Tower Hamlets GP Care Group (THGPCG) Data Protection and Confidentiality Policy

Date Issued	10/07/2020
Date to be reviewed	Periodically or if statutory changes are required
Title	Data Protection and Confidentiality Policy
Supersedes	All previous Policies
This policy will impact on	All staff
Financial Implications	No change
Policy Area	Information Governance
Version No	1.0

Issued By	Quality, Safety & Governance Sub-Committee
Policy Review	Hamsa Hassan
Contact Details	hamsa.hassan@nhs.net
Effective Date	October 2018
Review Date	May 2021

Document History

	Committees / Groups / Individual	**Date**
Reviewed by	Service Leads, Quality, Safety & Governance	August 2018
Approved by	Chris Banks, Chief Executive Officer	September 2018
Reviewed by / Policy Review	Hamsa Hassan, Information Governance	July 2020
Accountable Director	Ruth Walters, Director of Quality and Assurance	July 2020
Approved by	Quality, Safety & Governance Committee	July 2020

Contents

Data Protection & Confidentiality Policy

1. Introduction

This document describes Tower Hamlets GP Care Group (THGPCG) policy on Data Protection (General Data Protection Regulations 2018/Data Protection Act 2018); NHS Code of Confidentiality and Caldicott requirements, and employees' responsibilities for the safeguarding of confidential information held both manually (paper records) and electronically.

THGPCG stores, retains and manages a large number of personal and confidential information relating to patients, service users, carers, the public and employees of THGPCG.

Data protection laws exist to strike a balance between the rights of individuals to privacy and the ability of organisations to use data for legitimate purposes.

The General Data Protection Regulation and Data Protection Act 2018 came into force on 25th May 2018 and supersedes the Data Protection Act 1998. The Regulation/DPA is concerned with "personal and sensitive data" about living, identifiable individuals which is "automatically processed or manually stored as part of a relevant filing system or accessible record". Typical examples are, Name, Address, DOB, and NHS Number.

The Regulation/DPA is divided to "Recitals" and "Articles" and works in two ways, giving individuals certain rights whilst requiring those who record and use personal information certain responsibilities. The Regulations incorporates the following *principles* which are required for any organisation processing data:

Article 5 Principles of processing personal data (GDPR)

Personal data shall be:

(a) **processed lawfully, fairly and in a transparent manner** in relation to the data subject ('lawfulness, fairness and transparency');

(b) **collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes**; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed ('data minimisation');

(d) **accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) **kept in a form which permits identification of data subjects for no longer than is necessary** for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or

statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) **processed in a manner that ensures appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

ALL STAFF HAVE A LEGAL DUTY TO PROTECT THE PRIVACY OF INDIVIDUALS

2. Scope

This policy covers all identifiable information created, processed and stored on living individuals, patients or staff. Throughout this document the term “patient” is used to refer to an individual who is receiving a service from THGPCG, and this term includes those people who are also known as “Service Users”, and “Clients”. Similarly, the terms “clinician” and “health professional” are used but should be interpreted as encompassing social care staff and health practitioners.

3. Responsibilities

THGPCG has established a structure to deliver information governance, to meet the requirements of data protection and confidentiality.

3.1 The Chief Executive has a duty to ensure that:

- staff are aware of the need to comply with the GDPR/DPA 18, in particular with the rights of patients wishing to access personal information and or their health records.
- staff are aware of requirements of the common law duty of confidence as set out in Confidentiality: NHS Code of Practice.
- arrangements with third parties who process personal data on behalf of THGPCG are subject to a written contract which stipulates appropriate security and confidentiality.

3.2 THGPCG’s Caldicott Guardian is responsible for agreeing and reviewing protocols for governing the transfer and disclosure of personal confidential data across THGPCG and supporting agencies.

