APPENDIX A – Activity and Rationale List

The Practice will share patient information with these organisations where there is a legal basis to do so.

ACTIVITY	RATIONALE
Commissioning and contractual purposes Invoice Validation **Planning** **Quality and Performance**	**Purpose:** Anonymous data is used by the CCG for planning, performance and commissioning purposes, as directed in the practices contract, to provide services as a public authority. **Legal Basis:** UK GDPR 6 1(b) Contractual obligation as set out in the Health and Social Care Act for Quality and Safety 2015. **Processor:** NHS Brighton & Hove CCG, NHS Sussex CCGs/ICB
Summary Care Record including Additional Information (SCRAI)	**Purpose:** The NHS in England uses a national electronic record called the Summary Care Record (SCR) to support patient care. It contains key information from your GP record. Your SCR provides authorised healthcare staff with faster, secure access to essential information about you in an emergency or when you need unplanned care, where such information would otherwise be unavailable. **Legal Basis:** In order for your Personal Data to be shared or processed, an appropriate 'legal basis' needs to be in place and recorded. The legal bases for direct care via SCR is the same as the legal bases for the care you would receive from your own GP, or another healthcare provider: • for the processing of personal data: Article 6.1 (e) of the UK GDPR: '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'. • for the processing of 'Special Category Data' (which includes your medical information): Article 9.2 (h) of the UK GDPR: 'processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services'. **Legal basis for use of the services after COPI:** The COPI mechanism was used as the simplest and quickest way to communicate the changes to GP Connect and Summary Care Record Additional Information during a time of national crisis. However, the legal basis under which GP Connect and Summary Care Record Additional Information operated pre-pandemic was not affected by COPI and remains in place. The legal basis for both GP Connect and Summary Care Record Additional Information is Article 6(1)(e) and Article 9(2)(h) of the UK GDPR (General Data Protection Regulation). For Common Law Duty of Confidentiality, implied consent with opt out is used. The law on information sharing has not changed since the response to the crisis. Legal basis is driven by parliamentary law, and NHS policy is driven by NHS England, the Department of Health and Social Care, and national stakeholders. **Your rights:** Patients have the right to opt out of having their information shared with the SCR by completion of the form which can be downloaded here and returned to the practice. Please note that by opting out of having your information shared with the Summary Care Record could result in a delay to care that may be required in an emergency. **Processor:** NHS England and NHS Digital
GP Connect (NHS Digital)	**Purpose:** We use a facility called GP Connect to support your direct care. GP Connect makes patient information available to all appropriate clinicians when and where they need it, to support direct patients care, leading to improvements in both care and outcomes. GP Connect is not used for any purpose other than direct care. Authorised Clinicians such as GPs, NHS 111 Clinicians, Care Home Nurses (if you are in a Care Home), Secondary Care Trusts, Social Care Clinicians are able to access the GP records of the patients they are treating via a secure NHS Digital service called GP connect.

	The NHS 111 service (and other services determined locally e.g. Other GP practices in a Primary Care Network) will be able to book appointments for patients at GP practices and other local services. **Legal Basis:** In order for your Personal Data to be shared or processed, an appropriate "legal basis" needs to be in place and recorded. The legal bases for direct care via GP Connect is the same as the legal bases for the care you would receive from your own GP, or another healthcare provider: • for the processing of personal data: Article 6.1 (e) of the UK GDPR: "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". • for the processing of "Special Category Data" (which includes your medical information): Article 9.2 (h) of the UK GDPR: "processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services". **Legal basis for use of the services after COPI:** The COPI mechanism was used as the simplest and quickest way to communicate the changes to GP Connect and Summary Care Record Additional Information during a time of national crisis. However, the legal basis under which GP Connect and Summary Care Record Additional Information operated pre-pandemic was not affected by COPI and remains in place. The legal basis for both GP Connect and Summary Care Record Additional Information is Article 6(1)(e) and Article 9(2)(h) of the UK GDPR (General Data Protection Regulation). For Common Law Duty of Confidentiality, implied consent with opt out is used. The law on information sharing has not changed since the response to the crisis. Legal basis is driven by parliamentary law, and NHS policy is driven by NHS England, the Department of Health and Social Care, and national stakeholders. **Your rights:** Because the legal bases used for your care using GP Connect are the same as used in other direct care situations, the legal rights you have over this data under UK GDPR will also be the same – these are listed elsewhere in our privacy notice. **Processor:** NHS Digital **Further info:** Summary of GP Connect service - NHS Digital GP Connect - NHS Digital GP Connect: GDPR information - NHS Digital GP Connect Transparency Notice - NHS Digital GP Connect privacy notice - NHS Digital
Research	**Purpose:** We may share anonymous patient information with research companies for the purpose of exploring new ways of providing healthcare and treatment for patients with certain conditions. This data will not be used for any other purpose. Where personal confidential data is shared your consent will need to be sought. Where you have opted out of having your identifiable information shared for this Planning or Research your information will not be shared. **Legal Basis:** consent is not required to share anonymous data that does not identify a patient. Where identifiable data is required for research, patient consent will be needed, unless there is a legitimate reason under law to do so or there is support under the Health Service (Control of Patient Information Regulations) 2002 ('section 251 support') applying via the Confidentiality Advisory Group in England and Wales. **Processor:** Primary Care Research Network, National Institute for Health and Care Research (NIHR), Royal College of General Practitioners (RCGP), UK Biobank, ResearchOne
Individual Funding Requests	**Purpose:** We may need to process your personal information where we are required to fund specific treatment for you for a particular condition that is not already covered in our standard NHS contract. The clinical professional who first identifies that you may need the treatment will explain to you the information that is needed to be collected and processed in order to assess your needs and commission your care; they will gain your explicit consent to share this. You have the right to withdraw your consent at any time but this may affect the decision to provide individual funding. **Legal Basis:** Under UK GDPR Article 6 1(a) consent is required and Article 9 2 (h) health data. **Data processor:** NHS Brighton & Hove CCG, NHS Sussex CCGs/ICB

