HEALTHCARE INSPECTORATE WALES (HIW) PRIVACY NOTICE

Your privacy is important to the Healthcare Inspectorate Wales as part of the Welsh Government and in line with General Data Protection Regulations (GDPR) we have developed a Privacy Notice that covers why we collect and use your information.

A. WHO WE ARE

Healthcare Inspectorate (HIW) is part of the Welsh Government. Our role is to regulate and inspect NHS services and independent healthcare providers in Wales against a range of standards, policies, guidance and regulations and to highlight areas requiring improvement.

B. WHAT WE DO

Inspect healthcare - We inspect NHS and independent healthcare services in Wales to check people are receiving good care

Investigate - We carry out reviews of healthcare organisations or services in response to concerns arising from a particular incident or incidents, dependent upon seriousness and/or frequency of occurrence.

Registration and ongoing regulation of registered services – We register and regulate independent healthcare services.

Review Service for Mental Health - We monitor the use of the Mental Health Act and protect the interests of people whose rights are restricted under that Act.

The Second Opinion Appointed Doctor Service - We administer the Second Opinion Appointed Doctor Service, which safeguards the rights of patients detained under the Mental Health Act who either refuse the treatment prescribed by the Approved Clinician or are deemed incapable of consenting.

C. WHY WE COLLECT AND PROCESS YOUR PERSONAL DATA

The information HIW collects, uses and processes is necessary to enable us to carry out tasks in the public interest and in the exercise of our official authority. The purpose of data collection and the types of personal information we hold is given below:

C.1 Investigation of Concerns and safeguarding issues.

In order to investigate a concern or safeguarding issue, we are required to collect the following personal data:

- name,
- date of birth,
- address,
- telephone number,
- email address,
- language and communication preferences,
- allegations of misconduct at work and protection and abuse allegations.

We also collect special category data such as:

- medical records and care and treatment plans.

Your information will be processed internally and only be passed to officers within the relevant departments who need to provide input into the handling of your complaint and our response. All information relating to complaints are administered and held on secure records management systems. We will share your information when there are potential risks to public, patient or staff safety, with regulatory bodies and relevant authorities/organisations.

Your information will be kept for 10 years after the date of the last document.

C.2 Special reviews and investigations, including homicide reviews.

In order to investigate a homicide, death in prison and undertake special investigations, we are required to collect the following personal data

- name,
- date of birth,
- address,
- telephone number,
- email address,
- police records,
- convictions,
- allegations of misconduct at work.

We will share your information when there are potential risks to public, patient or staff safety, with regulatory bodies and relevant authorities/organisations.

Your information will be kept for 15 years after the date of the last document.

C.3 Registration and ongoing regulation of registered services

In order to register and regulate independent healthcare services we are required to collect the following personal data for the registered manager and responsible individual:

- name,
- date of birth,
- home address (Registered Manager only),
- business address,
- telephone number,
- email address,
- language and communication preferences,
- financial information (bank account details),
- personal/professional references,
- convictions.

We also collect special category data such as:

- medical histories (Medical reference),

We will share your information when there are potential risks to public, patient or staff safety, with regulatory bodies and relevant authorities/organisations.

Your information will be kept for 7 years after the date of the last document.

C.4 Disclosure and Barring Service

To register as a registered manager or responsible individual to provide independent healthcare we are required to undertake a Disclosure and Barring Service (DBS) check. In order to complete this check we are required to collect the following personal data on behalf of the DBS:

- name,
- date of birth,
- gender,
- place of birth,
- birth certificate reference number and issue date,
- adoption certificate reference number and issue date,
- biometric residence permit reference number and issue date,
- marriage/civil partnership certificate number and issue date,
- HM Forces ID card reference number, and issue date,

- firearms licence reference number and issue date,
- email address,
- telephone number,
- national insurance number,
- driving licence number and issue date,
- passport number, including nationality and country of issue'
- Scottish vetting and barring number,
- current address (also previous addresses for the last 5 years),
- financial and social history documents, e.g. bank or building society statement, credit card statement, work permit or visa etc.

convictions.

