FAQ on Data Protection and Information Security

Version 2.0; 21 December 2021

Content

1. How is compliance with the General Data Protection Regulation (GDPR) and other rules warranted?

It is the responsibility of the individual or organisation (the 'Participant') to ensure that all necessary agreements are obtained from their institution (and can be made available on demand) in respect to any local laws, guidelines, 'best practice', ethical requirements, etc. In particular, the Participant is explicitly responsible for obtaining and documenting each patient's informed consent for the use of the patient's data for the specific purposes of research and quality assurance in the Registry. The participant must also warrant that all necessary consents and approvals required for processing all information relating to an identified or identifiable natural person to be processed under this agreement have been obtained.

Upon registration of a new patient, the registry platform requires a confirmation that informed patient consent has been obtained freely and unambiguously, thus signifying an agreement to the processing of personal data relating to the patient.

2. What data are collected?

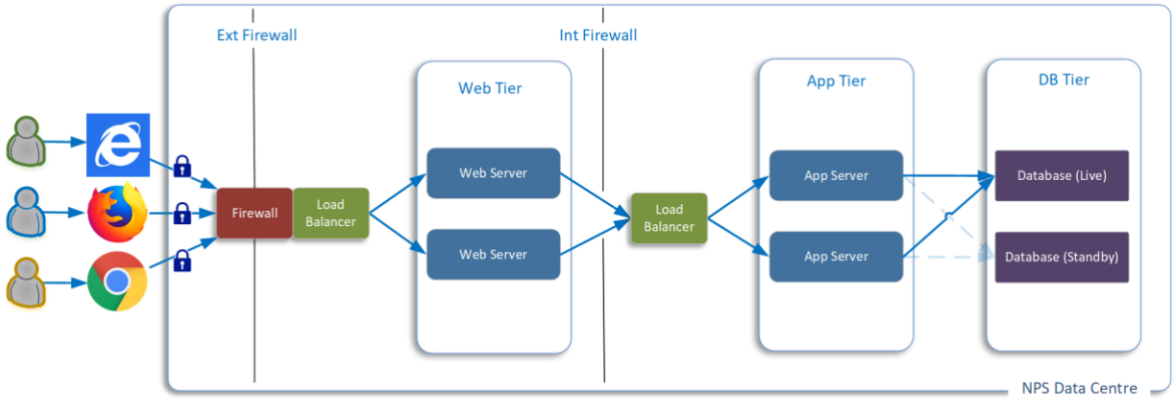
The registry data is comprised out two separately processed parts:

- Patient identifiable data
  - Patient first name
  - Patient last name
  - Gender
  - Date of Birth
  - Medical record number (MRN), a unique number provided by the participant
- Clinical data on patients' diagnosis, treatment and outcome

The registry platform requires a unique MRN, the patient's birthdate and their gender to be entered before a new patient record can be created in the system. A patient's first name and last name are not mandatory and do not need to be provided when creating a new patient record. However, providing a patient's first name and last name will enable a patient's record to be more easily identified by the participant. The patient identifiable and clinical data are hosted in separate databases and combined when the participant logs onto the system.

3. Where are the data hosted?

The following diagram shows the infrastructure used to host the Spine Tango solution. The service is hosted by NEC Software Solutions UK Ltd (formerly known as Northgate Public Services (UK) Limited) in one of its UK data centres.



NEC' Health Platform provides a minimum of a web server, application server and database server. To provide greater security, resilience and the ability to run reports without affecting data entry, the solution has been specified to provide redundancy throughout the infrastructure. This means that failure in any single component will not result in service interruption.

The entire database is encrypted with further encryption being provided to those data fields holding patient identifiable data. A very limited number of NEC staff have access to the database for the purposes of data management. Developers and network managers have access to the server on which the data resides but cannot view the data itself. Data sent from local clients to the database are sent via the Internet with the link being encrypted using a Secure Sockets Layer (SSL). This protects the data in transit.

3. How are the hosted data protected?

The secure and confidential handling of patient and clinical data is a fundamental part of the Spine Tango service provided by NEC. In delivering services to their clients, NEC manages confidential data relating to millions of citizens and patients in the UK and overseas. This not only involves technical solutions to protect the data, but also robust processes and procedures surrounding data access, based upon legislation and industry best practice. Given the nature of the data processed by NEC, security and governance are afforded the highest priority.

3.1 What security accreditation does the data processor have?

NEC is accredited to the following:

- ISO/IEC 27001:13, ISO/ISEC 9001.
- The UK government's Cyber Essentials.
- National Health Service (NHS) Data Security and Protection Toolkit (completed annually and required to process NHS data).
- NEC is also compliant with the UK Government's Information Technology Infrastructure Library (ITIL), a set of detailed practices for IT service management.

NEC' data centres and back up and disaster recovery facilities are also ISO/IEC 27001:13 accredited.

NEC is registered on the Information Commissioner's Office Data Protection Public Register under Registration Number Z5666588 (https://ico.org.uk/ESDWebPages/Entry/Z5666588).

3.2 What information security best practice standards does the data processor follow?

NEC adopts information security best practice standards which require it to:

- Undertake regular Information Security Risk Assessments.
- Comply with all legal obligations under a variety of different legislation, regulations, directives and codes of conduct.
- Maintain and test all Business Continuity and Disaster Recovery plans.
- Provide regular Security Awareness training to all staff.
- Provide standards for the acceptable use of information assets.
- Report any actual or suspected breach of the Security Policies and Standards to the Information Security Manager, who investigates all incidents, and to EUROSPINE as the data controller.
- Review the Information Security Management System performance at regular intervals.

