Service Definition

All IGspectrum services are cloud based with access from any supported browser and a typical renewable contract term of 12 months covering hosting, service management and support, and service upgrades.

All services conform to data protection legislation and adhere to organisational information governance policies and IGTK requirements.

Services are provided from a secure ISO27001 accredited facility with a N3 connection available.

IGspectrum is IGToolkit compliant.

Access is from any supported browser and an overview of each service will be found in this document.

Ordering and invoicing process

On receipt of a purchase order IGspectrum will invoice the client and initiate the service. Invoice terms are 30 days.

The service includes standard support during the working day, problem resolution and any updates that are released during the contract term.

Start-up

Start-up costs are usually included unless significant additional development is required.

Modifying an existing form would probably be offered at no additional charge, creating a new form would incur a one-off charge depending on the form complexity.

Training

A comprehensive service user guide is available. Initial on-site training is provided free of charge (one day is usually sufficient) and further training is offered as a chargeable option at a current (June 2016) rate of £500/day.

Service constraints

All services are available 24/7 with a 99% uptime.

An overview of the G-Cloud IGspectrum services

IGdsp - Data sharing reference portal

Return to Overview

Our unique portal provides a single web based repository where all reference documents e.g. Information sharing frameworks, protocols, agreements can be held. It will enable a record and evidence to be shared on Privacy Impact Assessments (PIAs) and Risk Assessments and signoffs by both Caldicott Guardians and DPOs. The service provides automatic alerts when agreements are shortly to expire to ensure that an organisation is operating within the relevant laws and directives.

Features

- Single repository for information sharing frameworks and protocols, agreements, templates
- Automatic alerts prior to expiry
- Portal controlled opening to the general public for document sharing
- Single view of all agreements
- Multi-agency information sharing agreement templates available
- Sign-off can be achieved inside the portal
- Administrator and user access

Benefits

- Easy review and management of all agreements
- Agreements recorded by partner organisation
- Solves protracted issues around capturing signatures / approvals
- Tiered security access enables sharing inside and outside the NHS
- Optional existing templates encourage rapid acceptance and implementation
- Cost effective

IGe-forms – Bespoke electronic forms

Return to Overview

The Electronic Forms (e-Forms) service, with integrated workflow management, provides a centralised, intuitive platform on which existing forms can be automated, accessed and managed using any device with a web browser. Rules and workflows for completing and submitting forms are fully automated and all information is captured, stored securely and made available to all that require access.

Examples of forms currently in use are:

MDT

This web based workflow and electronic forms service has recently been deployed to support the Vascular Multi-Disciplinary Team Meeting process. Clinicians can now safely and securely submit referrals for MDT meetings online and review recorded outcomes at any point thereafter.

Admission and Discharge Forms (Section 2 & 5)

This innovative, easy to use e-Forms service is being used by 260 ward staff as part of one Trust's paperless strategy.

Referrals

See IGrefer below.

IGrefer – Electronic Referrals

Return to Overview

Incorporating integrated workflow management this provides a centralised, intuitive, platform on which all referrals can be digitised, automated, accessed, transferred and managed using any web browser on all devices. Rules and workflows for completing and receiving forms are fully automated and information is captured, stored and made available securely.

Forms include:

- Cancer Referrals
- A&E Referrals
- Neurology and Neurophysiology Referrals
- Mum to be and GP Maternity Referrals

Features

- Enables sharing through approval, alerting and broadcasting functionality
- Supports navigation and image management functions
- Automated workflow and approval processes
- Different levels of user access to submit and view form data
- Secure online submissions using any internet-enabled device
- Secure system access with data held in an encrypted database

Benefits

- Automation and digitisation of forms quickly and cost-effectively
- Data accuracy increased through on-line validation
- No software installation required
- Service complies with the NHS IG Toolkit requirements
- Access to the service through any internet-enabled device
- Hosted securely at an ISO27001 accredited facility
- Simple e-referral creation process
- Immediate status and priority view of sent and received referrals
- Rapid deployment of new form
- Cost effective

IGencrypt – Document encryption

Return to Overview

The data encryption process which meets the AES 256 standard supports the complete anonymisation of all content in documents and files shared across nhs.net and beyond. Encrypted information may be reconstituted once the receiving party has been authorised and provided with a decryption code.

Documents may be shared across NHS Net and beyond. Encrypted information may be opened, reconstituted to produce a true facsimile and made legible, once the receiving party has been authorised and provided with a decryption code, by the sender.

There is no charge for decrypting a document thus enabling a cost effective service and wide user base of recipients.

