GDPR Compliance Statement

As a business we take issues of information governance very seriously and we already have in place a standing Information Governance Board looking at issues across the Group, including of course the forthcoming changes to data privacy law arising through the introduction of the General Data Protection Regulation ((GDPR) see: https://ec.europa.eu/info/law/law-topic/data-protection_en) to be implemented by the Data Protection Act 2018 (see: https://services.parliament.uk/bills/2017-19/dataprotection.html).

We are committed to:

- ensuring the security and protection of the personal information that we process, and to providing a compliant and consistent approach to data protection; and
- complying with the requirements of the GDPR and the data privacy related obligations in our contractual commitments.

We are actively working on our GDPR strategy and we have a project team who are mobilised and focussing on our strategy and implementation of GDPR. As part of these preparations:

- We have undertaken a GDPR training program available to all but aimed in particular at key employees identified as IG Champions across the group – we have also rolled out the Information Governance training provided by NHS Digital across all employees, to ensure that our staff understand the basics of data protection law, to instil in them the nature and importance of personal data, to educate them to recognise and respond to subject access requests and learn how to report privacy breaches.
- We are issuing an undertaking to be signed by all employees which reaffirms their commitment to information governance and maintain confidentiality.
- We have a Data Privacy Impact Assessment policy whereby all new products and services which would involve the processing of personal data are subject to an assessment in order to identify risks and to ensure that the principles of privacy by default and privacy by design are taken into account.
- We are revising and updating our privacy notices across the group and our internal policies and processes which relate to information governance (including in relation to subject access requests).
- We have revisited our existing incident reporting policy and process with a view to compliance with our obligation to report IG breaches without any undue delay.
- We are implementing intra-group agreements in order to ensure that were services are provided across EMIS Group it is done so in a consistent and compliant manner.
- We have undertaken a ‘data mapping’ exercise to ensure that we are clear as to the data and information assets we have across the Group (including patient data, employee data and customer data) and are working through the outputs from that exercise.
- We are updating our contracts to ensure that they meet the specific requirements set out in the GDPR and we are actively engaging with our customers (and suppliers) to update our existing contracts.
- As required by the GDPR we have appointed a Data Protection Officer, Ian Mckie, who may be contacted via privacy@emishealth.com if you have any queries regarding our approach.

If you should have any comments or concerns regarding our approach then please do not hesitate to contact us and we would be more than happy to discuss such matters with you in more detail.

Please note that this statement is provided for information purposes only and does not constitute a specific warranty or representation.