3.3 The Senior Information Risk Owner (SIRO) has ultimate responsibility for the management and mitigation of risks associated with THGPCG’s information management processes. This responsibility is formally delegated from the Chief Executive via a letter of delegation. The SIRO shall:

- Be accountable for the management and protection of all Information Assets
- Take overall ownership of the Information Risk Management Policy
- Provide a focal point for managing information risks and incidents
- Lead on Business Continuity in the context of Information Risk
- Act as champion for Information Risk on the Board
- Advise the Board on the effectiveness of Information Risk Management
- Ensure that Information Risk Assessments and management processes are embedded
- Lead and foster a culture for protecting and using information and data;
- Lead communications on Information Governance and Security throughout the organisation

3.4 **The Data Protection Officer** has overall responsibility for managing and effectively implementing all activities necessary to achieve compliance with the GDPR/DPA 18 throughout THGPCG:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR/DPA 18 and other data protection laws
- To monitor compliance with the GDPR/DPA 18 and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (patients/staff)

3.5 **Together, the Director of Quality and Assurance and Information Governance Officers** main responsibility is to:

- Facilitate all the data protection and Caldicott functions within THGPCG to support the above
- Advise and update the THGPCG in relation to directives/guidance from the Information Commissioner and the Department of Health; NHS England; NHS Digital
- Maintain an up to date Notification under the GDPR/DPA 18 with the regulatory body (Information Commissioner's Office).
- Via the Information Governance Framework – ensure that the Caldicott Guardian, Data Protection Officer and Senior Information Risk Owner (SIRO) are informed of relevant issues and decisions are recorded

3.6 **Senior Operational/Clinical/Service Managers** are responsible for ensuring compliance with policies and that staff attend and pass the annual mandatory IG training, and breaches and issues raised by staff are acted upon. Managers are also responsible for ensuring that Information Asset Owners and Administrators are appointed

3.7 **The Information Governance Group**, is chaired by the SIRO and is the forum responsible for ensuring that the THGPCG complies with the GDPR/DPA 18. It meets bi-monthly – and reports to the Quality and Assurance Directorate, which reports to the THGPCG Board and Executive Management.

3.8 **All staff:**

- Adheres to this policy and all related Information Assets and processes to ensure compliance with the GDPR / DPA 2018 and any other relevant data protection legislation.
- Have the responsibility of ensuring that patients are informed about THGPCG's Privacy Notice – which details information processing and rights. This should be done at an appropriate time to the patient, taking into account their health and wellbeing at the time.
- Have a responsibility to inform the IG Team of any new use of personal data immediately.
- Maintains an appropriate level of awareness of the GDPR / DPA 2018 and to attend training as appropriate as identified by the Data Security Training Needs Analysis.
- Ensures that all personal data is accurate, relevant, up-to-date and used appropriately, for both electronic and manual Information Asset.

- Ensures that personal data is not removed from the THGPCG premises except where specifically required for the execution of legitimate functions of THGPCG and, then, only in accordance with appropriate policies.
- Ensures that all copies of personal data output, or obtained from the system whether electronic, recorded on paper, microfilm, or any other form, are securely and confidentiality managed and destroyed/erased when they are no longer required for THGPCG purposes.
- Failure to adhere to this policy and its associated procedures may result in disciplinary action.

4. Main Outline

The General Data Protection Regulations/DPA 2018: Principles and Practices to ensure compliance:

4.1 GDPR Article 5: Data Protection Principles:

1. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject [lawfulness, fairness and transparency]
2. Personal data shall be collected only for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes [purpose limitation]
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed [data minimisation]
4. Personal data processed shall be accurate and, where necessary, kept up to date [accuracy]
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed [storage limitation]
6. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical of organisation measures [integrity and confidentiality]

4.2 **Under the GDPR/DPA 18, data subjects have certain rights**, which must be upheld:

- Be informed - through privacy notices (see below) and Data Protection Impact Assessments
- Access - Subject Access Requests [Refer to Subject Access Request Policy)
- Rectification - to have inaccuracies corrected
- Erasure - to have information erased (right to be forgotten). *However, this does not automatically apply to NHS clinical records and should an individual make a request to prevent processing then depending on the individual circumstances, THGPCG would have to make a judgement based on the risk to the individual or others whether it was right to provide a service. This decision can only be made by the Caldicott Guardian.*
- Object to processing (e.g. direct marketing)
- Prevent automated decision-making and profiling
- Data portability – have information provided in electronic format and not hinder the data subject's transmission of personal data to a new data controller
- Consent to process - silence, pre-ticked boxes or inactivity does not constitute consent to process

4.3 Privacy Notice

GDPR requires data controllers to provide certain information to people whose data they hold and use; this is known as a Privacy Notice. THGPCG publishes it's Privacy Notices on their

public website: https://www.gpcaregroup.org/section/462/Footer/page/f5c7cbd3-1848-4a68-9e35-1cf57885a368/Privacy-Policy

4.4 Lawful basis for processing

GDPR/DPA 18 requires that all organisations identify the legal basis for any processing (i.e. collecting, using, storing etc.) of personal or special category information relating to data subjects (patients and staff).