Features

- Encrypts any document or file regardless of content
- Full encryption to AES 256 standard
- Secure online access using any internet-enabled device
- Decryption by any recipient only with originating user permission

Benefits

- Simple to use
- Rapid deployment
- Data shared securely
- Cost effective

IGpatient - Patient Portal

Return to Overview

An innovative cloud-based patient portal that enables patients, and their referrers, to interact directly with Trusts or care organisations through bespoke electronic forms with simple access through any web-enabled device.

The system has been security assured under the Cabinet Office Risk Management and Accreditation Document (RMAD) process.

Examples of current usage are:

Maternity Referral

Enables patients to self-refer to maternity clinics.

Family History Form

Enables patients and their family members to enter personal medical histories in response to a referral to a genetics centre.

Private Patients

Allows the secure submission of medical records to Trusts or care organisation who receive automated notifications of enquiries and file uploads which can then be download thus fully supporting the principle of care without boundaries.

Captures patient enquiries and uploaded medical records from the Trust or care organisation website and by assigning a patient identifier allows submission and linking of further enquiries and medical records.

Notifies the Trust of all enquires and uploaded records with selective download, decryption and distribution of files, e.g. to clinicians.

Features

- Patient & selected family members completion of forms
- On-line data validation according to an organisation’s defined criteria
- Data export facilitates automatic organisation’s data-base updating e.g. genetics data-base

Benefits

- Patient access through any web browser from their own device
- Improved data accuracy
- Cost effective

IGrecord – Patient Consultations

Return to Overview

This is a web-based service that provides patients with access to voice recordings of their hospital consultation appointments.

The service provides invaluable information so patients may better understand the treatments being provided and any lifestyle adjustments required as part of care plans.

Overall the service seeks to promote clinical best practice on patient communications driving improved outcomes and patient safety standards all of which is a part of making the NHS a world class service.

Logistics

Consultants are provided with a list of patient appointments and relevant demographic data. Once the patient is selected a consent routine supports the optional recording process. During the first recorded consultation the process includes obtaining registration and contact details for the patient.

The service safeguards all information governance aspects.

Consultations are recorded via a microphone on the consultation room computer.

Once the consultation is concluded the session is ended and the patient is sent an email or text message providing login details to the online service.

Using a secure login procedure patients can access their consultation recordings.

Benefits

Patient understanding: Patients are more likely to understand and adhere to their recommended treatment.

Quality healthcare outcomes depend upon patients' adherence to recommended treatment regimens. Patient non-adherence can be a pervasive threat to health and wellbeing and carry an appreciable economic burden as well. In some disease conditions, more than 40% of patients sustain significant risks by misunderstanding, forgetting, or ignoring healthcare advice. When preventive or treatment regimens are very complex and/or require lifestyle changes and the modification of existing habits, non-adherence can be as high as 70%.

Piloting of the service demonstrates patients welcome the opportunity to revisit the consultation advice given. Frequently, sick, and frail patients can find it hard to fully comprehend treatments and advice at one sitting. The ability to replay key points, aids in treatment adherence.

Mutual collaboration: This can foster patient satisfaction and improve healthcare outcomes

Clinician–patient partnerships are essential when choosing amongst various therapeutic options to maximise adherence. Mutual collaboration fosters greater patient satisfaction, reduces the risks of non-adherence, and improves patients' healthcare outcomes.

IGrecord benefits continued

Return to Overview

Improved communication: Sharing access with third parties minimises the risk of misinterpretation.

Authorised relatives and carers can have access to the recordings, greatly aiding all concerned to work from a single set of messages and information. Details are not left to interpretation.

Information bank: Clinicians create a valuable information bank to which they can refer in support of on-going treatment planning and follow-up consultations.

Patient expectations: Increasingly patients are required to have access to their health records. There is a growing trend for patients to request appointment recordings.

Trust control: Consultation recordings put hospitals in the driving seat. The service allows hospitals to control the storage of the recordings and how they are accessed. All recordings are managed in respect of data protection and NHS information governance guidelines.

Clinical and Medico-legal considerations

IGrecord assists with clinical best practice:

- Helps record in the notes what a patient has been told
- Aids with consent process, which is patient-specific and depends on the individual's circumstances
- Creates discipline in discussing key treatments and ensuring information is sought, such as a patient's drug allergies
- Evidences dates for recordings
- Promotes making good notes as a habit
- Evidences decisions made, any discussions, information given, relevant history, clinical findings, patient progress, investigations, results, consent, and referrals
- Patients have a right to access their own medical records under The Data Protection Act 1998.

Getting started

Healthcare providers buy an annual licence to use the service, typically covering all consultants.

Once the licence is established, deployment of the service is straightforward.

As standard, IGrecord comes with interfaces to all the main hospital PAS systems.

IGspectrum liaises with the organisation's IM&T team to create necessary links and user registrations.

