support and maintenance purposes; in order to ensure continued provision of services and to resolve any complaints or technical issues
3. The transferred and stored data shall be accessed, upon the request of Tekihealth, to support the information rights of the data subject
4. Tytocare are determined to be a Sub Processor and are engaged through the Tytocare Data Processing Contract.

3. Lawful Processing

The aim of this section is to explore the purposes for processing personal data and to ensure that each has a specific legal basis.

Sources

Data Protection Act 2018 (DPA)

General Data Protection Regulations (EU) 2016/679 (GDPR)

Information Commissioner – Guide to the General Data Protection Regulations (ICO Guide)

The Health and Social Care (Safety and Quality) Act 2015: Duty to share information (HSCA)

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

Definitions / Context

- You must have a valid lawful basis in order to process personal data.
- There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.
- Most lawful bases require that processing is 'necessary'. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.
- You must determine your lawful basis before you begin processing, and you should document it.
- Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.
- If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).
- If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

As a Processor, Tekihealth are not in a position to determine the purpose and means of processing. However, for the purposes of supporting customers and ensuring that Tekihealth are acting within the law, the potential legal gateways will be explored.

The intended purpose for the use of software and hardware by Tekihealth customers is for delivery of healthcare. It is therefore anticipated that the product will be used by providers that have a legitimate relationship with the patient (data subject) to deliver direct care or play a role in the wider purpose of healthcare management.

It is concluded then, that customers collecting and processing data using the Tekihealth projects will be doing so because the;

Art 6 (1) (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

And

Art 9,(2)(h) processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of employee**, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.**…

Appendix B provides a checklist for the Tekihealth Data Processing Contract clauses against GDPR Article 28 and DPA 2018 s 59 to demonstrate its compliance.

4. Data Minimisation

The aim of this section is to explore whether the project aligns with the data protection principle of data minimisation.

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

Sources

Viewing the GDPR Through a De-Identification Lens:

Looking to comply with GDPR? Here's a primer on anonymization and pseudonymization

Data Protection Act 2018 (DPA)

General Data Protection Regulations (EU) 2016/679 (GDPR)

Information Commissioner – Guide to the General Data Protection Regulations (ICO Guide)

Definitions / Context

- Processing of personal data must be adequate – sufficient to properly fulfil your stated purpose
- Processing of personal data must be relevant – has a rational link to that purpose
- Processing of personal data must be limited to what is necessary – you do not hold more than you need for that purpose
- You should periodically review your processing to check that the personal data you hold is still relevant and adequate for your purposes
- You must **not** collect personal data on the off-chance that it might be useful in the future. However, you **may** be able to hold information for a foreseeable event that may never occur if you can justify it
- Article 6(4)(e) permits the processing of pseudonymized data for uses beyond the purpose for which the data was originally collected.
- Recital 78 and Article 25 list pseudonymization as a method to show GDPR compliance with requirements such as Privacy by Design

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

- Recital 26, the GDPR limits the ability of a data handler to benefit from pseudonymized data if re-identification techniques are "reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly."
- GDPR identifies four types of data;

(1) Identified (subject is immediately identified)

(2) Identifiable (subject could be identified through indirect identifiers such as NHS No)

(3) Article 11 De-Identified (identity is not apparent from the data; data is not directly linked with data that identifies the person. Could potentially be re-identified if matched to additional identifying data. No known, systematic way for the controller to reliably create or re-create a link with identifying data)

(4) Anonymous / Aggregated. Likely identification is "less than remote".

The use of the Tekihealth products and services results in the collection of the following data sets;

- Verbal exchange of relevant patient data between the RC and RHCP / Patient
- Audio / visual recordings or verbal exchange of patient explorations including;
    - ✓ Digital Stethoscope readings
    - ✓ Digital thermometer readings
    - ✓ Blood Pressure readings (verbal exchange via video)
    - ✓ Oxygen Saturation readings (verbal exchange via video)
    - ✓ Spirometer reading (emailed via NHS Mail)
    - ✓ ECG readings (emailed via NHS Mail)

These data appear to be the minimum necessary to facilitate a telehealth consultation. Customers can choose that no patient demographics are entered into the software and the session is identified through;

- A corresponding entry into the clinical system appointment book
- Contemporaneous notes made by the RC and the session times
- Record of the RCHP entry in the Exams section of the software.