Safeguarding Adults	**Purpose:** We will share personal confidential information with the safeguarding team where there is a need to assess and evaluate any safeguarding concerns. **Legal Basis:** in some case consent will be required otherwise • Article 6(1)(e) '…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…'; and • Article 9(2)(h) 'necessary for the purposes of preventative or occupational medicine **Data Processor:** Adult Social Services, Brighton & Hove City Council
Safeguarding Children	**Purpose:** We will share children's personal information where there is a need to assess and evaluate any safeguarding concerns. **Legal Basis:** in some case consent will be required otherwise • Article 6(1)(e) '…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…'; and • Article 9(2)(h) 'necessary for the purposes of preventative or occupational medicine **Data Processor:** Front Door for Families (FDFF), Brighton & Hove City Council
Risk Stratification – Preventative Care	**Purpose:** 'Risk stratification for case finding' is a process for identifying and managing patients who have or may be at-risk of health conditions (such as diabetes) or who are most likely to need healthcare services (such as people with frailty). Risk stratification tools used in the NHS help determine a person's risk of suffering a particular condition and enable us to focus on preventing ill health before it develops. Information about you is collected from a number of sources including NHS Trusts, GP Federations and your GP Practice. A risk score is then arrived at through an analysis of your de-identified information. This can help us identify and offer you additional services to improve your health. If you do not wish information about you to be included in any risk stratification programmes, please let us know. We can add a code to your records that will stop your information from being used for this purpose. Please be aware that this may limit the ability of healthcare professionals to identify if you have or are at risk of developing certain serious health conditions. Type of Data – Identifiable / Pseudonymised / Anonymised / Aggregate Data. **Legal Basis:** UK GDPR Art. 6(1) (e) and Art.9 (2) (h). The use of identifiable data by CCGs and GPs for risk stratification has been approved by the Secretary of State, through the Confidentiality Advisory Group of the Health Research Authority (approval reference (CAG 7-04)(a)/2013)) and this approval has been extended to the end of September 2022 NHS England Risk Stratification which gives us a statutory legal basis under Section 251 of the NHS Act 2006 to process data for risk stratification purposes which sets aside the duty of confidentiality. We are committed to conducting risk stratification effectively, in ways that are consistent with the laws that protect your confidentiality. **Processors:** Appointed data processor and for subsequent healthcare with the CCG, ICB, PCO, frailty service, etc.
Public Health Screening programmes (identifiable) Notifiable disease information (identifiable) Smoking cessation (anonymous) Sexual health (anonymous)	**Purpose:** Personal identifiable and anonymous data is shared. The NHS provides national screening programmes so that certain diseases can be detected at an early stage. These currently apply to bowel cancer, breast cancer, aortic aneurysms and diabetic retinal screening service. The law allows us to share your contact information with Public Health England so that you can be invited to the relevant screening programme. More information can be found at: https://www.gov.uk/topic/population-screeningprogrammes or speak to the practice **Legal Basis:** Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' and Article 9(2)(h) Health data as stated below. **Data Processors:** Public Health England
Direct Care **NHS Trusts** **Other Care Providers**	**Purpose:** Personal information is shared with other secondary care trusts and providers in order to provide you with direct care services. This could be hospitals or community providers for a range of services, including treatment, operations, physio, and community nursing, ambulance service. **Legal Basis:** The processing of personal data in the delivery of direct care and for providers' administrative purposes in this surgery and in support of direct care elsewhere is supported under the following Article 6 1 (e) direct care and 9 2 (h) to provide health or social care: In some cases, patients may be required to consent to having their record opened by the third party provider before patients information is accessed. Where there is an overriding need to access the GP record in order to provide patients with lifesaving care, their consent will not be required.

	Processors: University Hospitals Sussex NHS Foundation Trust (formerly Brighton and Sussex University Hospitals), Sussex Partnership NHS Foundation Trust (SPFT) and Sussex Community NHS Foundation Trust (SCFT)
Care Quality Commission	**Purpose:** The Care Quality Commission (CQC) is the regulator for the English Health and Social Care services to ensure that safe care is provided. They will inspect and produce reports back to the GP practice on a regular basis. The Law allows the CQC to access identifiable data. More detail on how they ensure compliance with data protection law (including UK GDPR) and their privacy statement is available on our website**:** https://www.cqc.org.uk/about-us/our-policies/privacy-statement **Legal Basis:** Article 6(1)(c) "processing is necessary for compliance with a legal obligation to which the controller is subject." and Article 9(2) (h) as stated below. **Processors:** Care Quality Commission (CQC)
Population Health Management	**Purpose:** Health and care services work together as 'Integrated Care Systems' (ICS) and are sharing data in order to: • Understand the health and care needs of the care system's population, including health inequalities • Provide support to where it will have the most impact • Identify early actions to keep people well, not only focusing on people in direct contact with services but looking to join up care across different partners. NB this links to the Risk Stratification activity identified above. Type of Data: Identifiable /Pseudonymised / Anonymised / Aggregate Data. NB only organisations that provide your care will see your identifiable data. **Legal Basis:** Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' and Article 9(2)(h) as stated below. **Data Processors:** Sussex Health and Care (Integrated Care System), NHS Sussex CCGs/ICB
Payments **Invoice Validation**	**Purpose:** Contract holding GPs in the UK receive payments from their respective governments on a tiered basis. Most of the income is derived from baseline capitation payments made according to the number of patients registered with the practice on quarterly payment days. These amounts paid per patient per quarter varies according to the age, sex and other demographic details for each patient. There are also graduated payments made according to the practice's achievement of certain agreed national quality targets known as the Quality and Outcomes Framework (QOF), for instance the proportion of diabetic patients who have had an annual review. Practices can also receive payments for participating in agreed national or local enhanced services, for instance opening early in the morning or late at night or at the weekends. Practices can also receive payments for certain national initiatives such as immunisation programs and practices may also receive incomes relating to a variety of non-patient related elements such as premises. Finally, there are short term initiatives and projects that practices can take part in. Practices or GPs may also receive income for participating in the education of medical students, junior doctors and GPs themselves as well as research. In order to make patient-based payments basic and relevant necessary data about you needs to be sent to the various payment services. The release of this data is required by English laws. **Legal Basis:** Article 6(1)(c) "processing is necessary for compliance with a legal obligation to which the controller is subject." and Article 9(2)(h) 'as stated below. **Data Processors:** NHS England, NHS Brighton & Hove CCG, NHS Sussex CCGs/ICB, Public Health England
Patient Record Database	**Purpose:** Your medical record will be processed in order that a database can be maintained, this is managed in a secure way and there are robust processes in place to ensure your medical record is kept accurate, and up to date. Your record will follow you as you change surgeries throughout your life. Closed records will be archived by NHS England. **Legal Basis:** Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' and Article 9(2)(h) as stated below. **Processor:** TPP (SystmOne); Primary Care Support England (PCSE)
Medical Reports: Subject Access Requests	**Purpose:** Your medical record may be shared in order that solicitors acting on your behalf can conduct certain actions as instructed by you. Insurance companies seeking a medical report where you have applied for services offered by then can have a copy to your medical history for a specific purpose. **Legal Basis:** Your explicit consent will be required before a GP can share your record for either of these purposes.

