

Healthwatch Hertfordshire Information Governance Policy

This policy applies to all staff, trustees, volunteers and board members of Healthwatch Hertfordshire (HWH).

Purpose of this Policy

The aim of this document is to provide an overview of HWH's information governance and to ensure that information is shared between partner organisations in a legally compliant manner and appropriate format. The sharing of information especially in respect of personal and / or sensitive information relating to a partner organisation or member of the public must only take place within the legislative, statutory and common law context that affects the agencies party to any agreement.

Legislation, Guidance & Principles

This policy identifies the common principles and procedures to be adopted in the adoption or development of information sharing protocols. The key legislation and guidance currently relevant to the sharing and disclosure of information includes:

UK General Data Protection Regulation (UK GDPR)

The GDPR sets out principles of data protection which limit the reasons for which personal data may be obtained and specify how it can be used. Please refer to HWH's Data Protection policy for further detail.

The [UK GDPR](#) is the [retained EU law](#) version of the *General Data Protection Regulation* as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of [section 3](#) of the European Union (Withdrawal) Act 2018 and as amended by [Schedule 1](#) to the [Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2019 \(SI 2019/419\)](#).

It is defined in [section 3\(10\)](#) of the Data Protection Act 2018 (DPA 2018), supplemented by [section 205\(4\)](#). It includes the provisions of what was previously the [applied GDPR](#), unless the context otherwise requires.

With effect from 1 January 2021, organisations need to bear in mind that there are two legal texts to consider, where relevant: the UK GDPR as well as the DPA 2018.

The Caldicott Principles

HWH will apply the Six Caldicott Principles as detailed in the Caldicott Report 1997 to its information governance. Caldicott is the name given to a set of six principles, which resulted from a Government investigation, by Dame Fiona Caldicott into confidentiality and security of personal information within the NHS. These principles and new arrangements were first introduced into the Health Service but have, with effect from 2002, been introduced by the Government for Family Services records.

The updated Caldicott Principles are:

- Justify the purpose
- Do not use personal data unless it is absolutely necessary
- Use the minimum necessary personal data
- Access to personal data should be on a strict need to know basis
- Everyone with access to personal data should be aware of their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality.

Purposes for which information may be shared

HWH may need to share personal or sensitive data with third parties for the following purposes:

- Gathering the views and experiences of patients, service users and the public and making these views known
- Making reports and recommendations about the improvement of services
- Promoting and supporting the involvement of people in the commissioning, provision and scrutiny of local services
- Recommending investigation and special review of services
- Signposting and information to enable people to make informed choices
- Making the views and experiences of people known to Healthwatch England and other bodies.
- Legal requirements

Where there is a need for sharing personal or sensitive data with third parties, HWH will only transfer personal data to, or allow access by, third parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient.

HWH has a 'Standard Data Processing Agreement' document that is used as a baseline template for creating UK GDPR compliant information sharing protocols with third parties. When HWH is outsourcing services to a third party (including cloud computing services), they will identify whether the third party will process personal data on its behalf and whether the outsourcing will entail any third country transfers of personal data. In either case, it will make sure to include, in cooperation with the HWH Data Protection Officer, adequate provisions in the outsourcing agreement for such processing and third country transfers.

As outlined under the principles of UK GDPR, in cases where HWH needs to share information internally or with a third party, HWH will only transfer the minimum amount of personal data necessary for the particular purpose of the transfer, ensure adequate security measures are used to protect the personal data during the transfer (including password-protection and encryption, where necessary).

Principles guiding the sharing of information

HWH will apply the following key principles to the sharing of information between any parties:

- Information shared will be accurate, timely, secure and meet confidentiality standards
- Only information in accordance with the organisation’s legal, statutory and contractual duties, and that meets the requirements of any additional guidance will be shared
- All parties with which information is shared will have in place policies and procedures to meet the requirements for Data Protection, security and confidentiality. The existence of, and adherence to, such policies provides confidence that information shared will be transferred, received, used, held and disposed of appropriately
- HWH volunteers will be fully informed about the type of information that is recorded about them and how this will be processed
- HWH acknowledge their ‘Duty of Confidentiality’ to individuals. In requesting release and disclosure of information from other organisations, and/or agencies, staff will respect this responsibility and not seek to override the procedures, which the organisation has in place to ensure that information is not disclosed illegally or inappropriately.
- As a minimum, individuals will be informed at the point at which information is collected, if information is to be shared, the circumstances in which this could happen and who the information may be shared with. HWH will ensure written or verbal consent of the individuals is sought and provided before sharing information
- An individual’s personal information will only be disclosed where the purpose for which it has been agreed to share clearly requires that this is necessary in accordance with Data Protection principles and the ‘Need To Know’ principle. For all other purposes information should be anonymous
- Where it is agreed to be necessary for information to be shared, only the information needed will be shared and that would only be on a “need to know” basis
- HWH recognises that, subject to the appropriate safeguards, individuals have a right to know and be fully informed about information that is recorded about them
- HWH will ensure that all relevant staff are aware of, and comply with, their responsibilities with regard to both to the confidentiality of information about individuals who are in contact with HWH and to the commitment of HWH to share information

- Disclosure of personal information, which cannot be justified on legal or statutory grounds, whether intentionally or unintentionally, could be subject to disciplinary action
- Information which is already in the public domain will be freely shared between the parties

Reviewed and signed off with minimal changes on 21st April 2022:

Nuray Ercan

Signed by Nuray Ercan, as Company Secretary

Responsible Officer

Geoff Brown, Chief Executive