South Infirmary Victoria University Hospital (SIVUH) Privacy Notice

This privacy notice sets out how the South Infirmary Victoria University Hospital as Data Controller processes all the personal information that it collects, generates and holds in the course of providing healthcare services. It explains what personal information we collect on data subjects as data controller, how we use it, who we share it with and the security in place to protect it. It also sets out the privacy rights that data subjects have under General Data Protection Regulation (GDPR) and Irish data protection legislation.

The South Infirmary Victoria University Hospital is a Voluntary Acute Hospital governed by a Board of Directors, operating under Section 38 of the Health Act, within the South South West Hospital Group (SSWHG). The SIVUH is data controller for personal data of our patients, staff and contractors.

1. Our obligations and rights of the data subjects

We aim to ensure all personal information is processed and stored in line with data protection principles and legislation and that our work activities do not infringe on the privacy rights of data subjects. This means that all personal information is:

- obtained and processed fairly, lawfully and transparently
- collected and processed for specific legitimate purposes only, and not in any manner incompatible with those purposes
- adequate and relevant and limited
- kept accurate and up to date
- kept no longer than is necessary
- kept safe and secure.

2. Why the SIVUH collects personal information

The South Infirmary-Victoria University Hospital Ltd. came into existence on 1st January 1988 as a result of the amalgamation of the South Charitable Infirmary and the Victoria Hospital. The South Infirmary Victoria University Hospital operates under the Health Acts 1947-2007. The SIVUH collects and processes personal data and special category personal data in the provision of health and social care services or in the management of health and social care systems and services on the basis of Irish law (Health Acts 1947-2007 / Mental Health Act etc.)

3. What information do we collect and on what basis do we process it?

The data that we typically process for patients and service users is classified in GDPR as personal data and "Special Category" data, i.e. mainly health data but also other special category data if it may impact the provision of medical care e.g. racial or ethnic origin, religious or philosophical beliefs, genetic data, biometric data. The processing of this data is strictly prohibited in general circumstances but the SIVUH may process this special category personal data in the provision of health and social care services or in the management of health and social care systems and services on the basis of Irish law (Health Act 1947-2007 / Mental Health Act etc.)

We will only process special categories of personal data where it is necessary:
• for the purposes of preventative or occupational medicine,
• for medical diagnosis,
• for the provision of healthcare, treatment or social care,
• for the management of health or social care systems and services,
• pursuant to a contract with a health professional.
Processing of special category data is lawful where it is undertaken by or under the responsibility of
• a health practitioner,
• a person who in the circumstances owes a duty of confidentiality to the data subject that is equivalent to that which would exist if that person were a health practitioner. For example the outpatient clinic secretary, Emergency Department Receptionist, Primary Care Centre staff etc.

We also process personal data of staff and contractors. Our lawful basis for processing staff personal data is that the processing is necessary in the fulfilment of a contract.

We have appropriate policies and procedures in place to ensure that staff only collect information that is necessary and ensures it is treated as highly confidential and that it is stored in a secure manner.

The South Infirmary-Victoria University Hospital collects patient personal information directly from the patient or from a person acting on the patient's behalf such as the General Practitioner or Consultant. The personal information that we process includes, name, date of birth, address. The special category data we process includes health history, test results, records of visits to the South Infirmary-Victoria University Hospital and the care received during those visits.