	Processor: iGPR
Medical Reports	**Purpose:** Personal confidential information will be shared with the person or their representative at their request. **Legal Basis:** Contractual agreement with the patient and consented. Patients can request to see reports before sharing. **Processors:** Patients and or their representatives – e.g., family members, solicitors, insurance companies.
Medical Reports	**Purpose:** Personal confidential information will be shared with insurance companies, or potential or active employers at the patient's request. **Legal Basis:** Consented by processors. Patients can request to see reports before sharing. **Processors:** Patients and or their representatives – e.g., employers, insurance companies, RAF, Army, Navy.
Statutory Reports: DVLA Reports; DWP Reports	**Purpose:** Personal confidential information will be shared in order to comply with organisations carrying out their statutory duties or from organisations to provide reports by their GP. **Legal Basis:** Contractual requirements with consent gained by processors. Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller'. **Processor:** DVLA, DWP
Medical Records Management: Scan & Collate	**Purpose:** Personal confidential data is shared with Scan & Collate document management services in order to provide an on-site scanning solution where their staff visits the practice on a pre-arranged appointment and process the records they need copying, usually in regards to subject access requests made under the General Data Protection Regulation (GDPR) (EU) 2016/679. Records are produced onto an encrypted CD-Rom ready to supply to the requesting party, e.g., solicitor, insurance company, patient. **Legal Basis:** The legal basis for this activity under UK GDPR is Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' and patient consent. **Processor:** Scan & Collate Ltd
Medicines Optimisation: OptimizeRX	**Purpose:** Your anonymous aggregated information will be shared in order to optimise medication. This will enable your GP to provide a more efficient medication regime for your personal care. Some of the anonymous information may be used nationally to drive wider understanding of the medication is used. **Legal Basis:** Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' and Article 9(2)(h) Health data as stated below. **Processor:** FDB Health
Medicines Management Team	**Purpose:** Your medical record is shared with the medicines management team, in order that your medication can be kept up to date and any changes can be implemented. **Legal Basis:** Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' and Article 9(2)(h) Health data as stated below **Processor:** Medicines Management Team, NHS Brighton & Hove CCG
Medication & Prescribing	**Purpose:** Prescriptions containing personal identifiable and health data will be shared with chemists/pharmacies, in order to provide patients with essential medication or treatment as their health needs dictate. This process is achieved either by face-to-face contact with the patient or electronically. Where patients have specified a nominated pharmacy, they may wish their repeat or acute prescriptions to be ordered and sent directly to the pharmacy making a more efficient process. Arrangements can also be made with the pharmacy to deliver medication. **Legal Basis:** Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' and Article 9(2)(h) Health data as stated below. Patients will be required to nominate a preferred pharmacy. **Processor:** Pharmacy of choice

Prescription Ordering Direct (POD)	**Purpose:** The NHS Prescription Ordering Direct (POD) service is provided on behalf of your GP practice by NHS Sussex CCGs who have launched the service as an alternative way for people to order their prescriptions. The service hopes to reduce prescription waste by helping to ensure you order the medication you need when you need it. When you contact POD telephone number you will be asked by a dedicated and fully trained prescription co-ordinator if you consent to your medical record being accessed to process your prescription request. You can also discuss your medication requirements and can be alerted if a medication review is needed. **Legal Basis:** Your consent will be required to share your record for this purpose. **Processor:** NHS Sussex CCGs/ICB **SERVICE ENDED ON 30th September 2023**
Anticoagulation Monitoring	**Purpose:** Personal confidential data is shared with DAWN Clinical Software in order to provide an anticoagulation clinic to patients who are on anticoagulation medication. This will only affect patients who are within this criterion. **Legal Basis:** The legal basis for this activity under UK GDPR is Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' and Article 9(2)(h) Health data as stated below. **Processor:** DAWN Clinical Software
Community Pharmacy Consultation Service (CPCS)	**Purpose:** The NHS Community Pharmacist Consultation Service (CPCS) was launched in October 2019 by NHS England and NHS Improvement, to progress the integration of community pharmacy into local NHS urgent care services, providing more convenient treatment closer to patients' homes. The GP referral pathway was launched nationally on 1st November 2020 and will continue until further notice. Patients presenting to a GP (either directly or via an online consultation service) with a low acuity or minor illness may be referred for a consultation with a community pharmacist, where they would have otherwise attended a GP appointment or other service (e.g. walk in centre or minor injury unit). This will require information about the patient and their presenting condition to be shared with the community pharmacy by the general practice. An output from the consultation will also be shared back to the GP for upload to the patient's medical record. This direct care service is expected to relieve pressure on primary, urgent and emergency care. Further information can be found in the CPCS pathway summary: https://www.england.nhs.uk/publication/nhs-community-pharmacist-consultation-service-toolkit-for-GP-PCN-staff/ Personal data will be collected directly from the patient by the GP, either through conversation with practice staff or via an online consultation application provided by the practice. This data will be used to verify the patient's identity and summarise the presenting condition. The information collected from the patient will be summarised and shared with the appropriate Community Pharmacist, who will then consult with the patient and provide a summary back to the practice for inclusion in the patient's medical record. The practice will use their clinical medical record recording system to collect and store all personal data relating to patients who use their Primary care services. The Surgery uses SystmOne TPP for their clinical recording system. The practice is responsible for ensuring the security of their records and access controls. The system will use the Pinnacle and Sonar software to enable transfer of data between systems. This has been approved by NHS England. **Legal Basis:** This processing is required to provide direct health care to patients, allowing GPs to discharge their statutory duties in the course of providing a health and care system. Under UK GDPR Article 6 1 (e) The processing is necessary for a task that is within our remit as a public authority; and 9 2(h) The processing is necessary for health or social care purposes will apply. **Processor:** GP Practice; Community Pharmacists; TPP (SystmOne); Sonar and Pinnacle; NHS England
GP Extended Access	**Purpose:** Your medical record will be shared with the Improving Access Service (IAS) in order that they can provide direct care services to the patient population as part of GP extended access clinics. **Legal Basis:** Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' And Article 9(2)(h) Health data as stated below. **Processor:** Here www.hereweare.org.uk