Consultants are given a web address and login details, specific for their hospital location. Following a ten minute online training instruction, the service is available for use.

IGpseudo and IGautopseudo - Data Pseudonymisation at source

Return to Overview

Enables data extraction and sharing of patient confidential data (PCD) pseudo-anonymised or anonymised at source conforming to: Pseudonymisation Implementation Project DOH 2010 IGTK requirements for compliant, safe, ethical and secure sharing of data across communities.

This provides the ability to securely and legally share information with other authorised organisations which enables multiple applications including business intelligence and risk stratification for both planning and case finding.

Supports the use of the NHS number as the primary patient identifier or a user defined pseudonyms where no NHS number exists with a full audit trail to complement the inherent security features.

A supporting product, IGautopseudo, is installed on user’s own servers and automatically pseudonymises files containing PCD.

Features

Securely share information with NHS and non-NHS organisations

Enables data analytics and risk stratification

Efficient system that exceeds IGTK requirements to optimise effectiveness

Hosted service at a secure ISO27001 accredited facility

Uses the surrogate NHS number as the primary patient identifier

Pseudonyms can be created where no NHS number exists

Controlled de-pseudonymisation available

Service access from any web browser

Full audit of all user activity

Full user training and helpline support

Benefits

Allows collation and consolidation of data from multiple sources

Effective enabler for data analytics, risk stratification, etc

Full security and confidentiality with controlled user access and log

Provides for more effective sharing through Pseudonymisation at source

Simple software installation for IGautopseudo

Simple and easy to deploy

Cost effective

View a case study here

IGsar - Subject Access Requests

Return to Overview

Subject Access Requests are increasingly being requested by patients or their representatives who wish to review their medical records.

This service facilitates the access of medical records via a secure web site link.

Features

- Full SAR lifecycle automation
- Capture of the Subject Access Request application and security credentials
- Uploading patient medical records from the physical case file/EPR /EDRM
- Case file access via a user-friendly screen set up
- Navigation and image management functions for medical records personnel and clinicians
- Patient medical records release approval process
- Notification that case file / medical records are available for viewing via the Patient Portal
- Download and print options along with simple and fast navigation functions
- Redaction capability
- Strong authentication security on records access

Benefits

- Increased efficiency
- Substantial stationery, printing and postage cost reductions
- Security improved over mailing paper or electronic media
- Hosting available on either our or your own infrastructure
- IG compliant access for citizens, patients and/or their authorised representatives
- Pre-built interface to local EDRM
- Cost effective

IGpaas - Platform as a Service

Return to Overview

Provides the highest level of security to Healthcare Service providers without the cost and timescales involved in developing and commissioning a secure platform for confidential patient data.

A secure service which can be deployed quickly and effectively to any of the 1.5 million NHS users without the need to engage with multiple authorities and stakeholders on deployment and IG issues.

Securely delivered in partnership with some of the world leaders in hosting, computing and security.

Fully compliant with regulations including: DPA (UK) 1998, EU Directives on Data Protection, SAS-70 (USA), FDA (USA), European Medicines Agency, FOI 2000, DoH and IGSOC 2 (IG Toolkit).

Protected by periodic penetration testing. IGspectrum's penetration testing services are accredited by the following organisations: CISSP CREST and CESG (CHECK).

Hosted 24 x 7 at secure facilities and managed by experienced BS27001 accredited support staff.

100% network and infrastructure uptime ensuring that your database is always up and running.

Ensures that your PaaS hosted configuration meets your required service levels and any back to back arrangements with your customers and partners.

IGsecurity - Application, Network and WIFI security testing

Return to Overview

Application Testing

Application security testing encompasses the use of manual and automated methods to detect internal and external threats and protect business applications and data, either in static or dynamic form. It emphasises the application fortification throughout the design, development, deployment, upgrade, and maintenance phases.

Our Application security services include scoping, identifying, assessing the security risks of the application/software product and identifying & recommending the risk treatment plans. The key stages are:

- Identifying application security vulnerabilities – manual & automated
- Simulating possible hacker scenarios to exploit the vulnerabilities
- Identifying the Impact and the possibility of the threat to determine the risk

Technical Testing – Key security Areas

- Input Validation. Buffer overflow; cross-site scripting; SQL injection; canonicalization
- Authentication. Network eavesdropping; brute force attacks; dictionary attacks; cookie replay; credential theft
- Authorisation. Elevation of privilege; disclosure of confidential data; data tampering; luring attacks
- Configuration management. Unauthorised access to administration interfaces; unauthorised access to configuration stores; retrieval of clear text configuration data; lack of individual accountability; over-privileged process and service accounts
- Sensitive information. Access sensitive data in storage; network eavesdropping; data tampering
- Session management. Session hijacking; session replay; man in the middle
- Cryptography. Poor key generation or key management; weak or custom encryption
- Parameter manipulation. Query string manipulation; form field manipulation; cookie manipulation; HTTP header manipulation
- Exception management. Information disclosure; denial of service
- Auditing and logging. User denies performing an operation; attacker exploits an application without trace; attacker covers his or her tracks

Test cases will be written that ensure complete coverage of the program logic. This requires a thorough understanding of the program i.e. we should know the specification and the code to be tested and knowledge of programming languages and logic.