On completion of a DBS check, we will destroy all personal information with the exception of the individual's name, DBS certificate number, date of issue and any convictions, after 7 years.

C.5 Take enforcement action

In the process of taking any enforcement action where applicable / required we may collect the following personal data

- name,
- address,
- telephone number,
- email address,

- PACE (Police and Criminal Evidence Act) notes and recordings,
- victim statements,
- covertly obtained evidence.

We will share your information when there are potential risks to public, patient or staff safety, with regulatory bodies and relevant authorities/organisations.

You information will be kept for 15 years after the date of the last document.

C.6 Inspection of services.

In order to carry out inspections of healthcare services, we may collect the following personal data:

- patient name,
- patient date of birth,
- patient gender,

- patient identification number,
- NHS commissioner of services being provided,
- staff names,
- staff roles,
- staff appraisal records,
- staff supervision records,
- staff DBS checks,
- staff photographs,
- staff recruitment/pre-employment checks, references, qualifications/professional body registration and employment history.

We may also collect special category data such as:

- patient information from medical records, care and treatment plans including diagnosis, risk, forensic type, treatment type and medication,
- details of detention if applicable,
- ethnicity, including religious/cultural needs.

HIW uses patient information in order to:

- track the effectiveness of care that a patient has received over time,
- reference any issues of ineffective or unsafe care when reporting back to healthcare providers.

HIW uses staff information in order to:

- ensure that necessary pre-employment checks have been carried out,
- evaluate whether staff have received relevant training and/or development,
- reference staff, if necessary, when reporting back to healthcare providers.

We will share personal information with regulatory bodies and relevant authorities/organisations when there are potential risks to public, patient or staff safety.

C.7 Statutory Notifications of death, unauthorised absence, serious injuries, outbreak of infectious disease, allegation of misconduct and deprivation of liberty

In order to investigate statutory notifications, we may collect the following personal data:

- name,
- date of birth,
- address,
- telephone number,
- email address.
- staff names,
- staff roles,
- staff appraisal records,
- staff supervision records,
- staff DBS checks,
- staff photographs,
- staff recruitment/pre-employment checks, references,
- qualifications/professional body registration and employment history,
- police records,
- convictions.
- allegations of misconduct at work and protection and abuse allegations,
- victims statements.

We may also collect special category data such as:

- ,
- medical histories (Medical reference),
- medical records and care and treatment plans,
- patient information from medical records, care and treatment plans including diagnosis, risk, forensic type, treatment type and medication,
- .

We will share your information when there are potential risks to public, patient or staff safety, with regulatory bodies and relevant authorities/organisations.

Your information will be kept for 10 years after the date of the last document.

C.8 Statutory Notification of IR(ME)R incidents.

We are responsible for monitoring compliance with the Ionising Radiation (Medical Exposure) Regulations(IR(ME)R)2017 to ensure that patients in Wales are protected when having treatment that requires exposure to ionising radiation. We will review incidents notified to us involving patients who may have been exposed to more ionising radiation than they should have.

In order to investigate statutory notifications, we may collect the following personal data:

- name,
- date of birth,
- address,
- telephone number,
- email address.
- staff names,
- staff roles,
- staff appraisal records,
- staff supervision records,
- staff DBS checks,
- staff photographs,
- staff recruitment/pre-employment checks, references,
- qualifications/professional body registration and employment history,
- Allegations of misconduct at work and protection and abuse allegations.

We may also collect special category data such as:

- medical histories (Medical reference),
- medical records and care and treatment plans,
- patient information from medical records, care and treatment plans including diagnosis, risk, forensic type, treatment type and medication,
  allegations,
- victim statements.

We will share your information when there are potential risks to public, patient or staff safety, with regulatory bodies and relevant authorities/organisations.

Your information will be kept for 10 years after the date of the last document.

C.9 Organisational record of each health board, NHS Trust and independent provider.

To achieve our goal of encouraging improvement in healthcare by doing the right work at the right time in the right place; we decide where to focus our activities on the basis of risk and intelligence. We hold the following personal data as part of our organisational records for NHS organisations:

- name,
- date of birth,
- address,
- telephone number,
- email address,
- language and communication preferences,
- allegations of misconduct at work and protection and abuse allegations

We also collect special category data such as:

- medical records and care and treatment plans,

.

