Patient Privacy Notice

This privacy notice explains what information we collect from you, how we store this, how long we retain it, and with whom and for which legal purpose(s) we may share it.

An introduction to UK data protection law	Your personal information is very important to you – and to us. The way we keep, collect and use information about you has developed alongside technology. The laws that govern the use of your personal data have changed to cover these developments, and include UK General Data Protection Regulations (UK GDPR), Data Protection Act 2018, and Data Use and Access Act 2025.
What does this mean for me and my data?	**You're better protected** The new rules make sure that all organisations are set up to protect any personal data they hold, and to act if something goes wrong. Rest assured, robust security has always been a crucial part of everything we do. **You have more control** You have a right to have your privacy respected and your data protected. The new law gives you easier access to the personal information we hold about you, if you wish to check or change it. It is designed to give you confidence that this information is accurate, up to date, and well managed. You can choose who can contact you, and how. You can change your mind at any time. You can control if and how we contact you, for example by email or phone. We must give you the opportunity to change your mind about the choices you have made. This helps to give you options and keep you in control.

Our services	East Suffolk and North Essex NHS Foundation Trust (ESNEFT) serves the geographical area of East Suffolk and North Essex with a population of more than 700,000. We are two acute hospitals (Colchester Hospital and Ipswich Hospital), but we are also responsible for and/or utilise the following community services: • Aldeburgh Community Hospital • Felixstowe General Hospital • Bluebird Lodge • Hartismere Place • Foot and Ankle Service • Community Nursing Services (East Suffolk) • North East Essex Community Services (NEECS) • Clacton and Harwich Community Hospitals • Halstead Hospital • North East Essex and Suffolk Pathology Services (NEESPS) • Paediatric therapy services previously provided by Health Care Resourcing Group (HCRG) Our Trust is registered with the Information Commissioner's Office (ICO) to process personal and special categories of information under the Data Protection Act 2018 / General Data Protection Regulations and our registration number is Z6601302.
What information do you collect from me?	We collect and store personal identifiable information about you in order to provide you with the necessary investigations, care and treatment that you need.This information includes but is not restricted to: • full name • date of birth • address • contact details (phone number/email address) • NHS number • details of current medical information • details of care and treatment previously provided by us • information received from other health care providers • information sent to other health care providers.

Where do you get my information from?	The hospital usually first receives information about you from the professional who refers you for further investigation or treatment. This may be: • your GP • another hospital • social care providers • community health services • private care practitioners • other care providers. When you attend the hospital, such as in an emergency, we record information you give us directly. You are not under a statutory or contractual obligation to provide this data, but we are unable to provide you with any treatment without this data.
How do I access my medical records?	Your medical and healthcare information is just that – yours. You can access the information we hold about you at any time – and at no additional cost. If you would like to see the information we hold about you, you can request a copy of your medical records. There is no charge for this services, and all requests will be completed within one calendar month. If this is something you would like to do, please visit our website at https://www.esneft.nhs.uk/about-us/privacy/access-to-your-medical-records/ to submit your request to the Access to Health Records portal. Alternatively, you can email the team at: SAREsneft@esneft.nhs.uk
What is our legal basis for processing your personal information?	Under the Data Protection Act 2018 and Article 6 of the GDPR, we must have a lawful basis to process, share and store your information. These are: consent, contract, legal obligation, vital interests, public task, and legitimate interests. In the majority of cases, the Trust will rely on the Public Task (Article 6(1)(e)) lawful basis to process and share your information. In order to process special category data, such as medical information, we must have a second lawful basis under Article 9 of the GDPR. In the majority of cases, the Trust will use the “Provision of Health and Social Care (Article 9(2)(h))” lawful basis to process special category data. When your information is processed to manage health emergencies such as COVID-19, the legal basis is ““the performance of a task carried out in the public interest or in the exercise of official authority vested in

	the controller" under the GDPR Article 6(1)(e) and "processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health" under the GDPR Article 9(2)(i). As a public body, the Trust will not rely on legitimate interests as a legal basis unless there are exceptional circumstances.
What are my rights under GDPR?	You have a number of rights regarding your data under the Data Protection Act 2018 / GDPR: **The right to request access** You have the right to obtain: • confirmation that your data is being processed • access to your personal data • other information • evidence that we treat your information within the rules of the law. **The right to be informed** You have the right to be informed about the collection and use of your personal information. We must provide you with information including: our purposes for processing your personal information, our retention periods for that personal information, and who it will be shared with. We call this 'privacy information'. **The right to request rectification** You have the right to ask that any information you believe is inaccurate be corrected or completed if it is incomplete. Please note that this is not an absolute right and is subject to review by the Data Protection Officer and the Caldicott Guardian. **The right to request erasure** You have the right to ask that we delete any information we hold about you. This is also known as the right to be forgotten. Please note that this is not an absolute right and is subject to review by the Data Protection Officer and the Caldicott Guardian. **The right to the restriction of processing**

	This means that you can limit the way we share your information. This is an alternative to requesting the erasure of your information. This means that we can hold your information but we cannot use it or share it with external organisations. **The right to object to processing** • to us using your information for reasons other than to provide you with care • to your information being used for direct marketing (including profiling) • to your information being used for purposes of scientific or historical research and statistics **The right to data portability** You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances. **Rights related to automated decision making including profiling** Automated individual decision-making is a decision made by automated means without any human involvement. The Trust relies on Article 6(1)(e): Public Task should we engage in any automated decision making and/or profiling. This includes using Artificial Intelligence (AI) technology in our healthcare services. Automated decision making will never be used at the Trust for direct marketing. You have the right to object to the Trust using your data for automated decision making purposes. You are not required to pay any charge for exercising your rights. If you make a request, we have one calendar month to respond to you. If you wish to exercise any of the above rights in relation to data we hold about you, please contact: **Information Governance Team** Ipswich Hospital, Heath Road, Ipswich IP4 5PD Email: dpo@esneft.nhs.uk
How do I withdraw consent from sharing my information?	If you were asked to give consent for your information to be shared and you no longer wish for this to happen, you can request to withdraw your consent at any time. All requests will be considered on a case-by-case basis.

	You can also request the following: • To have information you believe to be incorrect, corrected (Right to Rectification) • To have your information erased (Right to Erasure) • The processing of your information restricted (Right to Restrict Processing) • To object to the processing of your data (Right to Object to Processing) If this is something you wish to do please contact: Information Governance Team Ipswich Hospital, Heath Road, Ipswich IP4 5PD Email: dpo@esneft.nhs.uk
How do you protect my information?	All staff employed by ESNEFT are required to undertake mandatory annual training about their role and responsibilities when collecting and handling personal data. We keep your information safe and secure and comply with industry standards such as Cyber Security Essentials and the Data Security and Protection Toolkit. We only share your data in a way that identifies you when absolutely necessary and never sell it onto third parties.
What do you do with my information?	Most importantly we use your information to provide you with the care and treatment you need. In addition to this: • we may need to use your information to help us protect the health of the public for example; monitoring of certain infectious diseases such as tuberculosis • to ensure the Trust runs efficiently, plans for the future, trains its staff, pays its bills and can account for its actions • your information may be used for the benefit of clinical research • you may need to receive care or equipment from other providers therefore we would need to share your information so that they can provide you with the necessary equipment or care and treatment you need • in certain circumstances we are required by law to share your information with other organisations and authorities • your information may be used to defend a legal claim or where a court instructs us to • we may use your information to protect your vital interests or the interests of any individuals when you are unable to give consent.

