Scottish Ambulance Service
Taking Care to the Patient

NHS SCOTLAND 70 YEARS #nhsscot70

NOT PROTECTIVELY MARKED

Public Board Meeting	**May 2018** **Item No 14**

THIS PAPER IS FOR NOTING

GENERAL DATA PROTECTION REGULATION (GDPR)

Lead Director **Author**	Pat O'Connor, Director of Care Quality & Strategic Development Katy Barclay, Information Services & Governance Manager
Action required	The Board is asked to note the introduction of the General Data Protection Regulation and the organisational responsibilities associated with it.
Key points	The General Data Protection Regulation (GDPR) is broadly similar to the previous Data Protection Act which means that the processes, procedures and policies already in place provide a robust building block for the move to GDPR. One of the biggest changes is the increased emphasis on the responsibility of data controllers, of which the Service is one, to ensure all data processing activities are documented to demonstrate governance and accountability.
Timing	This paper will be presented to the Board in May 2018.
Link to Corporate Objectives	The Corporate Objectives this paper relates to: 1.2 Engaging with patients, carers and other providers of health and care services to deliver outcomes that matter to people 6.2 Use continuous improvement methodologies to ensure we work smarter to improve quality, efficiency and effectiveness.
Contribution to the 2020 vision for Health and Social Care	The governance of information is key to the Service's 2020 vision in terms of: • Appropriate sharing of information across health and other sectors. • Assessment of the privacy impacts of new initiatives and projects. • Protection of personal information held by the Service.
Benefit to Patients	The Scottish Ambulance Service has a robust Information Governance Framework to ensure patient information is handled in accordance with legislation.
Equality and Diversity	No implications identified.

NOT PROTECTIVELY MARKED

SCOTTISH AMBULANCE SERVICE BOARD

GENERAL DATA PROTECTION REGULATION (GDPR)

INFORMATION SERVICES & GOVERNANCE MANAGER

SECTION 1: PURPOSE

The General Data Protection Regulation came into force on 25 May 2018. This paper is to inform the Board of the organisational impact of this change.

SECTION 2: BACKGROUND

The General Data Protection Regulation (GDPR) is broadly similar to the previous Data Protection Act which means that the processes, procedures and policies already in place provide a robust building block for the move to GDPR.

One of the biggest changes is the increased emphasis on the responsibility of data controllers, of which the Service is one, to ensure all data processing activities are documented to demonstrate governance and accountability.

SECTION 3: DISCUSSION

3.1 Information held (processed) by the Scottish Ambulance Service

The Service is required to demonstrate that an Information Asset Register is in place. The Information Asset Register must detail all types of data held by the Service and include:

- the source of the data
- who it is shared with
- how the data is stored and for how long
- the legal basis for holding or processing the information must be documented,

To comply with the requirements under the GDPR an up to date and accurate Information Asset Register is required.

The Service's Information Asset Register will be developed over a period of 12-18 months and will be run as a project, reporting into the Audit Committee via the Information Governance Group. The initial scoping of the project is due to start in June 2018.

3.2 Individuals' Rights

An individual is any living person that the Service holds identifiable information about, this includes, but is not limited to, patients, staff, callers and volunteers.

Under GDPR, individuals' rights are broadly similar to those under the Data Protection Act 1998 with a few enhancements, notably the right to portability. This new right is not likely to apply to the data processed by the Service.

The GDPR includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

3.3 Data protection notices – the right to be informed

Under the Data Protection Act the Service had a privacy notice on the external website. This included information for the public such as; our identity and how we used their information.

The Service's previous privacy notice has been reviewed, amended and published as a Data Protection Notice. Under the GDPR there are some additional things we now have to tell people. For example

- explain our lawful basis for processing the data
- disclose our data retention periods
- inform individuals that they have a right to complain to the Information Commissioner's Office (ICO) if they have concerns around the way we are handling their data.

3.4 Subject Access – the right of access

The GDPR has introduced some changes around the way the Service is required to handle Subject Access Requests (SAR). The new rules mean the Service:

- will not be able to charge, previously the Service charged a nominal fee of £10 per request.
- will have a month (30 calendar days) to comply, rather than the 40 calendar days under DPA 1998.
- can refuse or charge for requests that are manifestly unfounded or excessive.

3.5 Data protection by design

The GDPR makes privacy by design a legal requirement. This means that 'Data Protection Impact Assessments' (DPIAs) are mandatory in certain circumstances.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of sensitive (special category) data.

If a DPIA indicates that the data processing is high risk, the Service will be required to address these risks. If this cannot be done, we will be required to consult the ICO to clarify that our processes comply with the GDPR.

3.6 Data breaches

The Service currently has procedures in place to detect, report and investigate a personal data breach. Under GDPR there is a requirement for all organisations to report the most serious breaches to the ICO. The Service has a policy and process in place for assessing and reporting data breaches. This includes the assessment of the severity and escalation of the most serious breaches to the ICO. Under GDPR the timescales for reporting these breaches has reduced to 72 hours. A failure to report a breach, when required to do so, could result in a failure to report fine in addition to a potential fine for the breach itself.

There will be two levels of fines based on the GDPR. The first is up to €10 million or 2% of the company's global annual turnover of the previous financial year, whichever is higher. The second is up to €20 million or 4% of the company's global annual turnover of the previous financial year, whichever is higher. The potential fines are substantial and a good reason for companies to ensure compliance with the Regulation.

The Parliament had requested for fines to reach €100 million or 5% of the company's global annual turnover. The agreed fines are the compromise that was reached.

Fines for infringements will be considered on a case-by-case basis and will take a number of criteria into consideration, such as the intentional nature of the infringement, how many subjects were affected and any previous infringements by the controller or processor.