Primary Care Network	**Purpose:** Your medical record will be shared with the Trinity Medical Centre and Charter Medical Centre in order that they can provide direct care services to the patient population. **Legal Basis:** Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' and Article 9(2)(h) Health data as stated below. **Processor:** Goldstone PCN comprising: Trinity Medical Centre, Charter Medical Centre, Brighton Health & Wellbeing Centre
Social Prescribers	**Purpose:** Access to medical records is provided to social prescribers to undertake a full service to patients dependent on their social care needs. Only those patients who wish to be party to this service will have their data shared **Legal Basis:** Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' and Article 9(2)(h) Health data as stated below. **Processor:** HERA Project; TogetherCo.
Private Healthcare Providers	**Purpose:** Personal information shared with private health care providers in order to deliver direct care to patients at the patient's request. Consent from the patient will be required to share data with Private Providers. **Legal Basis:** Consented and under contract between the patient and the provider. **Provider:** Private healthcare provider of choice.
Emergency Care	**Purpose:** There are occasions when intervention is necessary in order to save or protect a patient's life or to prevent them from serious immediate harm. In many of these circumstances the patient may be unconscious or too ill to communicate. In these circumstances we have an overriding duty to try to protect and treat the patient. **Legal Basis:** Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' and Article 9(2)(c) "processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent". **Processors:** Healthcare professionals and other workers in emergency and out of hours services.
Police	**Purpose:** Personal confidential information may be shared with the Police authority for certain purposes. The level of sharing and purpose for sharing may vary. Where there is a legal basis for this information to be shared no consent will be required. The Police will require the correct documentation in order to make a request. This could be but not limited to: DS 2, Court Order, s137, the prevention and detection of a crime. In some cases, consent may be required. **Legal Basis:** UK GDPR – Article 6 1 (f) legitimate interest 6 1 (c) Legal Obligation and Article 9 2 (f) requests for legal reasons. **Processor:** Police Constabulary
HM Coroner	**Purpose:** Personal information relating to a patient may be shared with the HM Coroner upon request. **Legal Basis:** UK GDPR Article 6 1 (c) Legal Obligation and Article 9 2 (h) Health data. **Processor:** HM Coroner
Mailing Service	**Purpose:** The practice uses a mailing service to assist with the sending of patient letters. A minimum of information is shared with the mailing service for this purpose; including patient identifiable data and health data. All data shared is deleted from the data base after 28 days of the letter being produced. **Legal Basis:** the practice uses their position as a public authority to contract a third party for this purpose. Data is not processed for any other purpose by this third party. GDPR Article 6(1)(e) Public Task and Article 9(2)(h) Health Data. **Processor:** CFH Docmail Ltd
Texting Service **Messaging Service**	**Purpose:** Personal identifiable information shared with the texting/e-mail service in order that text messages or e-mails including appointment reminders, campaign messages related to specific patients' health needs and direct messages to patients **Legal Basis:** UK GDPR Article 6 1 (b) Contract, Article 6 1 (e) Public task, Article 9 2 (h). **Provider:** AccuRx, Klinik Healthcare Solutions
Communication Services: accuRx / accuMail	**Purpose:** The purposes of processing are for health and social care purposes only. The nature of the processing may include, but is not limited to:

	• Communication between patients, healthcare and/or social care professionals, via SMS, email, or other electronic communication, which may include images or documents.
	• Sending links to surveys for patients to complete regarding their care.
	• Video and audio communication for the purposes of video consultation, as outlined below.
	• Healthcare and/or social care professionals using accuRx may disclose patient data to the Data Processor when receiving technical support and from time to time the Data Processor's Technical Team may have access to patient data when they are fixing a technical issue for example via remote support, which may include screen sharing.
	• Compilation of anonymised statistics about the use of Data Processor's platform, such as the use of its functions by its users in communication with patients. These statistics may be used for the Data Processor's own analytics and improvement purposes. The Data Processor may also share these anonymised statistics publicly or with third parties. These third parties include:
	  • National bodies, including NHS Digital and NHS England;
	  • Local NHS bodies, including CCGs and Primary Care Networks;
	  • Partners of the Data Processor, including commercial organisations, charities, and academic institutions.
	• In exceptional circumstances, the Data Processor may send a message to patients directly. For example, in the event that the Data Controller has cancelled its agreement for accuRx but patients remain using live Services, the Data Processor may text the patients to ask them to contact the Healthcare and/or Social Care Organisation for advice regarding next steps, prior to deleting or returning all the data according to Data Controller's instructions.
	• Where applicable (in the case of a commercial agreement), the Data Processor may process personal data about the use of the platform and its features by the Data Controller's employees to determine billing amounts in line with such agreements.
	The video and audio communication of any video consultation is only visible to participants on the call and is not recorded or stored on any server. The IP address of call participants may be stored as part of metadata stored, however no other personal information of call participants is collected or stored.
	The video consultation service provided through the accuRx platform is hosted by Whereby who are compliant with GDPR and based in the European Economic Area (EEA). A unique URL to the video consultation is generated and all participants are visible in the consultation, no third party can 'listen in'. The video and audio communication of the video consultation is only visible to participants on the call and is not recorded or stored on any server (not accuRx's, not Whereby's and not on any third party's servers).
	All communication between participants' devices and Whereby's service is transmitted over an encrypted connection (secure web traffic using HTTPS and TLS or secure websocket traffic or secure WebRTC). The video consultation connection either:
	• connects participants to one another, relaying the encrypted data content through Whereby's TURN server, where it is not retained beyond this relay operation; or
	• connects devices using 'peer-to-peer' connections between devices.
	In both cases, as long as the participants are using their devices in the European Economic Area, it is guaranteed that any data is hosted and processed within the EEA, in line with NHS best practice guidelines on health and social care cloud security.
	The data collected about patients is limited to that necessary to provide the meeting room service, and includes:
	• Display name (if enabled and the user chooses to set one)
	• Video meeting URL accessed
	• Technical logs - information will be recorded in technical logs when the service is used. These logs will contain information such as, but not restricted to:
	  ○ IP address
	  ○ Time of registered actions
	  ○ Browser type and version
	Technical logs are purged after 90 days, sufficient to allow accuRx as the Data Processor to assist the Data Controller to complete investigations into data protection or clinical safety incidents.