In addition, NEC undertake other, physical and procedural methods to protect data. These include but are not limited to:

- Continuous assessment of our processes under our ISO/IEC accreditations.
- The encryption of all data at the database level and the encryption of sensitive data at the data field level. This exceeds the recommendations set out in the UK Cabinet Office's guidance published in 'Electronic Government Services for the 21st Century'.
- Limiting access to data to only those staff working on delivery of the Spine Tango service, and also further restricting access to sensitive data.
- Processing data on the servers, not downloading it to, or storing it on, local computers.
- Never transmitting sensitive data by email over the public Internet.

- Regular penetration testing of services by an external, independent company.

3.3 Are staff aware of their responsibilities regarding data security and information governance?

The need for confidentiality when handling data is included in contracts of employment for all NEC employees.

There is a high level of organisational awareness and understanding of the needs for patient confidentiality within NEC and all staff are required to undertake mandatory annual training which covers data protections, data security, and data governance.

In addition, all staff within NEC' Health business undertake further mandatory annual training as required by the National Health Service (NHS) in order to achieve compliance with the NHS Data Security and Protection Toolkit, necessary in order to process NHS data.

All staff are vetted as part of the recruitment process.

3.4 Who ensures compliance with policies?

- **NEC Data Protection Officer** - NEC' governance model includes a named Data Protection Officer (DPO). This is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing. The DPO plays a key role in ensuring NEC satisfies the highest practical standards for handling patient identifiable information.

  Acting as the 'conscience' of the organisation and championing Information Governance, the DPO supports NEC by ensuring that all programmes and projects operate in line with national guidelines and lawful and ethical processing of information. This role is particularly important in relation to running of national and international systems and services. The DPO does not sit within the service management hierarchy, retaining an independent role and thus ensuring exclusive focus in the interest of Information Governance best practice.

- **Security and Compliance Department** - NEC' Security and Compliance Department is responsible for implementing written policies and procedures, conducting risk assessments, undertaking internal monitoring and audit against both internal policies and external standards, and ensuring that staff are familiar with the appropriate compliance and security standards, and ensuring that staff complete the mandatory annual training.

  All services are subject to security and compliance reviews starting at the design stage, through implementation, and into the operation stage. The reviews check not only adherence with policies but include physical security checks, including regular (monthly) penetration testing.

- **Audits** - NEC runs a full information security internal audit programme and are externally audited by the UKAS accredited audit body, the British Standards Institute, (BSI), which independently audits NEC compliance to ISO 27001. This audit reviews our security management controls and ensures these meet the required standard.

4. What are the information governance arrangements for Spine Tango?

For Spine Tango, the EUROSPINE Spine Tango Task Force (STTF) is the Data Controller and NEC is the Data Processor. Each have clearly defined roles and processes regarding the handling and management of all data.

As the data processor, NEC acts under the direct instruction of the Data Controller, the EUROSPINE Spine Tango Task Force (STTF) and within the appropriate legal framework. NEC also provides support and advice to the STTF in relation to the requirements of that legislation.

Both NEC and the STTF acknowledge the need to maintain robust and independent records of processing activities under their respective responsibilities. Accordingly, all of the processing to be carried out by NEC on behalf of the STTF will ensure sufficient guarantees in terms of expert knowledge, reliability and resources, to implement technical and organizational measures, which will always meet the requirements of the GDPR.

5. Who can access Spine Tango Data?

Anyone with a legitimate interest in using Spine Tango data can request access to it. All requests for data, whether data requests, research requests or Freedom of Information (FOI) requests, will be passed to the STTF for consideration and resolution. NEC will only release data to third party requestors when instructed to do so by the STTF and following agreement as to the exact data fields that will be provided. All requests for data are logged and the use of the data is subject to strict terms and conditions, including the destruction of the data at the expiry of the data sharing agreement.

Record level data may be provided for research purposes strictly earmarked but would normally be provided in a pseudo-anonymised format.

5.1 Non-commercial and academic use

Upon receipt of a request for non-commercial or academic use, the STTF will consider the application and ensure that any associated ethics, or other, approvals have been obtained or if they are required. Once the request has been considered and approved, STTF will agree with NEC the details of the data to be released and then instruct NEC to release the data. Where NEC has concerns over the release of

the data (e.g. potential non-compliance with the GDPR, lack of patient consent), these will have been raised with STTF at an early stage. NEC and STTF will ensure that the release and use of the data falls meets the requirements of the appropriate legislation.

5.2 Commercial use

Data can be requested for commercial use but would only be provided as aggregated data. Record-level data will not be provided. Even so, such commercial use should always be strictly limited to the specified use or purpose indicated at the time of obtaining the informed patient consent.

5.3 Conditions of use

The data released will be appropriate to the needs of the study/research and subject to the Spine Tango Code of Conduct. Before the release of any data, the requestor will be required to formally agree EUROSPINE Terms and Conditions which will include the specific purpose and permitted scope for use of the data, the length of the agreement, the actions to be carried out with the data at the end of the agreement and any general requirements, e.g. the requirement to acknowledge EUROSPINE as the source of data; the condition prohibiting the publication of record-level data.

No data shall be used for sales or marketing purposes.