The Processing Contract in place with Tytocare contractually binds them to undertake any activities that are unrelated to the provision of this service using anonymised data sets only.

Where it is possible for the particular service at hand, Tekihealth shall use only generic professional logins and dummy patient names to reduce the need for collection of patient data. –

5. Fair and Transparent

The aim of this section is to explore the transparency and fairness of the processing in relation to the Tekihealth products.

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

Sources

Data Protection Act 2018 (DPA)

General Data Protection Regulations (EU) 2016/679 (GDPR)

Information Commissioner – Guide to the General Data Protection Regulations (ICO Guide)

ARTICLE 29 DATA PROTECTION WORKING PARTY - Guidelines on Transparency

ICO Consent Guidance

Murray v Express Newspapers [2008] EWCA Civ 446

COCO V A N CLARK (ENGINEERS) LTD: CHD 1968

Definitions / Context

- You must be clear, open and honest with people from the start about how you will use their personal data.
- fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them.
- if anyone is deceived or misled when the personal data is obtained, then this is unlikely to be fair.
- Transparency is, in some cases even more important even when you have no direct relationship with the individual and collect their personal data from another source. In these cases, individuals may have no idea that you are collecting and using their personal data, and this affects their ability to assert their rights over their data. This is sometimes known as ‘invisible processing’

- WP29 and ICO guidance stipulate the content of Fair Processing / Transparency materials including all third countries to which the data will be transferred, the relevant legal basis, the source of personal data, the existence of automated decision-making including profiling, the categories of personal data concerned, the different storage periods, contact details for the data protection officer, the actual (named) recipients of the personal data, how to exercise information rights including objection, any further processing,

Consent is not the recommended lawful basis for processing of healthcare data and the legal gateway under data protection law is likely to be "public task" and "medical purposes", however, there is a still a legal requirement to ensure that the patient population are informed about the processing and have the opportunity to ask questions or to object to processing. Additionally, there is a need to ensure that the common law duty of confidentiality is also satisfied.

Traditionally, the test arising from Coco v. AN Clarke Engineering Ltd (Coco)2 applied. This provides that a duty of confidentiality arises where information has a quality of confidence, and a relationship of confidence exists.

Whether or not the obligation arises from a confidential relationship; case law development is such that, disclosure by a person that 'receives information he knows or ought to know is fairly and reasonably to be regarded as confidential', may result in a legal wrong.

2 [1968] EWHC 415 (CH).

Therefore, the test for a breach of confidence has developed (in correlation with the application of the Human Rights Act 1998 and Article 8 (1) of ECHR) and now concerns whether individuals have a reasonable expectation of privacy3 such that sharing information may constitute misuse of private information.

The duty can therefore be overridden where it is deemed that the individual *reasonably expects* such a disclosure.

It is therefore presumed that fair processing / transparency materials will be put in place by Controllers to make the patient population are aware of Tekihealth and their Sub Processor and to ensure that the "reasonable expectations" of the population align with that of the project.

Since Tekihealth has no direct relationship with the data subject, it is the Customer Controller's responsibility to engage with patient population to seek their views on the use of remote consultations in this way and the related processing of personal data.

6. Retention of Records

The aim of this section is to identify any records created as a result of the Tekihealth products and to ensure that they are retained in accordance with the law.

3 Murray v Express Newspapers [2008] EWCA Civ 446.

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

Sources

Data Protection Act 2018 (DPA)

General Data Protection Regulations (EU) 2016/679 (GDPR)

Information Commissioner – Guide to the General Data Protection Regulations (ICO Guide)

BMA Retention of Health Records

Definitions / Context

- You must not keep personal data for longer than you need it.
- You need to think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data.
- You need a policy, setting standard retention periods wherever possible, to comply with documentation requirements.
- You should also periodically review the data you hold, and erase or anonymise it when you no longer need it.
- You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.
- You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.
- Electronic patient records (EPRs) must not be destroyed, or deleted, for the foreseeable future.