	Whereby's Data Processing Agreement (available on their Data Storage and Security page) details the commitments it makes to us when we contract with them as a sub-processor. Type of data shared: Personal Data (relating to patients of the Data Controller): • Patient demographic details (name; date of birth; gender) • NHS number • Mobile phone number • Email address Personal Data (relating to healthcare and/or social care professionals): • Name • Email address • Mobile phone number • Affiliated organisations • Job role Sensitive Personal Data: • Content of the communications with – or regarding - patients sent via accuRx (which may include patient images or documents and contain data concerning health). • Other types of data (which may include contents of the patient's GP medical record and data concerning health that may from time to time be required to provide the Services). **Legal Basis:** Article 6(1)(e) '…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…'; Article 9(2)(h) '…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…'. **Processors:** accuRx Ltd, 27 Downham Road, London, N1 5AA; ICO Registration Number ZA202115; NHS Data Security and Protection (DSP) Toolkit assurance NHS ODS Code 8JT17; a list of sub-processors is available on the data processing agreement (https://www.accurx.com/data-processing-agreement) and details the company names and purpose.
Triage & Patient Flow Service: Klinik	**Purpose:** Processing your personal data is in order to carry out an automated healthcare needs assessment based on pseudonymised data, which in turn supports your practice in respect of your potential clinical diagnosis and the urgency with which you need to be seen and reviewed by a healthcare professional or to assist with non-clinical requests through a unified online software system. Klinik is configured to send and receive text messages and integrate attachments such as clinical photographs to assist diagnosis or management and will be included in the medical record based on data protection guidelines. **Legal Basis:** Processing for the purpose of the automated healthcare needs assessment We rely upon the following lawful bases for this particular processing: • Article 6(1)(f), on the basis that it is necessary for the legitimate interest of providing you with an automated healthcare needs assessment which you have chosen to undertake in connection with your access to healthcare services; and • Article 9(2)(h), on the basis that it is necessary to provide a healthcare service. **Processor:** Klinik Healthcare Solutions **FULL PRIVACY NOTICE – KLINIK HEALTHCARE SOLUTIONS** Klinik Healthcare Solutions (**"Klinik"**) is committed to protecting the privacy and security of your personal information. This privacy notice describes how we will collect and use personal information about you, in accordance with the data protection legislation including, but not limited to, the EU General Data Protection Regulation (2016/679/EC) (GDPR) the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018). **What is Klinik?** Klinik is a healthcare technology company who provides automated digital solutions to healthcare providers to help triage and prioritise patients based on the symptoms they provide. Klinik has entered into an arrangement with your GP or other healthcare provider (referred to this Privacy Notice as **"Your Healthcare Provider"**) to enable you to use the Klinik technology for the purpose of accessing the services you specifically need, based on your clinical presentation. That technology has to make use of your personal data, i.e. information relating to you from which you can be identified, and this privacy notice sets out the basis on which that data is used by Klinik.

	The law distinguishes between 'controllers' and 'processors', whereby controllers have ultimate responsibility for how and why your personal data is used, or 'processed' which is the legal terminology, and processors follow the instructions of controllers when using personal data. Klinik is both a controller and processor, depending on the specific ways in which your personal data is being processed by our technology. **Klinik as controller** Klinik has developed Artificial Intelligence, or 'AI' for short, which is designed to support healthcare providers and patients alike by triaging an individual's symptoms in order to assess their potential clinical diagnoses and the urgency with which they need to be seen by a healthcare professional. The AI uses automated processes, or algorithms, which are designed to run without human intervention using the specific personal data, including symptoms, that you enter. The personal data processed by our AI is 'pseudonymised' meaning that the identifiers have been removed such that we cannot directly identify you from it without using additional information, but it is still considered personal data in a legal sense. Klinik is the controller for the automated processing of that pseudonymised data, which enables our AI to provide a suggested diagnosis and indication of your clinical urgency to Your Healthcare Provider by carrying out an automated healthcare assessment. We would also like to use the pseudonymised data processed by our AI in order to develop and improve our product, technology and services, to include ensuring that our AI continually improves and safeguards patient safety, but only if you have given your explicit consent to us doing so. This is set out in further detail below, but in essence we will only use your data for these purposes beyond the healthcare needs assessment where you have specifically and explicitly confirmed that you consent to us doing so. **Klinik as processor** Klinik will be the processor for the digital interface you use to enter your personal details and relevant clinical information, as Your Healthcare Provider will be controller for that personal data. Klinik will also be the processor for the personal data which comprises the suggested diagnosis and clinical urgency our technology provides to Your Healthcare Provider, because it is those healthcare professionals who validate that information and determine what to do with it. As a result, the only data for which Klinik is controller is the pseudonymised data used by our AI and all directly identifiable data is processed in our capacity of a processor under instructions from Your Healthcare Provider. **Information in this privacy notice** We are required under data protection legislation to notify you of certain information about how we will use your personal data when acting as a controller, and we do so in this privacy notice. Please note that you should refer to the privacy notice of Your Healthcare Provider to find out the basis on which they process your personal data when they are acting in the capacity of a controller. It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the data protection legislation. **Data protection principles** We will comply with data protection law. This requires that the personal information we hold about you is: 1. Used lawfully, fairly and in a transparent way. 2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes. 3. Relevant to the purposes we have told you about and limited only to those purposes. 4. Accurate and kept up to date. 5. Kept only as long as necessary for the purposes we have told you about. 6. Kept securely. **The kind of information we hold about you** Personal data, or personal information, means any information about an individual from which that person can be (in)directly identified. It does not include data that does not allow you to be identified (anonymous data), but does include data where the identity has been removed but can be re- added so as to render the data identifiable again (pseudonymous data).