4. How the data we collect is used

Personal information is a key resource for us in order for us to make evidence-based decisions on the provision of healthcare for patients and is necessary to carry out our obligations under the Health Acts 1947-2007 and to manage and support our staff.
We may use patient information to manage and deliver patient care and treatment to ensure that the treatment is safe and effective, that the right decisions are made about patient care and so that we can co-ordinate with other organisations that may be involved in patient care.
Patient information may be used to:
• To treat and care for patients, and make appointments
• To plan and provide services
• To receive payment from insurers
• To fulfil insurance notification requirements
• Review the care and treatment provided to ensure it is of the highest standard possible and to evaluate and improve the safety of our services. This can be carried out by multiple quality improvement methods e.g. accreditation, audits, clinical audit, patient experience surveys.
• Investigate complaints, legal claims and adverse incidents
• Plan the future demand in the hospital e.g. analysing peak attendance times, staffing levels and average length of stay; establishing the projected demand by disease/condition
• Preparing statistics on hospital performance and monitoring how we spend public money
• Protect the wider public interests e.g. Influenza, winter vomiting bug, COVID-19.
• Provide training and development to health professionals.
• Invoicing, billing and account management.
• Remind you of appointments by text/email/letter.
• To identify patients/service users that might be suitable for clinical trials/research.
• To comply with Department of Health & Children and HSE requirements on returning data on waiting lists for services

• To report to the Hospital In-Patient Enquiry (HIPE)
• To comply with legal and regulatory requirements, such as reporting notifiable diseases to the HSE Department of Public Health and provision of information to the National Cancer Registry and Irish Medicines Board.

4.3 Shared services across Cork Acute Hospitals

The national re-organisation of Hospitals (Hospital Reconfiguration Programme) allowed for the sharing of information and services across hospital sites including SIVUH, Cork University Hospital (CUH) and the Mercy University (MUH). The user security model ensures users are only permitted to view activity data for the specific site where they have a role. Some users have been granted multi campus permissions on a need to know basis to view incidents in support of the new integrated service delivery model. The project introduced a new patient ID number (known as the RID number) that is used in all hospitals in the Cork region to uniquely identify the patient. This number is used as the main way of identifying the patient on all requests for patient services and it is linked to the laboratory and radiology systems.

4.4 Health Research and statistical analysis

The SIVUH is a teaching Hospital; we work closely with UCC and other academic institutions. We provide placements for students and allow access to information for essential student education and research. All clinical research projects must be approved by the Clinical Research Ethics Committee of the Cork Teaching Hospitals (CREC), or equivalent and the Board of Directors SIVUH. All clinical trials must be approved by the Clinical Research Ethics Committee of the Cork Teaching Hospitals (CREC), or equivalent and the Board of Directors SIVUH. All non clinical research must be approved by the Board of Directors, SIVUH. In addition each clinical trial and health research project is reviewed by the SIVUH Data Protection Officer (DPO) and Quality and Risk Management Department before approval is sought from the Board of Directors to check for compliance with the Data Protection Act (Health Research Regulations) 2018. All health research conducted on SIVUH data is conducted in keeping with the Data Protection Act (Health Research Regulations) 2018. Where patient personal data is processed for health research, explicit consent will be obtained where necessary and specific measures will be put in place to safeguard patient data in accordance with data protection requirements. Clinical audit and service evaluation is an essential part of clinical governance; patient data rendered anonymous may be reviewed as part of the quality improvement process to improve patient care and outcomes. All clinical audits must be notified to the Quality & Risk Management Department and DPO for review to ensure they are in keeping with data protection legislation.

The role of the SIVUH HIPE Department is to record and code inpatient and day case episode data. All of the hospital inpatient and day case patient activity is presented to the Department of Health & Children, where it is assessed for the designation of the hospital's Casemix Budget Adjustment Allocation. The HIPE Coding Office provide data reports to SIVUH staff and other healthcare providers and institutions conducting clinical audits as part of the provision of healthcare services and in the interest of public health.

4.5 Data Sharing for National Health Services

The HSE have governance over a large number of acute hospital systems e.g. NIMIS for radiology, iPMS for patient information, PCRS for Hospital Pharmacy Portal Primary Care Reimbursement Scheme, COVAX for Covid Vaccinations. The SIVUH has a data sharing agreement with the HSE and work closely with the HSE and South South West Hospital Group (SSHWG) on all aspects of shared services.

The National Cancer Registry Ireland (NCRI) collects information on cancer cases diagnosed in Ireland and other personal health information directly from the healthcare providers. The NCRI also collects personal health information on patients who may not have been diagnosed with cancer e.g. information on participants of screening programmes. This data is collected and processed for public health and cancer research purposes.

The National Treatment Purchase Fund (NTPF) collects, collates and validates information on persons waiting for public hospital treatment. In an effort to reduce waiting lists for public appointments or procedures the NTPF may arrange for the provision of hospital treatment for patients at an alternative hospital. In carrying out its functions, the NTPF works closely with the SIVUH, the Department of Health, the HSE, other acute public hospitals and private nursing homes across the health system. SIVUH are obliged to share data relating to patients waiting for inpatient and outpatient procedures with the NTPF. The SIVUH may also during the course of outsourcing procedures share patient data with treating hospitals. Data protection agreements are in place with potential treating hospitals. The NTPF operates under the National Treatment Purchase Fund (Establishment) Order, 2004 and the Nursing Homes Support Scheme Act (2009). For more information, please see www.ntpf.ie

Health Protection Surveillance Centre (HPSC) requires all medical practitioners to notify the Medical Officer of Health (MOH)/Director of Public Health (DPH) of certain diseases. This information is used to investigate cases thus preventing spread of infection and further cases. The information also facilitates the early identification of outbreaks. Information is also used to monitor the burden and changing levels of diseases, which can provide the evidence for public health interventions such as immunisation. The information collected on notifiable diseases from doctors is used to detect and investigate outbreaks, and prevent spread of infection and implement and monitor interventions such as immunisation to protect public health. Notification to the Medical Officer of Health is a legal obligation and is not in contravention of data protection legislation. The Medical Officer of Health is required to treat records of infectious disease notifications in a confidential manner. In general, access to personal information (such as name and address) is not provided, however, in some circumstances where public health action is needed for contact tracing or if HPSC doctors are leading a national or international outbreak investigation, HPSC doctors may be provided with identifying information. The SIVUH will notify the HSPC of infectious diseases as necessary. For further information visit www.hpsc.ie

National arrangements are in place for the supply and dispensing of high tech medicines through Community Pharmacies. Such medicines are generally only prescribed or initiated in hospital. The HSE Primary Care Reimbursement Service (PCRS) coordinates the provision of high tech medicines. Patient prescriptions are inputted on this national system by medical staff and the medicines are purchased by the HSE and supplied through Community Pharmacies, the cost of the medicines and patient care fees are paid by the PCRS. Where SIVUH patients require high tech medicines, relevant data is shared with the PCRS High Tech Co-ordination Unit. The system follows the journey of the prescription across the main stakeholders: Consultant/GP - Patient - HSE PCRS – Pharmacy – Supplier.

The HSE National Integrated Medical Imaging System (NIMIS) provides state of the art electronic radiology systems in hospitals. NIMIS enables secure and rapid movement of patient image data throughout the health service. NIMIS allows doctors to electronically view their patient's diagnostic images, such as X-Rays and CT Scans, quickly and easily. With NIMIS, Ireland's Radiology services are filmless and offer many benefits to patients including; patient's prior and current images will be available electronically in the radiology department, out-patient clinic, or hospital ward; fewer repeat exams; faster turn-around for reports; rapid transfer of images between clinicians for consultation or remote referral; security of patient data with controlled and audited access.

4.6 Data Sharing with GPs

A large volume of medical information is shared between a patient's GP and Hospitals. This information is usually sent by post or electronically. There are a number of secure electronic means of sharing information with GPs. Healthlink is a HSE system that allows patient information to be securely transferred between Hospitals and GPs via online systems and email (health mail), the type of information includes electronic referrals, discharge summaries, lab reports, radiology reports. Healthmail is a secure email system provided by the HSE for GPs, Community Pharmacies and Nursing Homes. Healthmail allows secure communication of patient information with colleagues in primary and secondary care. Healthmail is an email service that allows GPs send and receive clinical patient information in a secure manner. For more information visit www.healthlink.ie.

4.7 Sharing information with and use of third party agencies

Patients often receive health or social care from other providers i.e. private or other voluntary hospitals, HSE, specialists etc. In order to assist in this process, we may make referrals requiring the need to share patient personal information with those providers. We will only do so if there is a genuine need, in order to ensure the highest quality of care is provided to the patient and we will always seek permission of the patient when required. We are careful only to share the information that is necessary for this purpose. In certain situations, we may have to disclose your personal information to other agencies, in accordance with legal requirements, i.e. Dept. of Social Welfare, Department of Health, the Courts etc., or in an emergency situation to prevent injury to you or other persons. Data Processing Agreements, Service Level Agreements and/or Confidentiality Agreements are in place where data is shared with third parties.

SIVUH use T-Pro's Clinic Manager platform for managing our virtual clinics and our digital dictation software requirements. This system is integrated with our patient information system to ensure efficiency and accuracy.

A number of third party billing agencies are used in the Hospital. Claimsure is an electronic system which is used to process private health insurance claims. Medserv is an electronic billing system used by a number of Consultants for private billing.

Private health insurance companies including VHI, LAYA, Irish Life Health, process their member's information to validate healthcare claims. Private health insurance companies also audit claims information which requires access to patient medical records, this is done with consent.

We are obliged under HSE National Financial Regulation 25 to collect overdue accounts, this is outsourced to a third party collection agency.

Change Healthcare Ireland provide the software for operating NIMIS in our Radiology Department.

We work closely with suppliers of orthopaedic surgical implants and components, in instances where patients require made to measure products, patient information is shared with the supplier.

SIVUH may operate a visitor scheduling and a visitor contract tracing system with regard to COVID-19. The visitor scheduling and contract tracing system when in place is operated by Yellow Schedule. The system records the contact details of each visitor and the time and place of the visit which enables efficient and effective contact tracing should a COVID positive case be detected. Visitor data is saved for 14 days post visit.

We store a large volume of healthcare records and other records off site in secure storage. Our current provider is Iron Mountain. SIVUH records are stored at the Iron Mountain facility in Carrigtwohill. Patient healthcare records when archived after 6 months onsite are moved from our Medical Records Library to Iron Mountain.

All confidential waste is disposed of into secure bins, secure disposal of this confidential waste is provided by DGD Shredding.

Patient and/or staff personal data may also be disclosed to law enforcement/ An Garda Síochana for investigative purposes if requested by appropriate statutory authorities in the course of an investigation or court proceedings and in line with data protection legislation.

SIVUH has established a number of data-sharing agreements and memorandums of understanding (MOU) with other public authorities and private Hospitals in order to provide services and share information, which may include personal identifiable information. These agreements have been set up to help assist SIVUH with its regulatory duties and to ensure cooperation within common areas of interest between SIVUH and other public authorities.

4.8 The use of CCTV

The SIVUH uses camera surveillance systems (commonly referred to as CCTV) throughout its facilities for the purpose of maintaining the safety and security of its staff, service users, patients, visitors and members of the public. SIVUH is aware that footage or images containing identifiable individuals captured by CCTV systems are personal data for the purposes of data protection. The SIVUH CCTV systems may, but will not always, collect and store personal information. The SIVUH will comply with the GDPR and this privacy notice in respect of any personal information collected via its CCTV systems. Further information is available from the SIVUH DPO.

4.9 Information about our own staff and people applying to work with us

In order for SIVUH to carry out its work activities, SIVUH must process some personal information belonging to employees and contractors. This personal information is also processed and stored in line with any legal or contractual obligations that SIVUH must follow as an employer. SIVUH use third-party contractors to outsource certain human resources (HR) activities, certain details belonging to employees/potential employees are processed by a third-party processor. All information belonging to employees of SIVUH is processed in line with best practice guidance, stored for a period of time set out in a retention schedule and is only used for the specific purpose for which it was gathered. All applications for new posts at SIVUH are processed by an online recruitment agency Rezoomo. SIVUH must also ensure that potential employees are suitable for their roles, in this regard we may collect medical information or undertake the Garda Vetting process or seek evidence of education and qualifications, and we may also look for details of referees.

4.10 Data Protection Impact Assessments (DPIAs)

Where any new projects or changes in practice require new processing of personal data, a DPIA is completed where required. DPIAs are mandatory for any new high-risk processing projects. Completing a DPIA allows us to identify and mitigate against data protection risks, plan for the implementation of any solutions to those risks, and assess the viability of a project at an early stage.

5. Information about people who use our website

Cookies on www.sivuh.ie; we want our online services to be easy, useful and reliable. Our website uses one cookie to maintain your current session. It stores no personal information and is not used for any other purpose. For more information visit https://www.sivuh.ie/Cookies.html

6. Security and where we store your personal data

In order to protect the privacy rights of data subjects, physical and technical security measures are in place to ensure all data collected and processed by SIVUH has protection that is consistent with privacy and data protection laws. Physical records are kept securely within SIVUH and may be archived in a secure storage facility until the end of their retention periods when they are due for destruction.

SIVUH promotes good information governance practices among its staff. SIVUH continually monitors and improves internal policies, procedures and information communications technology (ICT) security tools to ensure that all personal data is protected against theft, accidental loss, unauthorised access or alteration, erasure, use or disclosure. SIVUH conducts staff training to ensure that all staff are aware of their responsibilities in relation to the gathering, using, storing and disposing of personal information.

7. Retention of Data

We only keep personal information for a period that is deemed necessary to carry out the purpose for which it was originally collected, unless it is specifically required by law to keep your information for longer.

8. Rights of data subjects

We aim to ensure that all data subjects' rights are upheld. We promote transparency when it comes to how we collect, process and retain personal information. As a data subject, you have the right to:

- access and receive a copy of your personal data
- seek to rectify or update any inaccurate personal information held
- seek to have data deleted
- object to the processing of data
- withdraw consent
- request restriction

1. Access and receive a copy of your personal data

You are entitled to know if SIVUH holds any personal information belonging to you and to receive a copy of this information free of charge. Some restrictions may apply to your right of access as per Article 15 of the GDPR. Requests for records can be made by emailing foi.officer@sivuh.ie.

2. Rectification and accuracy of data

SIVUH endeavours to keep all personal information accurate and up to date. In certain circumstances, you are entitled to have rectified any personal information belonging to you if it is incorrect or out of date.

3. Deletion of data

Under certain circumstances, such as if the data collected is no longer needed by SIVUH, you may request in writing the deletion of your personal data. This right may be restricted if the personal information is deemed necessary for SIVUH to carry out its regulatory duties under the Health Acts 1947- 2007.

4. Objecting to the processing of data

It is possible that you will object to SIVUH processing your personal information. SIVUH may refuse your right to object if it affects SIVUH carrying out its regulatory duties under the Health Acts 1947-2007.

5. Request restriction of processing of your personal data.
This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

6. Withdraw consent at any time
You can withdraw your consent at any time, where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. This only applies if consent is the basis on which we process your data.

9. Contact details for Data Protection Officer (DPO) SIVUH

If you have any queries in relation to your personal data or data protection, please contact the SIVUH Data Protection Officer at the following:
Email: dpo@sivuh.ie or Tel: 021-4926100
Postal Address: South Infirmary Victoria University Hospital
Data Protection Office
Old Blackrock Road
Cork
T12 X23H

If you are unhappy with any aspect of how SIVUH has handled your personal information and would like to have the matter reviewed, you can contact our DPO by post, email or phone through the contact details above.

If you are unhappy with the outcome of the investigation by our DPO, you also have the right to make a complaint to the Data Protection Commissioner directly by:
Email: info@dataprotection.ie or Tel: 1890 25 22 31
Postal Address: Data Protection Commissioner
Canal House
Station Road
Portarlington
Co. Laois
R32 AP23