The records created by the use of Tekihealth products are;

- Login details for RC into Web App
- Verbal exchange of relevant patient data between the RC and RHCP / Patient
- Audio / visual recordings or verbal exchange of patient explorations including;

- ✓ Digital Stethoscope readings
- ✓ Digital thermometer readings
- ✓ Blood Pressure readings (verbal exchange via video)
- ✓ Oxygen Saturation readings (verbal exchange via video)
- ✓ Spirometer reading (emailed via NHS Mail)
- ✓ ECG readings (emailed via NHS Mail)

Device information for the Tekihealth devices such as the tablet (IP address etc) have been determined not to fall under personal data since they can be used by various individuals in a professional capacity as opposed to allowing the identification of a single registered user.

The retention periods for each of the above records has been provided in the grid below.

Records Created as Part of Project	Location	Retention Period	Source	Retaining Responsible Party
Log in Details for RC users	Tytocare Software Platform	Term of the Processing Contract. Once contract is terminated, the Controller Customer login details will be removed from the platform by Tekihealth.	Tekihealth Data Processing Contract	Tekihealth
Verbal exchange of relevant patient data between the RC and RHCP / Patient	Exchanged using the iPad streaming video to RC Web App	Streaming video of conversation is not recorded	NA	NA

Audio / visual recordings or verbal exchange of patient explorations	Tytocare Software Platform	Once contract is terminated, any readings will be removed from the platform and hosted storage by Tekihealth. Whilst the contract is active, recordings are retained on the platform and hosted storage for 7 years.	Tekihealth Data Processing Contract	Tekihealth
Notes made by clinician during remote consultation	Entered into relevant clinical system	Consumed into Health Record / clinical notes and retained accordingly	NHS RM Code of Practice	Controller Customer

7. Information Rights

The aim of this section is to identify any information rights that apply to the personal data processed and to ensure that the Tekihealth products support Controller Customers in giving effect to these rights.

Sources

Data Protection Act 2018 (DPA)

General Data Protection Regulations (EU) 2016/679 (GDPR)

Information Commissioner – Guide to the General Data Protection Regulations (ICO Guide)

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

Definitions / Context

- The GDPR provides the following rights for individuals: The right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, rights in relation to automated decision making and profiling.

Tekihealth are contractually bound to supporting Customer Controllers with their information rights requests by virtue of s 2.5.7 of the Tekihealth Data Processing Contract.

This means that they will work to support the customer towards a timely and complete response to any request made by patients.

The grid below demonstrates which information rights apply to the identified lawful basis and how a response might be completed.

Information Right	**Applies?**	**How Supported**
Right to Access	Yes, patients do have a right to request then the lawful basis is Public Task and Medical Purposes.	The HCO has the ability to retrieve recordings from previous sessions and to share them with third parties. Tekihealth may query the server to retrieve particular records relating either to a patient (where demographics have been entered) or for a particular session (where dates and times have been provided) and so a request for copy information may be satisfied.

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

Rectification and Restriction	Yes, patients do have a right to request the rectification and restriction of their personal data when the lawful basis is Public Task and Medical Purposes.	The HCO has the ability to retrieve recordings from previous sessions and to share them with third parties to demonstrate accuracy of the recorded information. Tekihealth may query the server to retrieve particular records relating either to a patient (where demographics have been entered) or for a particular session (where dates and times have been provided) and so a request for accurate information may be satisfied.
Portability	The right to data portability only applies when your lawful basis for processing this information is consent or for the performance of a contract and so would not apply to processing under this DPIA.	NA
Erasure	The right to Erasure does not apply when processing is for Public Task and Medical Purposes and so would not apply to processing under this DPIA.	NA

Profiling and Automated Decision Making	There is no profiling or automated decision-making taking place and so these rights would not apply to processing under this DPIA.	NA
Object	Yes, the right to object applies to processing under Public Talk and Medical purposes. It is good practice that if you are relying upon the public task lawful basis and receive an objection, you should consider the objection on its own merits	Tekihealth may query the server to retrieve particular records relating either to a patient (where demographics have been entered) or for a particular session (where dates and times have been provided) and so a request to remove personal data may be satisfied. Some objections may be handled during the session, for example, where the patient did not want their data collected by virtue of the remote consultation software and hardware. Since Tekihealth are not present, these objections are out of scope for this assessment and should be managed by Controller Customer on a case by case basis.
Withdraw Consent	No, the right to withdraw consent is not available to patients where the lawful basis is Public Task and Medical Purposes.	NA

Right to be Informed	Yes, the right to be informed does apply when the lawful basis is Public Task and Medical Purposes.	Tekihealth will provide Controller Customers with information about the data flows and Sub Processors such that they are able to inform patients at the point of appointment booking as well as at the start of the consultation.