There are certain types of more sensitive personal data which require a higher level of protection, such as information about a person's health or sexual orientation. This known as 'special category data', and more detail on our approach in respect of this data is set out below.

In order for you to use the Klinik technology, Klinik in its role as **processor** (i.e. in respect of directly identifiable data collected from you in order to carry out the healthcare needs assessment and to provide a suggested clinical diagnosis and urgency to Your Healthcare Provider) will need to collect the following personal data:

- Personal and contact details
- First and last name
- Age
- Sex
- National Insurance Number or other personal identity code such as NHS number
- Home address
- Contact information (address, telephone number, and email address)
- IP address and other technology log information
- Approximate location of device using the patient form (if user consents to provide it)
- We will also need to collect the following special category data to enable the technology to make a fully informed assessment:
    - Current symptoms and ailments forming the basis of your proposed interaction with Your Healthcare Provider

Klinik in its role as **controller** would like to collect and use the following personal data:

- Age
- Sex
- Current symptoms and ailments

Please note, in line with the GDPR, all information that allows you to be directly identified will be stored separately by Klinik and be adequately secured to prevent identification.

Purpose of processing your personal data

The primary purpose of processing your personal data is in order to carry out an automated healthcare needs assessment based on pseudonymised data, which in turn supports Your Healthcare Provider in respect of your potential clinical diagnosis and the urgency with which you need to be seen and reviewed by a healthcare professional. Please note that it is entirely up to Your Healthcare Provider, and not Klinik, to decide on your diagnosis and whether, and if so when, any clinical intervention is required. Klinik will also, where you have given us your consent, use your personal data in pseudonymised form to develop and improve our products, service and technology. We will not use or disclose your personal data for marketing purposes.

Please note that if you access our service using your NHS login details, the identity verification services are managed by NHS Digital. NHS Digital is the controller for any personal information you provided to NHS Digital to get an NHS login account and verify your identity and uses that personal information solely for that single purpose. For this personal information, our role is a "processor" only and we must act under the instructions provided by NHS Digital (as the "controller") when verifying your identity. To see NHS Digital's Privacy Notice and Terms and Conditions, please click here. This restriction does not apply to the personal information you provide to us separately.

What is our lawful basis for using your personal data?

We will only use your personal information when the law allows us to. In this specific scenario, this means that we have to satisfy a so called 'lawful basis' for processing. Further, as some of the data we will process relates to your health then we must also identify a lawful basis. We set out below the lawful bases relied upon, depending on the specific purpose for which your data is being processed. For the avoidance of doubt, however, all the personal data which Klinik processes about you as controller for the purposes of the automated healthcare needs assessment and, if you have consented, validation and improvement of our AI has had the personal identifiers (such as name, address and contact details) removed.

Processing for the purpose of the automated healthcare needs assessment We rely upon the following lawful bases for this particular processing:

- Article 6(1)(f), on the basis that it is necessary for the legitimate interest of providing you with an automated healthcare needs assessment which you have chosen to undertake in connection with your access to healthcare services; and

- Article 9(2)(h), on the basis that it is necessary to provide a healthcare service.

As described above, this particular use of your pseudonymised data is used in order to support Your Healthcare Provider with a suggested clinical diagnosis and urgency. This form of processing is directly related to your clinical care and treatment, and so we do not need to rely upon your consent in order to use it for those particular purposes.

Processing for the purpose of improving technology and services

We would like to be able to additionally use your personal data, which again for the avoidance of doubt is in pseudonymised and not directly identifiable form, for the purpose of improving our services, including our AI technology, to ensure the highest standards of quality to patients and health professionals. We will only use your data for these purposes in circumstances where you have provided your explicit consent to us doing so, and the healthcare needs assessment can still be carried out even if you do not wish to consent to using your data for these additional purposes.

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Automated decision-making or profiling

You will not be subject to decisions or profiling that will have a significant impact on you based solely on automated decision-making. Our technology does run on an automated basis, using AI, but the outputs it produces are supportive in nature and, crucially, have to be validated by human intervention i.e. Your Healthcare Provider who will review your suggested diagnosis and/or indication of clinical urgency before making a decision themselves on how to proceed.

Data sharing

Your personal data collected and processed by the Klinik technology, including the outcome of the automated healthcare needs assessment, will be shared with Your Healthcare Provider for their own use as a controller. Your personal data will only be accessed by specified healthcare professionals who will be subject to a legal duty of confidentiality.

We also use a limited number of third party processors to help produce and provide our service, who will process your personal data on our behalf. Those third parties and the nature of the processing services they undertake are summarised in the table below. Please also be aware that they are subject to clear contractual restrictions to only use your personal data as we instruct them to do so, and subject to appropriate security measures.

Automated decision-making or profiling takes place when an electronic system uses personal information to make a decision without human intervention, which includes the use of AI. There are specific limitations and restrictions set out in the UK GDPR in respect of such decision-making and/or profiling which produces legal or similarly significant effects.

Name of processor	Country in which the processing takes place	Purpose of processing	Nature of personal data they process
Google LLC	UK	Hosting and storage services used to provide our services	All personal data
Infobip UK	UK	SMS delivery service	Telephone number and SMS messages to you
Microsoft	EU or EEA	Data reporting	Pseudoanonymized personal data

We will not otherwise share your personal information within the scope of this privacy notice unless required or permitted to do so by law. For the avoidance of doubt, however, such additional purposes will not include use of your data for insurance and/or broader commercial activities for which we not have your consent.