As a publicly funded GP federation, the legal basis for processing information is GDPR Article 6 1(e) - 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. It is important to note that,

Special Categories of personal data - examples of these are; racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union membership; processing of genetic data; biometric data (for the purpose of uniquely identifying a natural person); data concerning health; data concerning a natural person's sex life or sexual orientation:

Article 9 2(h) - 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 on the basis of Union or Member State law or pursuant to contract with a health professional

For more information relating to lawful basis's – please refer to Appendix 1.

4.5 Caldicott Principles for handling personal confidential data:

1. **Justify the purpose -** Every proposed use or transfer of personal confidential data within or from an organization should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate Guardian.

2. **Do not use personal confidential data unless it is absolutely necessary -** Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. **Use the minimum necessary personal confidential data -** Where the use of personal confidential data is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

4. **Access to personal confidential data should be on a strict need-to-know basis -** Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one information flow is used for several purposes. Health care organisations should be aware of the research conducted within the organisation and should ensure research teams are accountable to them

5. **Everyone with access to personal confidential data should be aware of their responsibilities** - The organisation must ensure that those handling personal confidential data, both clinical and non-clinical staff, are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. **Understand and comply with the law -** Every use of personal confidential data must be lawful. The Caldicott Guardian, is responsible for ensuring that the organisation complies with legal requirements.

7. **The duty to share information can be as important as the duty to protect patient confidentiality -** Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

   The Health and Social Care (Safety and Quality) Act 2015 includes a legal duty requiring health and adult social care bodies to share information where this will facilitate care for an individual.

4.6 'Confidentiality: NHS Code of Practice'
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf was published by the Department of Health following major consultation in 2002/2003. The consultation included patients, carers and citizens; the NHS; other health care providers; professional bodies and regulators. The guidance was drafted and delivered by a working group made up of key representatives from these areas.

The Code of Practice is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to the use of their health records. This document uses the term 'staff' a convenience to refer to all those to whom this code of practice should apply. Whilst directed at NHS staff, the Code is also relevant to any one working in and around health services. This includes local authority staff working in integrated teams and private and voluntary sector staff.

This document:

a. introduces the concept of confidentiality;
b. describes what a confidential service should look like;
c. provides a high level description of the main legal requirements;
d. recommends a generic decision support tool for sharing/disclosing information;
e. lists examples of particular information disclosure scenarios.

There is also additional guidance: **Supplementary Guidance - Public Interest Disclosures** – published in November 2010, this provides guidance to NHS staff in making what are often difficult decisions on whether a breach of patient confidentiality can be justified in the public interest.

Following the publication of the Caldicott Review in March 2013, the Health & Social Care Information Centre published "A guide to confidentiality in health and social care" which identified five rules for treating confidential information with respect:

Rule 1: Confidential information about service users or patients should be treated confidentially and respectfully

Rule 2: Member of a care team should share confidential information when it is needed for the safe and effective care of an individual

Rule 3: Information that is shared for the benefit of the community should be anonymised

Rule 4: An individual's right to object to the sharing of confidential information about them should be respected

Rule 5: Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed

The full version can be found at: https://www.gov.uk/government/publications/the-information-governance-review

4.7 Patient Confidentiality

Health information is collected from patients in confidence and attracts a common law duty of confidence until it has been effectively anonymised. This legal duty prohibits information use and disclosure without consent – effectively providing individuals with a degree of control over who sees information they provide in confidence. This duty can only be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification.

On admission and/or on first contact with the service user for a particular purpose, all patients should be asked which relatives, friends or carers they wish to reveal information regarding treatment and progress, and those they specifically **do not** give permission to reveal information. This information must be recorded in the clinical records – i.e. electronic patient systems, or in the paper records.

In cases where relatives have been heavily involved in patient care, the patient must be explicitly informed as to what level these relatives can be kept informed. This is particularly important in cases where relatives are requesting information on the patient's condition, perhaps before the patient has been informed.

It is always recommended though, that research is anonymised in the first instance. If, for research purposes, staff might screen patients' records to identify any potential research participants with the Consultants permission. Patients may also be approached by staff regarding participation for a particular research study in order to obtain consent.