8. Accuracy and Data Quality

The aim of this section is to identify the areas where accuracy and data quality must be assured and the measures in place to achieve this.

Sources

Data Protection Act 2018 (DPA)

General Data Protection Regulations (EU) 2016/679 (GDPR)

Information Commissioner – Guide to the General Data Protection Regulations (ICO Guide)

Definitions / Context

- Controllers must carefully consider any challenges to the accuracy of information
- Controllers must consider whether it is necessary to periodically update the information
- Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted
- if you are using the data to make decisions that may significantly affect the individual concerned or others, you need to put more effort into ensuring accuracy.

There are considered to be two main areas for consideration in terms of accuracy of accuracy and quality of personal data with respect to the processing under this DPIA;

1. Ensuring that the data collected during the remote session is matched to the correct patient by the clinician accessing the software portal and making notes in the clinical system
2. Ensuring that the data being produced by the hardware devices and transmitted to the software is accurate

Ultimately, it is anticipated that the recording functionality will be seldom used. When used, perhaps to obtain a 2nd opinion from a colleague around readings obtained, it is assumed that this can be done in an anonymous manner (it is not necessary for the reviewing clinician to know the identity of the patient concerned to offer such an opinion).

It is therefore concluded that, since there will be very low volumes of recordings created, the potential use of an identifier to maintain proper linkage to a patient is outweighed by the minimisation principle and the reduction of personal data flowing to Processor and Sub Processor. The product will therefore be offered as standard without any identifiers against recordings.

The customer can choose to have the software configured so that NHS Number is required when the RHCP is accessing the software for the session. This allows the RC to validate the patient identity and for the recordings to be attached to an identifiable session however, this is a customer decision based on risk appetite since it possibly conflicts with the data minimisation principle.

Where the customer opts for no patient demographics to be entered, the audit trail relies on the RC of the Controller Customer to validate the identity of the patient in collaboration with the RHCP who is attending the appointment. The clinician must use the necessary process to conclude that the health record they are amending is the corresponding health record for the patient being seen in remote consultation.

The absence of patient demographics entered into the software supports the minimisation principle of data protection but it must be balanced with the data quality principle such that there should be defined methods to ensure that recordings can be linked with a patient and that the information collected during a session is recorded against the correct patient.

Where NHS Number is not opted for inclusion, it is anticipated that this will be managed in the following way;

- ✓ A corresponding entry into the clinical system appointment book. Any Exams within the software will align with appointments recorded within the local clinical system

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

- ✓ Contemporaneous notes made by the RC. The RC is expected to make contemporaneous notes of the session within the local clinical system
- ✓ The Exams section of the software shows previous sessions, identified by date and the RHCP name is visible against each
- ✓ The RC can also make notes within the Exams session itself

With regards to the second item, the following measures are in place;

- Tytocare devices provided by Tekihealth are using are fully calibrated during the manufacturing process.
- As with all cameras and microphones (Tyto Otoscope, Exam Camera, and Stethoscope) there is no need to calibrate these products proactively.
- If a problem occurs during the usage of one of the Tytocare components, Tekihealth have direct access to the Tytocare IT team to resolve any issues
- The blood pressure machines are made by OMRON. These are commonly used by primary and secondary care teams in the NHS. The blood pressure machines require calibration every 12 months. OMRON will provide this service.
- As GP's are familiar with these devices, they are able to provide advice and guidance directly to the care home staff if they receive an incorrect reading.

- The fingertip pulse oximeter is the Oxywatch portable non-invasive oximeter by ChoiceMMed. Pulse oximeters do not require a zero calibration because the design incorporates continuous automatic zero calibration. Gain calibration is also not required because the measurement technique does not require gain accuracy.
- The MIR turbine flow meter used in the Bluetooth spirometer are individually factory calibrated with a computerised system. The Ideal Sensor does not require calibration.
- In the event that there are concerns or incidents relating to data accuracy, Tekihealth are contractually bound by virtue of s 2.5.7 of the Tekihealth Data Processing Contract to take appropriate measures to address any data protection breach.