Transferring information outside the UK and EU

Klinik is located in the UK and Finland, and the processing of personal data will therefore mainly take place within the UK and EU. No directly identifiable personal data about you will be transferred outside the UK. We will, however, transfer your data to the EEA (provided, of course, that we have a lawful basis enabling us to process it as set out above in this privacy notice and further that the proposed transfer is in accordance with the UK GDPR) in reliance on the fact

	that the UK government has approved transfers of personal data from the UK to the EEA. For the avoidance of doubt, this transfer will only be to Klinik Healthcare Solutions based in Finland. As for the data transfers from the EU to the UK or any other country or company located outside the EEA, this will be in line with the standards of the GDPR. **Data security** We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We also have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so. This includes ensuring that all personal data stored processed on Klinik's system is protected from unauthorised access, accidental or unlawful destruction and alteration, unauthorised disclosure and other unlawful processing. Your Healthcare Provider's access to personal data is restricted to persons who need access to the server environments in use for maintaining the service. The safety of the system and access to personal data are monitored using good data protection practices. All processing of personal data considers the requirements of the data protection legislation. **How long will you use my information for?** We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. In the case of the directly identifiable data we will (in our role as processor) retain this in accordance with the instructions given to us by Your Healthcare Provider. In the case of the pseudonymised data we will (in our role as controller) retain this for a maximum of 5 years from the point at which we have collected it. We will, during that retention period, only process your personal data in the event that we have a lawful basis to do so. Please note that in respect of using your data for AI validation and improvement then in the event that you subsequently withdraw your consent for us to use your data for such purposes then we may need to continue to retain, for instance to defend legal proceedings, but we will stop using it for any other purposes or it is converted it into a fully anonymised dataset. **Rights of access, correction, erasure, and restriction Your duty to inform us of changes** It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us. **Your rights in connection with personal information** Under certain circumstances, and as set out in further detail in our general privacy notice, by law you have the right to: • **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it. • **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected. • **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below). • **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. • **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it. • **Request the transfer** of your personal information to another data controller. • **Lodge a complaint** with the supervisory authority, if you think we process your personal data unlawfully. If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact our Data Protection Officer (details below) in writing. Please note that you should direct any queries to Your Healthcare Provider which relate to the personal data you have entered into the patient interface or has been subsequently received and used by Your Healthcare Provider following the output of the automated healthcare assessment.

	• **No fee usually required** You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances. **What we may need from you** We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it. **Right to withdraw consent** In the specific circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. This can be done at any time. Such withdrawal shall not affect the lawfulness of processing based on consent before its withdrawal. **Data protection officer** For further information please contact our Data Protection Officer, whose details are: Jukka Happonen Head of Product Development Klinik Healthcare Solutions Oy *tietosuoja@klinik.fi* **Changes to this privacy notice** We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.
Remote Consultations including Video Consultation and Clinical Photography	**Purpose:** Personal information including images may be processed, stored and with the patients consent shared, in order to provide the patient with urgent medical advice during the COVID-19 pandemic. **Legal Basis:** Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' and Article 9(2)(h) Health data as stated below Patients will be asked to provide consent if required to provide photographs of certain areas of concern. There are restrictions on what the practice can accept photographs of. No photographs of the full face, no intimate areas, no pictures of patients who cannot consent to the process. No pictures of children. **Processor:** AccuRx, Klinik Healthcare Solutions
Multidisciplinary Meetings **Group Consultations**	**Purpose:** For some long-term conditions, such as diabetes, the practice participates in meetings with staff from other agencies involved in providing care, to help plan the best way to provide care to patients with these conditions. During COVID 19 the practice may use secure video meeting platform to discuss patient needs. **Legal Basis:** Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' and Article 9(2)(h) Health data as stated below. **Processor:** MS Teams
COVID-19 Research and Planning	**Purpose:** To understand the risks to public health, trends and prevent the spread of infections such as COVID-19 the government has enabled a number of initiatives which include research and planning during the COVID-19 pandemic which may include the collection of personal confidential data has been necessary. This is to assist with the diagnosis, testing, self-isolating, fitness to work, treatment medical, social interventions and recovery from COVID-19. **Legal Basis:** Notice under Regulation 3(4) of the Health Service (Control of Patient Information) Regulations 2002 (COPI), which were made under sections 60 (now section 251 of the NHS Act 2006) and 64 of the Health and Social Care Act 2001. Coronavirus (COVID-19): notice under regulation 3(4) of the Health Service (Control of Patient Information) Regulations 2002, which were made under sections 60 (now section 251 of the NHS Act 2006) and 64 of the Health and Social Care Act 2001 – Biobank - GOV.UK (www.gov.uk) Coronavirus (COVID-19): notification to organisations to share information - GOV.UK (www.gov.uk) **Provider:** UK Biobank, NHS Digital, NHS England, other organisations included in the roll out of vaccinations, treatment and care of patients suffering with COVID-19