In the event of the patient being unable to give permission the Mental Capacity Act 2005 must be followed. Staff should refer to the Mental Capacity Act Policy and procedures for detail.

In all cases, the wishes expressed must be appropriately documented in the patient's clinical records.

4.8 Staff Confidentiality

All staff are required to keep any information confidential regarding patients and staff, only informing those that have a need to know. In particular, telephone conversations and electronic communications should be conducted in a confidential manner, and discretely.

Confidential information must not be disclosed to unauthorised parties without prior discussion and confirmation with a senior manager in THGPCG. Staff must not process any personal information in breach of GDPR/DPA 18. Further advise can be sought from a senior manager or the Information Governance Team.

Staff must not access patient or staff information on any system (electronic or paper) that relates to family (including spouses; children; parents etc.) or friends, even if it is considered to be within their role in the organisation.

Any breaches of these requirements will potentially be regarded as serious misconduct and as such, may result in disciplinary action.

All staff have a confidentiality handbook as part of their induction pack. THGPCG also has an approved Data Protection and Confidentiality clause in all contracts with 3rd party contractors and suppliers who process personal information.

4.9 Exemptions to confidentiality

In certain circumstances personal information may be disclosed and guidance is outlined below. However, it is vital in each case that staff make an assessment of the need to disclose the information and document that the information has been released to whom and for what reason. If they are in any doubt, they should seek advice from their Team Manager/Senior Clinician, Information Governance or the Caldicott Guardian.

4.10 Disclosing Information against the Subject's wishes

The responsibility to withhold or disclose information without the data subject's consent lies with the senior manager or senior clinician involved at the time and cannot be delegated.

Circumstances where the subject's right to confidentiality may be overridden are rare. Examples of these situations are:

- Where the subject's life may be in danger, or cases in which s/he may not be capable of forming an appropriate decision
- Where there is serious danger to other people, where the rights of others may supersede those of the subject, for example a risk to children or the serious misuse of drugs
- Where there is a serious threat to the healthcare professional or other staff
- Where there is a serious threat to the community

In other exceptional circumstances, based on professional consideration and consultation.

The following are examples where disclosure without consent is required:

- Births and deaths - National Health Service Act 1977
- Notifiable communicable diseases - Public Health (Control of Diseases) Act 1984
- Poisonings and serious accidents at the work place - Health & Safety at Work Act 1974
- Terminations - Abortion Regulations 1991
- Child abuse - Children's Act 1989 and The Protection of Children Act 1999
- Drug Addicts - Drugs (Notification of Supply to Addicts) Regulations 1973
- Road traffic accidents - Road Traffic Act 1988
- Prevention/detection of a serious crime e.g. terrorism, murder - The Crime and Disorder Act 1998

If in doubt, staff should seek guidance, in confidence, from the senior Clinician/Senior Manager, Information Governance or the Caldicott Guardian.

THGPCG will support any member of staff who, after using careful consideration, professional judgement, and has sought guidance from their manager, can satisfactorily justify and has documented any decision to disclose or withhold information against a patient's wishes.

4.11 Non–Disclosure of personal information contained in a health record

An individual requesting access to their health records may be refused access to parts of the information if an appropriate clinician deems exposure to that information could cause physical or mental harm to the data subject or a third party. Clinicians should be prepared to justify their reasons in a court of law if necessary. In all cases reasons for non-disclosure must be documented.

Where access would disclose information relating to or provided by a third party, consent for release must be sought from the third party concerned, unless that third party is a health professional who had provided the information as part of their duty of care. Where the third party does not consent, the information may be disclosed provided the identity of the third party is not revealed. The Information Commissioner's Code of Practice suggests that this might be done by omitting names and identifying particulars from the records. Care should be taken to ensure that the information if released is genuinely anonymous.

Further information can be found from THGPCG's Subject Access Request (SAR) Policy found on the shared drive on Sharepoint.

The Information Commissioner's Guide provides guidance on issues of law concerning the right of access to personal data: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

4.12 Personal Identifiable Data in Medical Research

All project based research within THGPCG must comply with the Data Protection & Caldicott Guardian Principles as set out within this Policy, be registered by the Research and Development Department and undergo review through the NHS Health Research Authority (HRA) approval process to provide assurance to THGPCG, our patients and the public that all research meets the necessary legal and compliance standards.