	• we may share your health information where we are required to do so under law in order to comply with a public inquiry, review, investigation or law court, for example the Infected Blood Enquiry or the Covid-19 Enquiry There are occasions where we would like to use your information for reasons other than stated above. This could mean providing your information to third parties who require it to test new technologies or providing your information to assess the services we currently provide so that we can improve them. Where we require your information for these purposes we would need your explicit consent to use it. This is because it is your information and we must have your consent to use it for any purpose other than those stated above. Please be assured that your care will not be affected if you do not provide consent for your information to be used for anything other than your direct care. If you do give your consent but later change your mind you have the right to withdraw your consent at any time.
Who do you share my information with?	Below is a list of some of the types of organisations we may share your information with: • Epic, the Trust's Electronic Patient Record (EPR). Your data held in Epic will not be shared outside of the Trust's servers based in the UK. Your personal data (healthcare record) is held within the EPR as well as other clinical systems external to the EPR but within ESNEFT. For example, some data from the EPR may be processed within ESNEFT's Data Reporting Environment for analysis to improve clinical care, operational planning and patient experience. Epic EPR also includes MyChart, which is the patient portal where patients can access information relating to themselves or on a proxy basis. Please note, proxy access is not automatic and requires an authorisation process. • Epic CareEverywhere is used within the Epic patient record to exchange electronic health records with outside organisations who have an Epic electronic patient record. It provides access, at the point of care, to a patient's health records in situations where an NHS Trust, using the Epic system, has a patient in common. • Epic CareLink is a secure, web-based portal for viewing patient information. GP surgeries, care homes and hospices would be provided with access to patient data via EpicCare Link. These users do not have access to a patient's full Epic record, but will have limited access to the patient database

	at ESNEFT. EpicCare Link users can view information, order tests and send secure messages to ESNEFT but they cannot enter patient data on their Epic record. • GP practices • other NHS trusts • Integrated Care Boards (ICB) • the police • community teams • social care providers • equipment providers • regulatory bodies • IT providers • support services • registry offices • coroners • funeral directors • medical schools • the Health Research Authority (if you have consented to participate in clinical research) • other healthcare providers • The Care Coordination Solution – which processes patient special category (health) personal data to support the better coordination of Elective Care. The aim is to improve the delivery of planned treatment through better use of the information that the Trust already holds. It aims to make sure the data is valid and accurate, and that the Trust can use the information to improve on the waiting times for elective care in the wake of the COVID-19 pandemic. • GP Connect – the Trust uses 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. You can opt out of your information being shared by GP Connect at your GP surgery. More information is available here: GP Connect - NHS England Digital • We also share your information with other healthcare providers via the NHS App, if you have signed up to this service. • National audits and surveys, such as the National Cancer Patient Experience Survey (NCPES) • Statutory enquiries
How long do you keep my information for?	How long we keep your information depends on what the information is. For up to date details about the retention periods please refer to the NHSX Records Management Code of Practice for Health and Social Care, which is available on the NHS Digital website

Is my data held or transferred overseas?	All Trust servers are based in the UK, however, some of the service providers we use may hold your information outside the UK. If we do transfer your personal information outside of the UK we will ensure that it is protected to the same extent as it would be within the UK. A Data Protection Impact Assessment is completed for all systems and processes that use personally identifiable data, with appropriate risk assessments for transferring data overseas.
Who is responsible for Data Protection at ESNEFT?	There are a number of roles within the Trust that have responsibility for protecting the information you provide us with. • The Data Protection Officer (DPO) is George Chalkias, Director of Governance • The Senior Information Risk Owner (SIRO) is Mike Meers, Director of Digital and Logistics • The Caldicott Guardian is Dr Martin Mansfield, Deputy Chief Medical Officer All our staff are required to access only the information they need to provide you with the care and treatment you need. They must also keep it safe and secure at all times.
Any further questions or concerns?	If you have any concerns about the security of your information please contact the Data Protection Officer via email at dpo@esneft.nhs.uk You can also complain to the Information Commissioner's Office if you are unhappy with how we have used your data. The ICO can be contacted at: Information Commissioner's Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF Helpline number: 0303 123 1113 ICO website: https://www.ico.org.uk