General Practice Extraction Service (GPES) 1. At risk patients' data collection Version 3 2. COVID-19 Planning and Research Data 3. CVDPREVENT Audit 4. Physical health checks for people with Severe Mental Illness	**Purpose:** GP practices are required to provide data extraction of their patients' personal confidential information for various purposes to NHS Digital. The objective of this data collection is on an ongoing basis to identify patients registered at General Practices who fit within certain criteria, in order to monitor and either provide direct care, or prevent serious harm to those patients. Below is a list of the purposes for the data extraction, by using the link you can find out the detail behind each data extraction and how your information will be used to inform this essential work: 1. At risk patients including severely clinically vulnerable 2. Covid-19 Planning and Research data, to control and prevent the risk of Covid-19 3. NHS England has directed NHS Digital to collect and analyse data in connection with Cardiovascular Disease Prevention Audit 4. GPES Physical Health Checks for people with Severe Mental Illness (PHSMI) data collection. **Legal Basis:** All GP Practices in England are legally required to share data with NHS Digital for this purpose under section 259(1)(a) and (5) of the 2012 Act Further detailed legal basis can be found in each link. Any objections to this data collection should be made directly to NHS Digital. enquiries@nhsdigital.nhs.uk **Processor:** NHS Digital or NHSX
Professional Training	**Purpose:** We are a GP training surgery. On occasion you may be asked if you are happy to be seen by one of our GP registrars. You may also be asked if you would be happy to have a consultation recorded for training purposes. These recordings will be shared and discussed with training GPs at the surgery, and also with moderators at the RCGP and HEE. **Legal Basis:** Article 6 1 (a) consent, patients will be asked if they wish to take part in training sessions. Article 9 2 (a) - explicit consent will be required when making recordings of consultations. Recordings remain the control of the GP practice and they will delete all recordings from the secure site once they are no longer required. **Processor:** Royal College of General Practitioners (RCGP), Health Education England (HEE), iConnect, Fourteen Fish, Agilio Software / Clarity Informatics Ltd (TeamNet)
Practice Management Solution: TeamNet	**Purpose:** TeamNet is a web or cloud-based service offering a central hub for knowledge, compliance and workforce management which includes practice communications; storage of staff human resources data as per national legislation and guidelines in a safe and secure way; training compliance and resources; systems safety data such as significant events, safeguarding reviews and complaints data; compliance with CQC requirements; compliance with other business legislation, e.g., health and safety, COSSH; enables documentation of information for professional registration, appraisals, and revalidation following professional regulation legislation. Information is protected by password and staff roles access rights and staff confidentiality applies. Staff information is accessible by the local PCN group. Information can be shared with other Agilio/Clarity Informatics Ltd services to enable professional regulation with appraisal documentation – Clarity Doctors / Clarity Nurses. Individual clinicians are responsible for maintaining information governance compliance when using these services for their professional development. Any patient data held within this service is pseudonymised and no personally identifiable information is recorded. For the full privacy policy see the following: https://agiliosoftware.com/policies/primary-care-policies/privacy-policy/ **Legal Basis:** The lawful basis for processing this data under UK GDPR is Article 6 1 (b) contract where the subject is subject to the contract and 9 2 (h) Health data **Processor:** Agilio Software / Clarity Informatics Ltd (TeamNet)

Telephony Services	**Purpose:** The practice uses an internet-based telephony system that records telephone calls, patients will have the right to decline recordings of calls as is their individual right. The calls will be held on the external server for a duration of 3 years unless requested for them to be removed sooner. The telephone system has been commissioned to assist with the high volume and management of calls into the surgery, which in turn will enable a better service to patients. **Legal Basis:** While there is a robust contract in place with the processor, the surgery has undertaken this service to assist with the direct care of patients in a more efficient way. Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' and Article 9(2)(h) Health data as stated below. **Provider:** Louiscomm
Learning Disability Mortality Programme (LeDeR)	**Purpose:** The Learning Disability Mortality Review (LeDeR) programme was commissioned by NHS England to investigate the death of patients with learning difficulties to assist with processes to improve the standard and quality of care for people living with a learning disability. **Legal Basis:** It has approval from the Secretary of State under section 251 of the NHS Act 2006 to process patient identifiable information who fit within certain criteria. **Processor:** NHS Brighton & Hove CCG, NHS Sussex CCGs/ICB, NHS England
Technical Solution Pseudonymisation	**Purpose:** Personal confidential and special category data in the form of medical record, is extracted under contract for the purpose of pseudonymisation. This will allow no patient to be identified within the data set that is created. SCW CSU has been commissioned to provide a data processing service for the GPs, no other processing will be undertaken under this contract. **Legal Basis:** Under UK GDPR the legitimate purpose for this activity is under contract to provide assistance. Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' and Article 9(2)(h) Health data as stated below. **Processor:** South, Central and West Commissioning Support Unit (SCW CSU)
Shared Care Record	**Purpose:** In order for the practice to have access to a shared record, the Integrated Care Service has commissioned a number of systems including GP connect, which is managed by NHS Digital, to enable a shared care record, which will assist in patient information to be used for a number of care related services. These may include Population Health Management, Direct Care, and analytics to assist with planning services for the use of the local health population. Where data is used for secondary uses no personal identifiable data will be used. Where personal confidential data is used for Research explicit consent will be required. **Legal Basis:** Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' and Article 9(2)(h) Health data as stated below. **Processor:** NHS Digital, ICS member providers
Medical Records Storage: noteSpace	**Purpose:** noteSpace offers GPs secure off-site record storage and easy access to patient records (Lloyd George medical records) to release space for practices to use. noteSpace meets CQC requirements for records storage security standards. Barcodes and web-based software are used to organise and track information stored in their secure vaults which is monitored with video surveillance 24 hours a day and use the strictest access features such as keypad controls and biometric fingerprint scanners. **Legal Basis:** Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' and Article 9(2)(h) Health data as stated below. **Processor:** Niche Health, OASIS Group
Medical Equipment Software: Kardia	**Purpose:** Near patient testing to assist clinician diagnosis of cardiac conditions, e.g., arrythmias, with use of a clinician held device using their smart phone with their personal Kardia account. ECG tracing and pulse rate and rhythm is analysed and stored on the device and documented on patient medical records. Data is anonymously collected and regularly cleared from these accounts. **Legal Basis:** Consent prior to examination. **Processor:** AliveCor, WellBN
Dictation Services	**Purpose:** Personal confidential data is shared with Lexacom software or cloud-based services in order to facilitate clinicians providing healthcare services for patients, i.e., referrals to health and social care providers. **Legal Basis:** The legal basis for this activity under UK GDPR is Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' and Article 9(2)(h) Health data as stated below. **Processor:** Lexacom

Lawful basis for processing:

The processing of personal data in the delivery of direct care and for providers' administrative purposes in this surgery and in support of direct care elsewhere is supported under the following Article 6 and 9 conditions of the UK GDPR:

- Article 6(1)(e) '…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…'; and
- Article 9(2)(h) 'necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services..."

Privacy Officer & Senior Information Risk Owner (SIRO): Maureen Wilcock (Operational Practice Manager & Partner)

Caldicott Guardian: Dr Francis Richards (GP Partner)

Data Protection Champion: Ruby O'Shea (Secretary)

Data Protection Officer: provided by South, Central, West Commissioning Support Unit (SCW CSU) https://www.scwcsu.nhs.uk/

Reviews of and changes to our Fair Processing (Privacy) Notice

We will keep our Fair Processing (Privacy) Notice under regular review. This notice was last reviewed on 14th October 2023 by Dr Francis Richards (General Practitioner & Caldicott Guardian).