9. Technical and Organisational Measures to Protect Personal Data

The aim of this section is to ascertain whether Tekihealth have employed technical and organisational measures such that the personal data is protected from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access

Sources

Data Protection Act 2018 (DPA)

General Data Protection Regulations (EU) 2016/679 (GDPR)

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

Information Commissioner – Guide to the General Data Protection Regulations (ICO Guide)

- Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
- While information security is sometimes considered as cybersecurity (the protection of your networks and information systems from attack), it also covers other things like physical and organisational security measures
- Measures taken should consider available technology, costs, nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons
- The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk
- The impact of non-secure data processing can be as serious as becoming a victim or fraud or being put at risk of physical harm or intimidation
- Additionally, individuals are entitled to be protected from less serious kinds of harm like embarrassment or inconvenience
- the data should be accessed, altered, disclosed or deleted only by those you have authorised to do so (and that those people only act within the scope of the authority you give them);
- the data you hold is accurate and complete in relation to why you are processing it; and
- the data should remain accessible and usable, i.e., if personal data is accidentally lost, altered or destroyed, you should be able to recover it and therefore prevent any damage or distress to the individuals concerned.

Inherent Risk	Low	Medium	High

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

Sensitivity of the information at risk (highly personal / stigmatised information)			
Number of data subjects who may be affected should the data be disclosed			
The potential impact on rights and freedoms if confidentiality was compromised			
The potential impact on rights and freedoms if data was unavailable			
The potential impact on rights and freedoms if data was of poor integrity			
Based on the corporate appetite, estimate the potential reputational damage			
Based on the type of data, estimate the financial cost of a breach			

The Tekihealth products process data that is inherently high risk by its sensitive nature. From Tekihealth's prospective, the volume of data they process, as a data processor, is not considered to be high. GP practices inherently process large amounts of personal data and would therefore be classed as 'large scale' processing. Although the process involves just one patient per session, a practice will offer this solution to all their patients residing in care homes.

This assessment will explore each of the elements drawn out within the GDPR for mitigation of those risks.

Encryption of Personal Data in Transit

During the session, recordings are made of the readings obtained from the various devices. These are identified by the RHCP user profile and session time and stored within the Tytocare App allowing retrieval at a later date.

The ability for the recordings to be retrieved at a later date requires the data sets to be transmitted from the Tytocare App to the Tytocare hosted storage servers in AWS EU hosted servers (Ireland).

Tekihealth uses Tytocare devices and software application. Tytocare have confirmed that data being transmitted via the devices and software application are encrypted to TLS V1.2 https://www.tytocare.com/faq/).

Encryption of Personal Data at Rest

During the session, recordings are made of the readings obtained from the various devices. These are identified by the RHCP user profile and session time and stored within the Tytocare App allowing retrieval at a later date.

This requires the data sets described above to be transmitted from the Tytocare App to the Tytocare hosted storage servers in AWS EU hosted servers (Ireland).

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

AWS (Amazon Web Services) S3 server-side encryption uses one of the strongest block ciphers available to encrypt data, 256-bit Advanced Encryption Standard (AES-256). AWS has certification for compliance with ISO/IEC 27001:2013, 27017:2015, 27018:2019, and ISO/IEC 9001:2015. AWS offer a data processing contract that complies with GDPR Article 28 and narrowly defines how data can be processed by Amazon.

The data is backed up to the same specification in AWS EU hosted servers (Frankfurt).

Access Control

Tytocare hold administrative permissions to Tekihealth which allows them to set up user profiles for their HCO customers.

Tekihealth will allocate a certain number of user generic clinician profiles per customer and these logins can be used to access the software portal by the RC and the Tytocare software accessed by the RHCP iPad.

Due to the high usage of locums amongst the customer base, practices are issued generic practice log ins. The 'live' nature of the access (both the patient and the RHCP are able to see the RC and vice versa and the requirement to make contemporaneous notes, supports an audit trail of the telehealth visit including who was in attendance. However, it is the customer responsibility to ensure that any generic log ins issued are issued and managed in a way that supports an audit trail of sessions attended.