4.13 Data Protection Impact Assessment Procedure and Template

All projects and processes that involve processing personal information or intrusive technologies give rise to privacy issues and concerns. To enable THGPCG to address the privacy concerns and risks, the GDPR/DPA 18 requires a Data Protection Impact Assessment (DPIA) be completed, and signed off by the Data Protection Officer and/or the Information Governance Team. THGPCG's DPIA template can be found by contacting THGPCG's Information Governance Team.

5. Training requirements

All staff are required to complete the annual mandatory Information Governance Training, which includes topics on data protection and confidentiality. Monthly reports will be provided to operational managers to ensure compliance, and this will be monitored via the Governance and Performance Group.

6. Monitoring Compliance

This framework and the associated controls: policies, protocols, and procedures - will be monitored routinely by the Information Governance Team and Risk Management System. The information governance risk register will be reviewed on a regular basis and additionally in response to any information incident or enforcement action by the Information Commissioner's Office. Information risk management is a key component of wider assurance and control in setting the priorities for the information governance work plan. Information Asset Owners, assisted by Information Asset Administrators, will be required to routinely review the risks and information flows associated with the information assets utilised to fulfil the business functions and activities within their remit.

Non-Compliance:

By not complying with these standards explained in this policy can result in disciplinary action. All staff are reminded that this policy covers a variety of aspects of legal and legislative compliance, that individuals are all responsible for. Failure to maintain these standards is taken seriously and can result in criminal proceedings being made against the individual as an unlawful act. These include but are not limited to:

- Common law duty of confidentiality
- Computer Misuse Act 1990
- Data Protection Act 2018
- Freedom of Information Act 2000
- Human Rights Act 1998
- Public Records Act 1958
- Health and Social Care Act 2012
- Care Act 2014
- General Data Protection Regulation (EU) 2016/679

7. Dissemination and Implementation

Upon approval, this policy will be shared with all members of staff through the 'all staff' email, and also updated on THGPCG intranet page. A team and management briefing will be provided to support this dissemination.

Appendix 1: GDPR/DPA 18 Processing – legal basis

- **Personal data** – any information relating to an identifiable person who can be directly or indirectly identified – name; identification number, location data or online identifier
    - Personal data that has been pseudonymised can fall within the scope depending on how difficult it is to attribute the pseudonym to an individual

Lawfulness of processing **personal data** – Article 6

6; 1(a)	the data subject has given **consent** to the processing of his or her personal data for one of more specific purposes:
6; 1(b)	processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
6; 1(c)	processing is necessary for compliance with a legal obligation to which the data controller is subject
6; 1(d)	processing is necessary in order to protect the vital interests of the data subject or of another natural person
6; 1(e)	**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** ***see below for detail of legal obligations**
6; 1(f)	processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

***6; 1-e – legal obligations**

- Health and Social Care (Quality & Safety) Act 2015
- Health & Social Care Act 2012
- Care Act 2014
- The Children Act 1989
- The Children Act 2004
- Childcare Act 2006
- Children (Leaving Care) Act 2000
- Children and Families Act 2014
- National Health Service Act 1977
- National Health Service Act 2006
- Education Act 2002
- Special Education Needs and Disability Regulations 2014
- Localism Act 2011
- Immigration and Asylum Act 1999
- Crime and Disorder Act 1998

]

Sensitive data – "special categories of personal data"
Article 9 – Processing of special categories of personal data

Racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union membership; processing of genetic data; biometric data (for the purpose of uniquely identifying a natural person); data concerning health; data concerning a natural person's sex life or sexual orientation – SHALL BE PROHIBITED ***[see below]

1. Paragraph 1 shall NOT APPLY if one of the following applies:

2 (a)	**The data subject has given EXPLICIT consent to the processing of those personal data for one or more specified purposes**, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject
2 (b)	Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, in so far as it is authorised by Union or member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject
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 *[Capacity Act would apply – or if the person is at risk i.e. Mental Health Act Assessment]*
2 (d)	Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects
2 (e)	Processing relates to personal data which are manifestly made public by the data subject
2 (f)	Processing is necessary for the establishment, exercise or defence or legal claims or whenever courts are acting in the judicial capacity.
2 (g)	Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

2 (h)	**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 on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3** *Paragraph 3: Personal data referred to in para 1 may be processed for the purposes referred to in point (h) of para 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies*
2 (i)	Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, particular professional secrecy; or
2 (j)	Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject