Item No: 13

Meeting Date: **Wednesday 9th May 2018**

Glasgow City Integration Joint Board

Report By: **Sharon Wearing, Chief Officer, Finance and Resources**

Contact: **Fiona Lockhart, Business Development Manager**

Tel: **0141 287 8873**

GENERAL DATA PROTECTION REGULATIONS (GDPR) REQUIREMENTS FOR INTEGRATION JOINT BOARD

Purpose of Report:	To provide the IJB with an overview of the changes and implications arising from new Data Protection laws and the implementation of Public Records (Scotland) Act 2011.

Background/Engagement:	To provide an outline of the impact of these changes for the IJB and relates processes

Recommendations:	The Integration Joint Board is asked to: a) note the actions outlined in the report; b) read and note the requirement to comply with the attached guidance; and c) approve the proposed arrangements for appointment of a Data Protection Officer and application of GCC processes to data handling and record management activities.

Relevance to Integration Joint Board Strategic Plan:

Page 4 Description of IJB as distinct legal entity. This paper addresses one aspect of the responsibilities of IJB acting in that capacity.

Implications for Health and Social Care Partnership:

Reference to National Health & Wellbeing Outcome:	None

Personnel:	Potential resource implications to support the additional workload from complying with the new act.

Carers:	None

Provider Organisations:	Potential implications in terms of our interactions and ensuring all personal data is share in line with the new act.

Equalities:	None

Financial:	Potential financial implications for the organisation if new act is not administered as it will lead to fines.

Legal:	Legal requirement to implement.

Economic Impact:	None

Sustainability:	None

Sustainable Procurement and Article 19:	None

Risk Implications:	Financial and reputational risk for the organisation.

Implications for Glasgow City Council:	As above.

Implications for NHS Greater Glasgow & Clyde:	As above.

Direction Required to Council, Health Board or Both	Direction to:	
	1. No Direction Required	✓
	2. Glasgow City Council	
	3. NHS Greater Glasgow & Clyde	
	4. Glasgow City Council and NHS Greater Glasgow & Clyde	

1. Background

1.1 Data Protection laws are changing on 25th May 2018. EU General Data Protection Regulations (GDPR) come into force on that date. A new UK Data Protection Bill is currently under parliamentary scrutiny. When enacted this will repeal and replace the existing Data Protection Act (1998) however GDPR do have immediate effect in U.K law when enacted.

1.2 The legislation introduces new rules on how we collect and process personal data to ensure individuals have greater control and privacy rights for their information we hold. It shortens timescales for certain processes and significantly increases penalties for failure to comply.

1.3 The new legislation also notably changes the fundamental relationship between data subjects and statutory authorities that are responsible for health and social care such that consent is no longer the legal basis for processing in most cases and instead specific statutory duties, powers and the need to manage health and social care systems (a new and specific provision) forms the fundamental legal basis for processing of personal data.

1.4 This is balanced by a need for greater transparency. Formal notifications of the nature of, reason for and parties involved in data processing and data sharing are mandatory. These are referred to as Privacy notices.

1.5 Because the IJB is a statutory authority and Data Controller then it is subject to these new regulations (and the new Data Protection Act when that is enacted). However, the IJB in practice handles very little personal data and the impacts on the IJB specifically, as opposed to the partner organisations, is anticipated to be quite limited.

1.6 There are a wide range of activities across the Council family and NHS aimed at putting suitable arrangements in place in readiness for these changes. These are being progressed within the Partnership.

1.7 A more limited range of activities will require to be progressed for IJB itself to ensure compliance with the new legislation. All members should have awareness of these changes.

2. Summary of changes for the Council and NHS

Within both organisations the following changes will be implemented to ensure compliance with the new legislation. A range of activities have been progressed include internal communications, staff awareness and training, review of all documentation and the creation of Privacy Statements for all key services.

2.1 **Breach notifications** – Breaches of personal data must be notified to the Data Protection Regulator within 72 hours and if high risk then also the subject.

2.2 **Fines** – Higher fines apply if the rights of individuals are breached - 4% of global annual turnover which is up to £80 million for GCC.

2.3 **Rights of the data subject** – There are new rights for individuals to have their personal data erased entirely. We are required to justify any refusal.

2.4 **Subject Access requests** – We need to respond within 1 month (currently 40 days) and we can be fined if late in responding.

2.5 **Privacy by design** – Explicit principles are introduced for the minimum collection of personal data and strict rules on the collection, storage and recording of information. There will be a requirement for us to review and change all paper and electronic forms and to ensure standardisation of processes to minimise risk. These changes will link to document management and file retention procedures. New and existing processes may be subject to 'Data Protection Impact Assessments'.

2.6 **Consent** – We must be clear whether relying on consent, contractual obligations or statutory functions as a basis for processing. We should not however seek consent if there is a 'power imbalance' that restricts the subject's free choice but should instead look to our statutory functions as the fundamental legal basis for processing. If relying on consent it must be explicit, freely given and informed.

2.7 **Fair processing notices (Privacy Statements)** – Data must be processed fairly and lawfully. We will need an explicit and extensive process of informing the public of what personal data we process, why and with whom we share the data. Privacy Statement will be created for all our services confirming these arrangements.

2.8 **Data Protection Officer** – There is a new mandatory requirement for all public authorities to create a post of DPO. Both GCC and NHS will be separately appointing such a position.

2.9 **Clear reporting processes and management of our systems** – We must establish clear reporting, governance and compliance arrangements to evidence adherence to the act.

3. Key Actions for IJB

3.1 **Public Records Plan** - as part of existing legislation - The Public Records (Scotland) Act 2011 - we are required to establish an IJB records management plan and submit this by September 2018.

Currently all IJB information is held on the Council's Electronic Document Records Management System (EDRMS) so these records require a management plan to be established outlining details of the file location, what information is held and the retention periods for the storage of this data.

3.2 **Fair processing notice** - a Privacy Statement must be created for the IJB which will outline what personal data the IJB processes and why, the legal basis for processing, how this information is stored and retained and with whom it is shared.

3.3 **Data Protection Officer** – A Data protection Officer must be appointed meeting certain criteria. There is no barrier to a Data Protection Officer acting for more than one statutory body. Given that any personal data processed by IJB is likely to be held on GCC Information systems and one of the primary roles of the DPO is the handling of Data Breaches then it is proposed that the IJB Data Protection Officer should be Dr Kenny Meechan, who will also act as DPO for Glasgow City Council.

3.4 **Clear reporting and data handling processes and management of our systems** – given that the records managed with the IJB Records Management Plan will be hosted on GCC systems and that (if accepted) the Data Protection Officer will also act for GCC as regards any personal data being processed, it is further proposed that (a) the arrangements for records management and execution of the DPO role would follow processes established by GCC and (b) any actions or functions arising (such as breach reporting or exercise of data subject rights) would be discharged according to those procedures, following the council process. It is anticipated that there will minimal requirement to discharge such functions given the limited handling of personal data by IJB.

3.5 To assist members to gain an understanding of the changes attached are copies of NHS Greater Glasgow and Clyde and Glasgow City Council guidance. This provides members with awareness and further information of the new arrangements and processes to support them in their Board role.

4. Recommendations

4.1 The Integration Joint Board is asked to:

a) note the actions outlined in the report;
b) read and note the requirement to comply with the attached guidance; and
c) approve the proposed arrangements for appointment of a Data Protection Officer and application of GCC processes to data handling and record management activities.

GET READY – data protection law is changing

What is the Data Protection Act?

The current Data Protection Act (1998) regulates the way we handle and process personal data that we hold. This will be replaced by a new data protection law on 25 May 2018 – it will introduce new rules on how we collect and process personal data.

This leaflet will help you understand what is changing and what this means for the council family.

We have a legal requirement to comply with all elements of the Data Protection Act.

Breaching data protection rules is a very serious matter and can incur substantial fines and other sanctions.

What is Personal Data?

Personal data – this is information which relates to a living individual who can be identified from the information itself or by linking it with other information.

For example:

- a person's name and address
- an online profile
- a member of staff's HR record
- records relating to individual's such as school pupils or service users.

The new Act recognises '**special categories' of personal data**. These include:

- health information
- social care and criminal offences
- genetic and biometric data (where processed to uniquely identify an individual)
- personal matters such as a person's
  - racial or ethnic origin
  - sexual orientation
  - sex life
  - religious or philosophical beliefs
  - political opinions
  - trade union membership.

What is changing?

The rules around processing personal data are more demanding – particularly if we do so without the individual's consent.

The new Data Protection Act will **give individuals more rights and control** over how their personal data is handled by organisations such as the council and our Arm's Length External Organisations (ALEOs).

The new Data Protection Act will mean that we need to:

➢ appoint a Data Protection Officer	➢ notify our customers and the data protection regulator when there is a breach of personal data
➢ introduce new documenting procedures	➢ be much more open with our customers about what we do with their data
➢ make sure we only use the minimum amount of personal data needed to get the job done	➢ recognise that we won't ask for consent as much as we do now – much processing will be in order to carry out our statutory functions. If consent is still required, the rules around this are much stricter
➢ perform risk assessments	➢ strengthen our rules for deleting and removing personal data

Why is it important to get it right first time?

The new Data Protection Act will introduce very hefty financial penalties for a breach of data protection:

- we will only have 72 hours after a breach of personal data has been discovered to notify the data protection regulator
- the fines are substantial – up to £17 million or 4% of global annual turnover – which for the council could be up to £80 million.

LOST INFORMATION – REPORT IT IMMEDIATELY

If you have lost personal information, or have concerns about a Service User's personal information, you should **report it** to your line manager immediately so that they can email databreach@glasgow.gov.uk

For more information speak to your manager to access Connect at Know Your Council/ #SafeGlasgow/Keeping our Information Safe/Protecting Information/Data Protection

#SafeGlasgow

DATA Protection
It's changing

NHS GG&C Guidance

Appendix 2

General Data Protection Regulation Roadshows Schedule

On May 25th the existing Data Protection Act is replaced with a new set of regulations known simply as GDPR (General Data Protection Regulation). NHSGGC has a legal requirement to comply with the new Regulation.

In addition to other activity already underway to ensure compliance, the Information Governance Team are hosting a number of Roadshows which are open to all staff. These short presentations are aimed to give you an understanding of the main changes in the legislation and how this may affect you when handling and processing personal data.

Events have been scheduled as follows:

Venue	Date	Time	Room
QEUH Campus	16/3/18	10am – 11am	Laboratory Medicine Building, Ground floor L0/A/009 Seminar Room 1
	26/4/18	10am – 11am	Laboratory Medicine Building, Ground Floor L0/A/010 Seminar Room 2
Gartnavel Admin Building	19/3/18	3.30pm – 4.30pm	Ground Floor GRH Admin Boardroom
	16/4/18	10am – 11am	Ground Floor Meeting Room 1
New Victoria	29/3/18	9.30am – 10.30am	ADM 2.16B Conference Room (Level 2 Admin Corridor)
	20/4/18	3.30pm – 4.30pm	ADM 2.16A Conference Room (Level 2 Admin Corridor)
Stobhill Hospital,	20/3/18	3.30pm – 4.30pm	Ground Floor Seminar Room 6
	24/4/18	10am – 11am	Ground Floor, Seminar Room 5
West Glasgow,	23/3/18	10am – 11am	CS Block Main Tower, 4th Floor Meeting Room 3 (Access Code 1952Y)

	30/4/18	10am – 11am	CS Block Main Tower, 4th Floor Meeting Room 3 (Access Code 1952Y)
Glasgow Royal Infirmary	27/3/18	10am – 11am	Level 1, Video Conference Room
	27/3/18	3pm – 4pm	Level 1, Video Conference Room
	2/5/18	3pm – 4pm	Level 1, Video Conference Room
Vale Centre for Health & Care, First Floor	3/4/18	10am – 11am	Seminar/Meeting/Training Room G1/02
QEUH	6/4/18	10am – 11am	Level 1 Stroke Ward Seminar Room STW-011
	6/4/18	2.30pm – 3.30pm	Level 1 Stroke Ward Seminar Room STW-011
	10/4/18	10am – 11am	Level 3 FMA3-008 Core D FM Meeting Room
	18/4/18	10am – 11am	Level 1, Stroke Ward Seminar Room STW-011
Royal Hospital for Children	12/4/18	10am – 11am	Level 3, Seminar Room GWS-027

NB: To help manage room capacity, please email Jacqueline.Henderson2@ggc.scot.nhs.uk to register your interest in attending.

The General Data Protection Regulation

Data Protection law is changing on 25 May 2018.

GDPR strengthens the obligations and accountability on organisations, like NHSGGC, to handle personal data in a transparent and secure manner. Its fundamental principle however is to increase the rights individuals have over how organisations manage the personal information they hold about them.

This Factsheet will provide you with details on what these enhancements are and what they mean for you and how you handle peoples' personal information.

IMPORTANT

It is important to note that the reform to the existing Data Protection Act 1998 is being brought by the EU's General Data Protection Regulation (GDPR).

The Government has confirmed the UK's decision to leave the EU will not affect the commencement of the GDPR. The Government is introducing measures related to this and wider data protection reforms in a Data Protection Bill.

GDPR introduces new rules that regulate how we handle and process the personal data that is entrusted to us. NHSGGC has a legal requirement to comply with the new Regulation.

Although like many organisations NHSGGC has already adopted privacy processes and procedures compliant under the existing legislation, the GDPR introduces a number of new requirements that if breached can incur substantial fines or other regulatory action.

The overall purpose of the new regulation is to increase the rights individuals have over how organisations manage the personal information they hold about them. It also strengthens the obligations and accountability for organisations to handle personal data in a transparent and secure manner.

A summary of the key changes are:

The right of access (Subject Access Requests)

The current £10 fee to administer a request for non-clinical personal information will be removed as will the current fee of up to £50 for providing a copy of clinical information – all personal, and the information must be provided free of charge.

The statutory time for responding to a request for personal information is reduced from 40 days to one month.

Data Protection Officer

Public authorities, such as NHSGGC must appoint a Data Protection Officer (DPO). The DPO's role is to:

- Inform and advise NHSGGC about its obligations under the new regulations, including staff training and awareness
- Monitor NHSGGC's compliance with GDPR
- Be the first point of contact for the Information Commissioners Office

Isobel Brown is our Data Protection Officer. Email: Isobel.Brown@ggc.scot.nhs.uk or Tel: 0141 355 2020.

Individual rights are enhanced under the new regulations:

- **The right to be informed** - individuals have the right to be informed of why we are collecting/holding data about them, and how that data will be used.
- **The right of access (subject access requests)** – individuals have the right to access the data we hold about them.
- **The right to rectification** – the right to have personal data rectified if inaccurate or incomplete.
- **The right to erasure (right to be forgotten)** – the right to have personal data erased and to prevent processing in specific circumstances.
- **The right to restrict processing** – individuals have the right to 'block' or to suppress processing of personal data.
- **The right to data portability** – the right in certain circumstances for individuals to obtain and reuse their personal data for their own purposes across different services.
- **The right to object** – the right to object to processing of data based on legitimate interests of the organisation, direct marketing or for the purposes of scientific/historical research and statistics.
- **Rights in relation to automated decision making and profiling** – individuals have the right not to be subject to a decision based on our automated processing of their personal information.

The new data protection regulations change the way we seek and record consent from individuals. GDPR states that:

- There needs to be a clear indication of consent and must involve an affirmative action
- Consent should be captured separately from other terms and conditions
- Consent should not be a precondition of signing up to a service
- Pre-ticked boxes are specifically banned from use
- Clear records must be kept demonstrating consent
- Individuals have the right to withdraw consent, we must tell them about their right, and offer easy ways for consent to be withdrawn

NB. Organisations, like NHSGGC must have a valid lawful basis for processing personal information. This is not a new requirement, and the lawful bases listed under GDPR are broadly similar to the old conditions for processing, however there are some differences. Consent is only one of 6 valid lawful bases that can be relied upon.

The biggest difference impacts public authorities, like NHSGGC, where we now need to consider the new 'public task' lawful basis first for most of our processing, and we will have more limited scope to rely on consent or legitimate interests. Activity is underway to establish what the valid lawful basis is for all of our processing and update our documentation and processes accordingly.

It is unlawful under the new regulations not to undertake 'Privacy by Design' at the beginning of a business change, such as a new business process. Data Protection Impact Assessments (DPIA's) will assist in meeting that requirement:

- **We need to conduct DPIA's when:**
  - Using new technologies
  - Processing is likely to result in a high risk to the rights and freedoms of individuals

- **DPIA's should contain:**
  - A description of processing operations and the purposes, including where applicable, the legitimate interests pursued by a controller, such as NHSGGC
  - An assessment of the necessity and proportionality of the processing in relation to the purpose
  - An assessment of the risks to individuals
  - Measures in place to address associated risks
  - A DPIA template will be available for staff to use if required

GDPR introduces a duty on us to report certain types of personal data breach to our supervisory authority, the Information Commissioner (ICO). Additionally, if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, then we must also inform those individuals without undue delay.

Where deemed appropriate, we must:

- Report the breach to the ICO within 72 hours of becoming aware of it
- The Breach Notification should:
  - Describe the nature of the breach including;
    - The categories and approximate number of individuals concerned; and
    - The categories and approximate number of personal data records concerned
  - Provide the name and contact details of our DPO
  - Describe the likely consequences of the breach
  - Give a description of the measures taken, proposed to be taken, and where appropriate the measures taken to mitigate any possible adverse events.
- Failing to notify a breach to the ICO can results in a significant fine up to 10 million Euros or 2% of turnover.
- All relevant breaches will be reported to the ICO by the Data Protection Officer

GDPR introduces significant increased sanctions for non-compliance

Besides the power to impose fines, the ICO has a range of corrective powers and sanctions to enforce the GDPR. These include issuing warnings and reprimands; imposing a temporary or permanent ban on data processing; ordering the rectification, restriction or erasure of data; and suspending data transfers to third countries.

What are we doing to prepare for these mandatory changes:

Activity is already taking place across NHSGGC to get us ready for this change. You and some of your colleagues may already be involved.

We are updating all our policies, procedures, leaflets and documentation. For example our Privacy Notices, which we give to our Patients as part of their appointment pack, has been updated to include all the information now required. Our Subject Access Rights Policy has been updated to reflect the new requirements and our procedures adapted to deal with such requests going forward.

Our Safe Information Handling LearnPro modules are being updated and will be launched shortly. Roadshow presentations open to all staff are touring our Health Board premises – date and venue information available here.

For further information please contact the Information Governance Department at data.protection@ggc.scot.nhs.uk

The General Data Protection Regulation

Individual Rights

Data Protection law is changing on 25 May 2018.

GDPR strengthens the obligations and accountability on organisations, like NHSGGC, to handle personal data in a transparent and secure manner. Its fundamental principle however is to increase the rights individuals have over how organisations manage the personal information they hold about them.

The GDPR creates some new rights for individuals and strengthens some of the rights that exist under the Data Protection Act 1998. This Factsheet will provide you with details on what these enhancements are and what they mean for you and how you handle peoples' personal information.

IMPORTANT

It is important to note that the reform to the existing Data Protection Act 1998 is being brought by the EU's General Data Protection Regulation (GDPR).

The Government has confirmed the UK's decision to leave the EU will not affect the commencement of the GDPR. The Government is introducing measures related to this and wider data protection reforms in a Data Protection Bill.

GDPR introduces new rules that regulate how we handle and process the personal data that is entrusted to us. NHSGGC has a legal requirement to comply with the new Regulation.

Although like many organisations NHSGGC has already adopted privacy processes and procedures compliant under the existing legislation, the GDPR introduces a number of new requirements that if breached can incur substantial fines or other regulatory action.

The overall purpose of the new regulation is to increase the rights individuals have over how organisations manage the personal information they hold about them. It also strengthens the obligations and accountability for organisations to handle personal data in a transparent and secure manner.

The GDPR grants rights that enable data subjects to have a better understanding of and more control over their personal information. The GDPR obliges organisations to provide transparency on their data processing methods and restore individuals' sense of control over their personal data.

The rights individuals have under the Regulation are:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision

1. The right to be informed
 	
Individuals have the right to be informed of why we are collecting/holding data about them, and how that data will be used.
 	
The information NHSGGC provides about the processing of personal data must be:
 	
• Concise, transparent, intelligible and easily accessible;
 	
• Written in clear and plain language, particularly if addressed to a child; and
 	
• Provided free of charge
 	
Both our Privacy Notices and Patient Information Leaflets are being updated. Please contact Information Governance for further information.
	2. The right of access
	
	Individuals have a right of access to the data we hold about them (known as a Subject Access Request).
	
	• Individuals have the right to obtain:
	  ○ Confirmation that their data is being processed; and
	  ○ Access to their personal data
	• We must provide a copy of their information **free of charge** under the new regulations. However, we can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if the request is repetitive.
	• The information must be provided without delay and **at least within one month** of the date the request was received.
	
	• If individuals request the information by electronic means, then we should respond in that way (if we are able to do so), unless the Individual requests otherwise.

• **The right to rectification**
 	
The right to have personal data rectified if inaccurate or incomplete.
 	
• Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.
 	
• This can be done by means of providing a supplementary statement.
 	
• If you have disclosed the personal data to a third party, you must inform them of the rectification requirement where possible.
 	
• We must respond to the request for rectification within one month.
  ○ This can be extended by two months where the request is complex.
 	
N.B. Clinical information should not be removed from a health record unless approval has been granted by the Board's Caldicott Guardian.
 	
• If a patient believes clinical information in their health record to be inaccurate we should ask them to put their concerns in writing, stating clearly what part of the
	3. The right to erasure
	
	The right to have personal data erased (also known as the 'right to be forgotten') and to prevent processing in specific circumstances.
	
	• This does not provide an absolute 'right to be forgotten'.
	
	• Applicable circumstances includes:
	  ○ It is no longer necessary in relation to the purpose for which it was originally collected/processed;
	  ○ Individual withdraws consent;
	  ○ Individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
	  ○ It was unlawfully processed;
	  ○ It must be erased in order to comply with a legal obligation;
	  ○ It is processed in relation to children.

record they disagree with. This should be signed and dated. Health Records will arrange for a copy of this letter to be retained in the patient's health record. ○ If the patient remains dissatisfied, they should be advised to raise a complaint in line with the Board's Complaints Procedures. In addition, they may wish to raise a complaint with the Information Commissioner's Office whose contact details can be obtained from the Information Governance Department.	• We can refuse to comply with a request for erasure: ○ To comply with a legal obligation or for the performance of a public interest task or exercise of official authority. ○ For public health purposes in the public interest; ○ For NHSGGC this could mean that we would record someone's request, however, if we believe a clinical position is accurate this does not need to be erased; ○ Archiving purposes in the public interest, scientific research, historical research or statistical purposes; ○ To exercise the right of freedom of expression and information; or ○ The exercise or defence of legal claims.
4. The right to restrict processing Individuals have the right to request their personal data is 'blocked' or processing is suppressed. NHSGGC is required to consider requests to restrict the processing of data in the following circumstances: ○ Where an individual contests the accuracy of the personal data; ○ Where an individual has objected to the processing; ○ When processing is unlawful and the individual opposes erasure and requests restriction instead of erasure; ○ If we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim. Where we have agreed to, or have a legal obligation to, cease processing personal data, NHSGGC is permitted to continue to store the	**5. The right to data portability** The right for individuals to obtain and reuse their personal data for their own purposes across different services. • This allows individuals to obtain and reuse their personal data for their own purposes across different services under specific circumstances. • It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. • The right to data portability only applies: ○ To the personal data an individual provided to a controller; ○ Where the processing is based on the individual's consent or for the performance of a contract; ○ When processing is carried out by automated means.

personal data, but not further process it.	• **If** any of the above circumstances apply, we:
	  ○ Must provide the information in a structured, commonly used and machine-readable form;
	  ○ Must provide this free of charge;
	  ○ May be required to transmit the data directly to another organisation (if technically feasible);
	  ○ If the data concerns more than one individual, we must consider whether providing the information would prejudice the rights of any other individual.

6. The right to object
 	
The right to object to processing of data based on legitimate interests of the organisation, direct marketing or for the purposes of scientific/ historical research and statistics.
 	
• Individuals have the right to object to:
  ○ Processing based on legitimate interest or the performance of a task in the public interest/exercise of official authority (including profiling);
  ○ Direct marketing (including profiling); and
  ○ Processing for purposes of scientific/ historical research and statistics.
 	
There are exceptions where:
 	
• NHSGGC can demonstrate compelling legitimate grounds for the processing which overrides the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
 	
• Where the personal data is being used for research purposes and the processing is necessary for the performance of a task carried out for reasons of public interest.
	7. Rights in relation to automated decision making and profiling
	
	Individuals have the right not to be subject to a decision based on automated processing.
	
	• Individuals have the right not be subject to a decision when:
	  ○ It is based on automated processing;
	  ○ It produces a legal effect or a similarly significant effect on the individual;
	
	• You must ensure that individuals are able to:
	  ○ Obtain human intervention;
	  ○ Express their point of view;
	  ○ Obtain an explanation of the decision and challenge it.
	
	• Profiling is defined as any form of automated processing intended to evaluate certain personal aspects of an individual in particular to analyse or predict:
	  ○ Performance at work;
	  ○ Economic situation
	  ○ Health;
	  ○ Personal preferences;
	  ○ Reliability;
	  ○ Behaviour;
	  ○ Location; or
	  ○ Movements

How we are ensuring we meet individual rights:

Activity is already taking place across the NHSGGC to get us ready for this change. You and some of your colleagues may already be involved in this.

We are updating all our Policies and Procedures to ensure the rights are adhered to. For example our Privacy Notices, which are already provided to Patients, will be updated to include all the necessary information so the process itself does not change. Our Subject Access Rights Policy has been updated to reflect the new requirements and our procedures adapted to deal with such requests going forward.

Our Safe Handling Information Training modules are being updated and will be launched shortly. GDPR information roadshows will be touring our Health Board premises – dates and venues will be issued locally.

For further information please contact the Information Governance Department at data.protection@ggc.scot.nhs.uk

The General Data Protection Regulation

Information Asset Register

Data Protection law is changing on 25 May 2018.

GDPR strengthens the obligations and

accountability on organisations, like NHSGGC to handle personal data in a transparent and secure manner. This Factsheet will help you understand one of the new explicit requirements on our need to document all our processing activities.

This Factsheet will help you understand what this means for you as an employee who may handle personal data as part of your role.

IMPORTANT
It is important to note that the reform to the existing Data Protection Act 1998 is being brought by the EU's General Data Protection Regulation (GDPR).

The Government has confirmed the UK's decision to leave the EU will not affect the commencement of the GDPR. The Government is introducing measures related to this and wider data protection reforms in a Data Protection Bill.

GDPR introduces new rules that regulate how we handle and process the personal data that is entrusted to us. NHSGGC has a legal requirement to comply with the new Regulation.

Although like many organisations NHSGGC has already adopted privacy processes and procedures compliant under the existing legislation, the GDPR introduces a number of new requirements that if breached can incur substantial fines or other regulatory action.

The overall purpose of the new regulation is to increase the rights individuals have over how organisations manage the personal information they hold about them. It also strengthens the obligations and accountability for organisations to handle personal data in a transparent and secure manner.

What is the Information Asset Register?

Basically, it is 'documentation' that captures all NHSGGC processing activities under its responsibility, covering areas such as processing purposes, data sharing and retention. This is a new requirement under Article 30 of GDPR. This has to be documented in written (including electronic) form and should be made available to the Information Commissioner on request.

Documenting our processing activities is important, not only because it is itself a legal requirement, but also because it will support good data governance and help NHSGGC demonstrate its compliance with other aspects of GDPR and Public Records Scotland Act. For example, under GDPR there is a need to report a significant harm data breach to the Information Commissioner within 72 hours. The type of information recorded in the Information Asset Register should allow us to quickly identify what type of records have been breached along with the volume and category of information involved.

Data Controllers and third party processors each have their own documentation obligations.

What do we need to document:

The Information Asset Register will document the following information:

- The purpose of the processing
- A description of the categories of individuals and categories of personal data.
- The categories of recipients of personal data.
- Details of any transfers to third countries including what agreements are in place.
- Retention schedules
- A description of our technical and organisational security measures.

How we are doing this:

Activity is already taking place across the NHSGGC to populate the Information Asset Register. You and some of your colleagues may already be involved in this.

Information Champions have been identified and guidance provided to help complete the Information Asset Register requirements. This information will then be reviewed to identify if it is sufficient for purpose or whether further more granular information is required.

This is not a one-off exercise as the maintenance of the Information Asset Register is imperative. Asset requirements will need to be regularly reviewed, and any new assets, or changes to existing processes will need to be updated in a timely fashion. An annual internal audit review of the asset register will take place.

For further information please contact the Information Governance Department at data.protection@ggc.scot.nhs.uk

The General Data Protection Regulation

Subject Access Requests

Data Protection law is changing on 25 May 2018.

GDPR strengthens the obligations and accountability on organisations, like NHSGGC to handle personal data in a transparent and secure manner. It also increases Individual's rights to control how organisations process their information. An individual's right of access (subject access request) is not a new concept, however, GDPR has introduced enhancements which organisations, like NHSGGC, now have to incorporate into how we respond to such requests.

This Factsheet will help you understand what this means for you as an employee if you receive a subject access request as part of your role.

IMPORTANT
It is important to note that the reform to the existing Data Protection Act 1998 is being brought by the EU's General Data Protection Regulation (GDPR).

The Government has confirmed the UK's decision to leave the EU will not affect the commencement of the GDPR. The Government is introducing measures related to this and wider data protection reforms in a Data Protection Bill.

GDPR introduces new rules that regulate how we handle and process the personal data that is entrusted to us. NHSGGC has a legal requirement to comply with the new Regulation.

Although like many organisations NHSGGC has already adopted privacy processes and procedures compliant under the existing legislation, the GDPR introduces a number of new requirements that if breached can incur substantial fines or other regulatory action.

The overall purpose of the new regulation is to increase the rights individuals have over how organisations manage the personal information they hold about them. It also strengthens the obligations and accountability for organisations to handle personal data in a transparent and secure manner.

What is a subject access request?

A **subject access request** (SAR) is simply a **request** made by or on behalf of an individual for the information an organisation holds about them. This right existed under the Data Protection Act 1998, and remains with some enhancements within the new General Data Protection Regulation (GDPR). The GDPR clarifies that the reason for allowing individuals access to their personal data is so that they are aware of and can verify the lawfulness of the processing being undertaken by an organisation.

What information is an individual entitled to?

- Confirmation that their data is being processed;
- A copy of the personal data we hold about them; and
- Other supplementary information – this largely corresponds to the information that should be provided in the Boards Privacy Notice, including:
    - Why we are processing their personal data;
    - The categories/types of personal data concerned;
    - If we share/have shared their data with third parties, who they are, in particular if they are based in third countries or international organisations and security measures have we taken;
    - How long we will hold their information;
    - What rights they have over how we process their personal data;
    - How they can make a complaint to the ICO; and
    - If we process personal data about them which they did not supply, then what that source of information is.

What has changed?

- Previously we could charge individuals for the cost of providing this information. **This information must now be provided free of charge.** However, we can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. Contact the Information Governance team for assistance with this.

  Where this is the case, we can:

  - Charge a reasonable fee taking into account the administrative costs of providing the information; or
  - Refuse to respond
    - Where we refuse to respond to a request, we must explain why to the individual, informing them of their right to complain to the supervisory authority (Information Commissioner (ICO)) without undue delay and at the latest within one month.
  - Advice should be sought from the Information Governance Department before refusing or charging for a request.

- The regulation also allows us to charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that we can charge for all subsequent access requests.
    - The fee must be based on the administrative cost of providing the information.

- Information must be provided **without delay and at the latest within one month of receipt**. Previously, we had 40 days to respond.
    - We can extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, we must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

- Previously a request had to be made in writing, this will no longer be the case.

- If the request is made electronically, we should (if we are able to do so) provide the information in a commonly used electronic format.

  The GDPR includes a best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information. There is recognition that this will not be appropriate for all organisations, but there are some sectors where this may work well.

What about requests for large amounts of personal data?

We often process large quantities of information about an individual, in such cases the GDPR permits us to ask the individual to specify the information the request relates to.

The GDPR does not include an exemption for requests that relate to large amounts of data, but we may be able to consider whether the request is manifestly unfounded or excessive.

How are we implementing these changes?

Activity is already taking place across the NHSGGC to get us ready for this change. You and some of your colleagues may already be involved in this.

We are updating all our policies, procedures and documentation. Our Subject Access Request (SAR) Policy has been updated to incorporate the above enhancements.

Our Safe Information Handling LearnPro modules are being updated and will be launched shortly. Roadshow presentations open to all staff are touring our Health Board premises – date and venue information available here .

For further information please contact the Information Governance Department at data.protection@ggc.scot.nhs.uk

The General Data Protection Regulation

Right to be Informed (Privacy Notices)

Data Protection law is changing on 25 May 2018.

GDPR strengthens the obligations and accountability on organisations, like NHSGGC to handle personal data in a transparent and secure manner. Its fundamental principle is to increase the rights individuals to know how organisations process and use the personal information they hold about them.

The right to be informed encompasses our obligation to provide 'fair processing information' to our patients and staff, the typical way to do this is via a privacy notice. This Factsheet will describe the additional information we have added to our Privacy Notices to ensure our Patients and staff now how we use their personal data.

IMPORTANT
It is important to note that the reform to the existing Data Protection Act 1998 is being brought by the EU's General Data Protection Regulation (GDPR).

The Government has confirmed the UK's decision to leave the EU will not affect the commencement of the GDPR. The Government is introducing measures related to this and wider data protection reforms in a Data Protection Bill.

GDPR introduces new rules that regulate how we handle and process the personal data that is entrusted to us. As a Data Controller, NHSGGC has a legal requirement to comply with the new Regulation.

Although like many organisations NHSGGC has already adopted privacy processes and procedures compliant under the existing legislation, the GDPR introduces a number of new requirements that if breached can incur substantial fines or other regulatory action.

The overall purpose of the new regulation is to increase the rights individuals have over how organisations manage the personal information they hold about them. It also strengthens the obligations and accountability for organisations to handle personal data in a transparent and secure manner.

What is a Privacy Notice?

An Individual's right to be informed on how organisations will use their personal data is not a new concept, it exists under the Data Protection Act 1998. It is basically our obligation to provide 'fair processing information' to patients and staff at the point of collection of their personal information, ie why we are collecting the information, how we will use it and who we will share it with. The information to be provided under GDPR is more detailed and specific than in the DPA and places an emphasis on making privacy notices more transparent, understandable and accessible. Data Controllers, like NHSGGC are expected to take 'appropriate measures' to ensure that data subjects receive the information they need in a way that is appropriate, balanced and accessible. Our obligation is to identify the best way to provide information to patients and staff, provide it in a meaningful format (paper, electronic), and at the right time ie prior to us collecting their personal information.

What does 'appropriate measures' mean?

The information provided must be:

- Concise, transparent, intelligible and easily accessible;

- Written in clear and plain language, particularly if addressed to a child; and
- Free of charge

These requirements are deemed necessary to ensure that privacy information is clear and understandable for our patients and staff. The GDPR makes explicit what has always been set out as good practice by the Information Commissioner (ICO) under the DPA.

We have reviewed and updated our Privacy Notices and processes taking into consideration guidance provided by the ICO as necessary.

What information must be supplied?

Our Privacy Notice will now include all of the following:

- NHSGGC's contact details, including our Data Protection Officer's details;
- The type of personal information we need, and why we need it;
- What kind of personal information we could receive about you from third parties, and who those third parties could be; if any;
- If we share any of your information, who we share it with;
- If we send your information to countries out-with the EU how we ensure it is secure;
- how long we will keep the information;
- what your rights are, including right of: access to and rectification of; erasure of personal data; restriction to processing; to object to processing as well as the right to data portability;
- where you have given consent, the right to withdraw it at any time;
- the right to lodge a complaint with a supervisory authority (ICO);
- whether the information we collect is a legal requirement, and what the possible consequences of not providing it would be; and
- details of any automated decision making we undertake, including profiling and information about how decisions are made, the significance and the consequences of those decisions.

What action are we taking?

Activity is already taking place across the NHSGGC to get us ready for this change. You and some of your colleagues may already be involved in this.

Our Privacy Notices, which are already provided to Patients and members of staff, have been updated to include all the necessary information. Access to the updated version of the Privacy Notice will be provided shortly. It is important to note that the process of providing the Privacy Notice to Patients at certain contact points is not changing.

For further information please contact the Information Governance Department at data.protection@ggc.scot.nhs.uk

The General Data Protection Regulation

Data Protection Officer

Data Protection law is changing on 25 May 2018.

GDPR strengthens the obligations and accountability on organisations, like NHSGGC to handle personal data in a transparent and secure manner. One of the new requirements is that organisations like NHSGGC must appoint a data protection officer (DPO). The GDPR also contains details about the tasks a DPO should carry out, along with the duties that the NHSGGC should do as an employer to support the DPO's role.

This Factsheet will summarise the role responsibilities, describe what support NHSGGC will provide to the role holder, and our DPO's contact details.

IMPORTANT
It is important to note that the reform to the existing Data Protection Act 1998 is being brought by the EU's General Data Protection Regulation (GDPR).

The Government has confirmed the UK's decision to leave the EU will not affect the commencement of the GDPR. The Government is introducing measures related to this and wider data protection reforms in a Data Protection Bill.

GDPR introduces new rules that regulate how we handle and process the personal data that is entrusted to us. NHSGGC has a legal requirement to comply with the new Regulation.

Although like many organisations NHSGGC has already adopted privacy processes and procedures compliant under the existing legislation, the GDPR introduces a number of new requirements that if breached can incur substantial fines or other regulatory action.

The overall purpose of the new regulation is to increase the rights individuals have over how organisations manage the personal information they hold about them. It also strengthens the obligations and accountability for organisations to handle personal data in a transparent and secure manner.

The organisation's responsibilities – the position of the DPO

The DPO is an essential role in facilitating 'accountability' and the ability to demonstrate compliance with the GDPR. As noted above NHSGGC must appoint a DPO whose job description is compliant with GDPR requirements (see section 'The qualities and tasks of the DPO' below). NHSGGC must ensure that:

- the role directly reports to the highest management level of the organisation. This does not necessarily imply line management at this level, but direct and unimpeded access to the senior management team;
- the DPO is provided with adequate resources: financial and human resources, and is supported in maintaining their own expertise;
- the DPO has proven 'expert knowledge of data protection law and practices', the ability to perform the tasks specified in the GDPR, and sufficient understanding of the organisation's business and processing;

- it has in place information governance and related policies that address:
    - organisational accountability;
    - DPO reporting arrangements;
    - timely involvement of the DPO in all data protection issues;
    - compliance assurance: privacy by design and default;
    - advising on where data protection impact assessment is required; and
    - the DPO's role in incident management.
- the DPO does not receive any instruction regarding the exercise of these duties, and is protected from disciplinary action, dismissal or other penalties when carrying out these duties;
- if the DPO performs another role or roles, that there is no conflict of interest; and
- the DPO's contact details are published in our Privacy Notice and other documents detailing how we process personal information, and are communicated to the ICO.

The qualities and tasks of the DPO

The DPO shall be appointed to the role on the basis of their professional qualities and, in particular their:

- expertise in national and European data protection laws and practices and an in depth understanding of the GDPR;
- sufficient understanding of NHSGGC's processing operations, as well as its information systems and data security and data protection needs; and
- demonstrable ability to fulfil their duties. The principle tasks being:
    - to provide advice to the Board and its employees on compliance obligations;
    - to advise on when data protection impact assessments are required and to monitor their performance;
    - to monitor compliance with data protection legislation and organisational policies, including staff awareness and provisions for training;
    - to co-operate with, and be the first point of contact for the Information Commissioner;
    - to be the first point of contact for all data protection matters;
    - to be available to be contacted directly by patients and members of staff – the contact details of our DPO will be published in our Privacy Notice and on our website; and
    - to take into account information risk when performing the above tasks.

NHSGGC's Data Protection Officer is:

Isobel Brown

Tel: 0141 335 2059, or email data.protection@ggc.scot.nhs.uk

The General Data Protection Regulation

Third Party Contracts

Data Protection law is changing on 25 May 2018.

GDPR strengthens the obligations and accountability on organisations, like NHSGGC to handle personal data in a transparent and secure manner. Where we share personal information with a third party as part of our patient care we need to ensure that third party will handle that information securely, will only use it for the purposes we have shared it, and in line with the new legislation.

This Factsheet will help you understand what this means for you as an employee if you need to share personal information with a third party processor as part of your role.

IMPORTANT
It is important to note that the reform to the existing Data Protection Act 1998 is being brought by the EU's General Data Protection Regulation (GDPR).

The Government has confirmed the UK's decision to leave the EU will not affect the commencement of the GDPR. The Government is introducing measures related to this and wider data protection reforms in a Data Protection Bill.

GDPR introduces new rules that regulate how we handle and process the personal data that is entrusted to us. NHSGGC has a legal requirement to comply with the new Regulation.

Although like many organisations NHSGGC has already adopted privacy processes and procedures that are compliant under the existing legislation, the GDPR introduces a number of new requirements that if breached can incur substantial fines or other regulatory action.

The overall purpose of the new regulation is to increase the rights individuals have over how organisations manage the personal information they hold about them. It also strengthens the obligations and accountability for organisations to handle personal data in a transparent and secure manner.

What is the purpose of the change?

Under Article 4 of GDPR, a "Controller" is the company that decides how the data is processed. A "Processor" is a company that processes the data on behalf of the Controller.

Under GDPR, Controllers will bear ultimate responsibility for the data processing however Processors are much more accountable now than they were under the previous Law and are subject to much of GDPR.

There are some very specific rules that Controllers, such as NHSGGC must comply with when choosing Processors. These rules include choosing Processors that provide "sufficient guarantees" that they will meet their legal obligations under GDPR. The new Regulation is based on "show not tell", so both Controllers and Processors will need to ensure they can evidence the security and protection they take when handling data and that they conform to all relevant GDPR requirements.

Processors have new responsibilities and can incur fines for breaches from the ICO if these are not met. For example they must make sure they keep adequate records of any processing they carry out and must process the data securely and in line with Data Processing Agreements.

What Changes are required to Data Processing Agreements?

There are some very specific rules around the Controller/Processor relationship. GDPR's Article 28 explicitly:

- States that a data processing agreement must be in place between the Controller and Processor.
- Lists a number of obligations that need to be covered within the data processing agreement. In particular, it states
    - That the data processor provides the data controller with all information necessary to demonstrate compliance with the GDPR.
- The data processor must only act on the documented instructions of a controller.
- It is a breach of GDPR if Processors do not sign up to these obligations.

NHSGGC engages with a significant number of third parties that allows us to carry out all the services we provide. Any contracts that we have in place on, or after 25 May 2018 will need to meet the new GDPR requirements. We have new Data Processing Agreement templates and clauses that will ensure we meet our obligations under GDPR. Please contact the Information Governance Department for further information.

In summary these obligations state that the Processor:

- Will only use the data in the way we instruct them;
- Will only employ people who have promised to keep the data confidential;
- Will keep our data secure;
- Will not hire another Processor to do the work unless we have given our permission;
- Will help us fulfil requests brought by patients or members staff enforcing their rights under GDPR. For example, if a patient requests their data be rectified, then the Processor will help us by amending their systems accordingly (ie the Processor's) if we instruct them to do so;
- Will help us with our GDPR duties including breach notification requirements. So, if the Processor loses some of the data given to it by us, the Processor will tell us so that we will be able to report the breach to the ICO within the 72-hour time limit;
- Will delete the data we have shared at the end of the contract with us; and
- Will allow their processes to be inspected and audited.