Controller Customers are able to access a record of when the software was accessed and when remote consultations took place (via the History tab within the Web App).

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

In accordance with the Identity Verification and Authentication Standard for Digital Health and Care Services Version 2.0 - Specification and Implementation issued by NHS Digital, the verification of the patient themselves is carried out by the health and care providers.

The RHPC will complete Face to Face vouching and relay to the RC the confirmed identity of the patient. This will allow the RC to access the correct health record in the clinical system and make accurate and contemporaneous records of the consultation.

Similarly, the provision of the RHPC with the iPad should be logged as with any removeable information asset / device. This forms an audit trail who is accessing this device during that particular timeframe. When the information asset is returned and re-issued, a log would be kept such that it provides an audit trail of access during that timeframe.

Tekihealth and Tytocare will only access the hosted personal data in very limited circumstances and audit trails would be available against the particular user profiles granted at each organisation. Both parties are contractually bound to confidentiality. in line with GDPR Article 28, they are be engaged by virtue of a Data Processing Contract that restricts the use of any personal data for activities outside of those defined as necessary for the service delivery.

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

10. Risk Identification

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
There is a risk that Tekihealth do not put in place an appropriate article 28 contract to legitimise the processing of customer personal data. This could result in either the Controller or Processors being unaware of the limitations or obligations placed on processing of personal data. Ultimately, this could result in a fine being issued to the Controller Customer or Tekihealth as a result of data protection non-compliance.	**Moderate**	**Moderate**	**Moderate**
There is a risk that the contract with Tytocare does not place the same obligations of compliance as the Controller has placed on Tekihealth. This could result in either Tekihealth making commitments to the Controller Customer that it cannot fulfil by virtue of the processing by Tytocare. Ultimately, this could result in a fine being issued to the Controller Customer or Tekihealth as a result of data protection non-compliance.	**Moderate**	**Moderate**	**Moderate**
There is a risk that the Controller's obligations towards transparency are compromised due to a lack of clarity in the supply chain. This could result in not giving effect to the patient's Right to Be Informed and subsequently their Right to Object. Ultimately, this could result in a fine being issued to the Controller Customer or Tekihealth as a result of data protection non-compliance.	**Moderate**	**Moderate**	**Moderate**

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

There is a risk that Tekihealth are retaining data for longer than necessary by virtue of their Sub Processor (Tytocare) collecting and storing data beyond the completion of the remote consultation session. This could result in patient data being transferred overseas without adequate protection and infringement of data subjects rights. Ultimately, this could result in a fine being issued to the Controller Customer or Tekihealth as a result of data protection non-compliance.	**High**	**Moderate**	**Moderate**
There is a risk that the information collected as part of a remote consultation is entered into the incorrect patient record, in particular as the NHS number will not be used as the primary identifier for the process This may result in inaccurate or incomplete information within a person's health record and could consequently result in an impact to their care and health.	**High**	**High**	**High**
There is a risk that the devices will not provide accurate information in relation to readings taken during a remote consultation. This may result in inaccurate or incomplete information within a person's health record and could consequently result in an impact to their care and health.	**High**	**High**	**High**
There is a risk that data in transit is not appropriately encrypted such that interception might result in an unauthorised disclosure and information breach. This may result in patient data being accessed by authorised personal or made public causing damage and distress. This would result in reputational damage and a potential monetary fine from the authority.	**High**	**High**	**High**

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

There is a risk that the software will be accessed inappropriately by Controller customer staff using the generic log ins. This may result in patient data being accessed by authorised personal or made public causing damage and distress. This would result in reputational damage and a potential monetary fine from the authority.	**High**	**High**	**High**
There is a risk that data flow from Frankfurt to the UK may not occur if appropriate safeguards are not in place. Data flow will be required for business continuity and disaster recovery purposes.	**High**	**High**	**High**

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

11. Risk Mitigation

Identify additional measures taken to reduce or eliminate risks identified as medium or high risk in section above				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
There is a risk that Tekihealth do not put in place an appropriate article 28 contract to legitimise the processing of customer personal data.	Draft an Article 28 compliant contract and supply to customers during the onboarding process. Compliance with contract must be proactively audited each year.	Eliminated	Low	Approved by Stephen Katebe
There is a risk that the contract with Tytocare does not place the same obligations of compliance as the Controller has placed on Tekihealth.	An Art 28 contract is in place with Tytocare – restricting in particular: their autonomous use of the data and international transfers	Eliminated	Low	Approved by Stephen Katebe

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

There is a risk that the Controller's obligations towards transparency are compromised due to a lack of clarity in the supply chain.	Tekihealth have obtained confirmation about the use of data by Tytocare – in particular that there will be no autonomous of use of personal data or international transfers without adequate safeguards in accordance with GDPR.	Eliminated	**Low**	Approved by Stephen Katebe
There is a risk that the Controller's obligations towards transparency are compromised due to a lack of clarity in the supply chain.	Tekihealth has provided materials (by way of the DPIA) to support the development a privacy policy by customers. The DPIA identifies the sub processors involved in the project.	Eliminated	Low	Approved by Stephen Katebe
There is a risk that Tekihealth are retaining data for longer than necessary by virtue of their Sub Processor (Tytocare) collecting and storing data beyond the completion of the remote consultation session.	Tekihealth have obtained information about the use of data by Tytocare – in particular that there will be no autonomous of use of personal data or international transfers without	Eliminated	Low	Approved by Stephen Katebe

	adequate safeguards in accordance with GDPR.			
There is a risk that the information collected as part of a remote consultation is entered into the incorrect patient record.	Tekihealth will include guidance for HPO around patient identity validation and contemporaneous note making as part of onboarding materials. Standard Operating Procedure (SOP) has been developed to ensure staff using the solution follow a clear process in relation to documenting contemporaneous records within the correct patient record.	Reduced	Low	
There is a risk that the devices will not provide accurate information in relation to readings taken during a remote consultation.	Ensure that Tekihealth are aware of the calibration requirements for all devices	Reduced	Low	

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

There is a risk that data in transit is not appropriately encrypted such that interception might result in an unauthorised disclosure and information breach.	Tekihealth have confirmed the level of encryption provided by Tytocare and confirmed that it aligns with best practice in terms of its suitability for the nature and volume of information transmitted (Client Side AWS)	Reduced	Low	Approved by Stephen Katebe
There is a risk that data flow from Frankfurt to the UK may not occur if appropriate safeguards are not in place. Data flow will be required for business continuity and disaster recovery purposes.	GDPR compliant agreement/contracts will need to be in place for any information stored outside of the UK.	Reduced	Low	Approved by Stephen Katebe
There is a risk that the software will be accessed inappropriately by Controller customer staff using the generic log ins.	It is the responsibility of the Controller customer to ensure that the generic log ins are issued to the appropriate staff members and audited appropriately. This should be made clear in the onboarding materials.	Customer Responsibility	Customer Responsibility	Approved by Stephen Katebe

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

There is a risk that the combination of generic log ins and no patient demographics results in an opaque audit trail such that it becomes more difficult to ascertain who was present at each session	Customer is required to make an assessment of risk based on their own risk appetite as to whether patient demographics are added. This assessment puts priority on the minimisation principle since recording will be used in exceptional circumstances that generally do not require identification.	Customer Responsibility	Customer Responsibility	Approved by Stephen Katebe
There is a risk that inappropriate access and system misuse is undetected or identified when using generic logins and without having a robust audit trail in place.	Practice/regulated care provider to implement a robust audit trail to determine users provided with a generic log in to perform consultations. A sign-in/out audit log must be maintained in order to track individual user access. A SOP to be developed to ensure the customer-controller follows and implements an adequate audit process. All users must be up to date with their mandatory IG training.	Customer Responsibility	Low	Approved by Stephen Katebe

There is a risk that the devices become lost or stolen and, consequently, accessed by unauthorised individuals if not appropriately handled and secured.	SOP to be developed for customer-controller and care home to ensure appropriate safe havens and information governance guidelines are adhered to prevent unacceptable use, to secure any confidential information stored on the devices and to prevent unauthorised access to the Tekihealth app. All users must be up to date with their mandatory IG training.	Customer Responsibility	Low	Approved by Stephen Katebe

12. Sign Off

Item		**Name / Position / Date**	**Notes**
Measures approved by:		Stephen Katebe, Tekihealth Solutions Ltd, August 2020	
Residual risks approved by:		Emma Cooper, Kafico Ltd, July 2020	
Data Protection Advice provided:		Emma Cooper, Kafico Ltd, April 2020	Advised that mitigations around onboarding materials and signing of sub processor

			contract are in place prior to processing of personal data.
Data Protection Advice accepted or overruled:			
If residual risks are high, DPIA must be reviewed by ICO			
Periodic DPIA review dates:		Emma Cooper, Kafico Ltd, July 2020	October 2020 Review Due

13. Appendix A - Is this a Suitable DPIA?

Different organisations will use different templates and structures for their Data Protection Impact Assessments (DPIA). This assessment serves to confirm that the approach taken by Tekihealth meets the necessary thresholds. The ICO advises that DPIAs must meet the criterion identified by the EDPB as identified below;

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

Criteria	Status	Location
A systematic description of the processing is provided	Present	Link to data flow map provided
Nature, scope, context and purposes of the processing are taken into account	Present	Link to data flow map provided Context provided in Section 1
Personal data, recipients and period for which the personal data will be stored are recorded	Present	Section 1 (Controllers and Processors), Section 4 (Data Minimisation) and Section 6 (Retention of Records)
a functional description of the processing operation is provided	Present	Section 1 (Project Context)
the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified	Present	Throughout
compliance with approved codes of conduct is taken into account	Present	Section 6 (Records of Processing)
necessity and proportionality are assessed	Present	Section 4 (Data Minimisation)
measures envisaged to comply with the Regulation are determined	Present	Section 11 (Risk Mitigation)
Lawfulness of processing is assessed	Present	Section 3 (Lawful Processing)
Rights of data subjects are assessed	Present	Section 7 (Information Rights)

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

Transparency is assessed	Present	Section 5 (Fairness and Transparency)
Relationship with processors is assessed	Present	Section 2 (Controllers and Processors)
International transfers are assessed	Present	Section 10 (Risk Identification)
The need for prior consultation is assessed	Present	Section 12 (Sign Off)
Risks to the rights and freedoms of data subjects are identified and managed	Present	Section 10 (Risk Identification) and Section 11 (Risk Mitigation)
Origin, nature and severity of risks are appreciated	Present	Section 10 (Risk Identification)
Risks are assessed and measures envisaged to treat risks are determined	Present	Section 10 (Risk Identification) and Section 11 (Risk Mitigation)
Interested parties are involved	Present	Section 12 (Sign off)
The Advice of the DPO is sought	NA	DPO not required for Tekihealth due to volume of information processed
The views of data subjects or their representatives are sought	Present	Section 5 (Fairness and Transparency)

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

1. Appendix B - Is the Tekihealth Data Processing Contract Compliant with Article 28?

Required clause/areas covered by contract	Included y/n/NA	Notes/Comments
Is the processor required to provide, on request evidence that they have implemented appropriate technical and organisational measures to protect Personal Data including storage and transmission of data, business continuity, staff training, auditing, access control and Cyber security?	Yes	2.5.5
Does the contract state that the processor shall not engage another processor without prior specific or general written authorisation of the controller?	Yes	2.4
Does the contract set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller?	Yes	Schedule 1
Does the contract stipulate that the Processor processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by law and in those cases will notify the Controller?	Yes	2.5.1
Does the contract state that all staff employed by the processor have contracts that include confidentiality clauses and that Personal Data will not be shared with third party unless required to do so by law?	Yes	2.5.4

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

Does the contract require the Processor to assist the Controller to respond to requests for exercising the data subject's rights i.e. access to information, correction of errors?	Yes	2.5.7
Does the contract require the Processor to assist the Controller in reporting information incidents promptly including where it might be required to contact the data subject?	Yes	2.5.6
Does the contract state what should happen to the data at the end of the contract or in the event of termination such as return of the data or secure destruction?	Yes	Schedule 2
Does the contract require the Processor to allow for a comply with audits including inspections conducted by the Controller or a third party engaged by the Controller?	Yes	2.6