We will share your information when there are potential risks to public, patient or staff safety, with regulatory bodies and relevant authorities/organisations.

Your information will be kept for 10 years after the date of the last document.

C.10 Second Opinion Appointed Doctor Service.

We administer the Second Opinion Appointed Doctor Service, which safeguards the rights of patients detained under the Mental Health Act. In order to carryout this function, we are required to collect the following personal data.

- patient name,
- patient date of birth,
- patient gender
- patient home address
- address of place of detention,
- patient language and communication preferences
- contact name of clinician,
- contact details of clinician, including telephone number and language and communication preferences,
- detaining authority.

We also collect special category data such as:

- medical records, diagnosis, care and treatment plans (including legal documents e.g. detention under the Mental Health Act),
- ethnicity.

We will only share your information with the clinical team who is caring for the patient and who already has access to this information legally.

Your information will be kept for 8 years after the date of the last document or visit.

C.11 Review Service for Mental Health.

We monitor the use of the Mental Health Act and protect the interests of people whose rights are restricted under that Act. In order to carryout this function we are required to collect the following personal data.

- patient name,
- patient date of birth,
- patient gender
- patient home address
- address of place of detention,
- patient language and communication preferences
- contact name of clinician,
- contact details of clinician, including telephone number and language and communication preferences,
- detaining authority.

We also collect special category data such as:

- medical records, diagnosis, care and treatment plans (including legal documents e.g. detention under the Mental Health Act).
- ethnicity.

We will only share your information with the clinical team who is caring for the patient and who already has access to this information legally.

Your information will be kept for 25 years after the date of the last document.

C.12 Respond to general correspondence.

In order to respond to general correspondence we record the following personal data:

- name
- address

- email address
- telephone number
- summary of correspondence
- language preferences

We will not share your information and will keep it for 12 months for audit purposes.

C.13 Organise events, meetings, launches and consultations.

In order to invite individuals to events and meetings and to take part in launches and consultations we may collect the following personal data.

- name
- email address
- home/work address
- telephone number
- dietary requirements
- accessibility and special requirements
- language and communication preferences

We will not share your information and will keep it for the period of the launch / consultation and on completion of the meeting/event.

D. WHO DO WE SHARE YOUR INFORMATION WITH

HIW has a number of information sharing agreements with other organisations that we work closely with. These agreements set out the rationale for information sharing to assist the organisations in meeting their common statutory objectives and to focus respective activities. They support the creation of work programmes which are complementary ensuring that there are clear processes in place for sharing information, risks and concerns. Where there are potential risks to public, patient or staff safety. HIW will share information with relevant authorities/organisations such as the police and local authority safeguarding boards. HIW will only share your personal data as set out in Section C

You can access the information sharing agreements by selecting the above link or accessing the documents on our website:
http://hiw.org.uk/about/workingwithother/mou/?lang=en

E. YOUR RIGHTS UNDER THE GENERAL DATA PROTECTON REGULATIONS (GDPR)

You have the right to:

- Have access to the personal data that HIW are processing about you,
- Require HIW to rectify inaccuracies in that data,
- The right (in some circumstances) to object to processing,
- The right for your information to be erased,
- Lodge a complaint with the Information Commissioner who is the independent regulator for data protection.

For further information about the data which HIW holds and its use, or if you wish to exercise your rights under GDPR, please contact the following:

Departmental Knowledge Information Manager
Healthcare Inspectorate Wales
Rhydycar Business Park
Merthyr Tyfil
CF48 1UZ

Email: HIW@gov.wales

Data Protection Officer
Welsh Government
Cathays Park
Cardiff
CF10 3NQ
Email; data.protectionofficer@gov.wales

For independent advice regarding the GDPR, please contact the following:

Information Commissioner's Office
Wycliffe House
Water Lane
WILMSLOW
CheshireSK9 5AF

Telephone: 01625 545 745 or 0303 123 1113
Website: www.ico.gov.uk