Our security testing method is conducted to ensure the robustness of a system in the face of malicious attacks or regular software failures. White Box Testing (WBT) is performed based on the knowledge of how the system is implemented.

Return to Overview

Apart from regular vulnerability assessments WBT Includes:

- Analysing data flow
- Control flow
- Information flow
- Coding practices
- Exception
- Error handling

WBT helps in the knowing intended and unintended software/application behaviour and can be performed to validate whether code implementation follows intended design, to validate implemented security functionality, and to uncover exploitable vulnerabilities of the source code.

Network Testing

Our CREST/CISSP accredited testing will cover vulnerability and penetration testing and security attack simulations, as follows:

- Attempts on DNS zone transfers
- Enumeration of services
- OS detection and build version fingerprinting
- Password attacks
- Firewall traversal attacks
- Checks for anonymous access and file/folder privileges
- Configuration files will be searched and access attempts
- Enumeration command support
- Email spoofing and mail / web/ relay tests
- Web crawls, method support and web directory enumeration
- Back-door discovery attempts
- Upload attempts
- Subject to applications visible, specific testing of collaboration services
- Input validation attempts (null access, SQL injection, basic cross site scripting checks, http splitting)

Wi-Fi Testing

Our Wi-Fi testing programme is extremely effective for testing and improving the security surrounding networks and systems. Security weaknesses are identified and managements' attention is drawn to the need for improvement. The weaknesses exploited become focal points and are used to help develop a plan of improvement for the overall system of information security, rather than simply "applying a patch" on isolated weaknesses.

Return to Overview

The purpose of the Wi-Fi security penetration test is to gain access externally into the customer's network without causing any service disruptions to the customer's IT assets. We start with little knowledge of Customer's systems. The key phases are:

- Discovery / Identification
- Vulnerability assessment
- Exploitation and Penetration activities

A detailed description of the above-mentioned phases is provided below:

Discovery / Identification

This exercise is carried out with zero knowledge of the network. The following methodologies will be employed to evaluate the external security exposures related to the network access points.

During this phase we enumerate and gather information that helps us in exploiting the vulnerabilities. Activities include the following:

- Identifying and sniffing access points
- Attempting bypass and brute-force attack techniques
- Sizing the network and identifying the associated hosts

Vulnerability assessment of internet infrastructure

Activities performed during this phase include the following:

- Using of "port scanning" software to determine the open service ports on any device connected to the Internet

- Connecting to service ports on the identified devices trying to gain enticement information such as the type(s) of operating system(s) and application(s) in use based on the banner information

- Utilising "vulnerability scanning" tools to assist in assessing the vulnerabilities present in the network

- Vulnerability assessment of Internet facing systems for misconfigurations or known vulnerabilities

Return to Overview

Exploitation and penetration activities

Based on identified access points and known vulnerabilities, we examine access points in an attempt to gain access to the internal network. The following techniques will be used during this phase:

- Manual and automated penetration techniques will be performed to exploit inherent weaknesses in the wireless access points in an attempt to gain unauthorised access or to penetrate other hosts that have a "trusted relationship" with the host that we are attempting to penetrate

- Identifies security weaknesses and exploits to gain access will be tried using attack tools

Reporting

Critical issues, if identified, will be reported immediately to ensure the organisation is aware of the issue. We will propose solutions as required, following discussion.

Our final report will contain a detailed list of identified issues and suggestions to fix issues including:

- Management summary
- Scope of the assignment
- Tools utilised
- Output of tests performed
- List of identified issues
- List of action points and fixes to be implemented

Benefits

Business benefits of our wireless LAN penetration testing include the following:

- Identifies vulnerabilities and risks in your wireless network infrastructure
- Validates the effectiveness of current security safeguards
- Quantifies the risk to internal systems and confidential information
- Raises executive awareness of exposure to corporate liability directives
- Provides detailed remediation steps to help prevent network compromise
- Determines security weaknesses and misconfigurations through a comprehensive vulnerability assessment of the infrastructure
- Conducts technical testing by security experts who have strong background in vulnerability assessment, penetration testing and risk assessment
- Provides a targeted, cost-effective code review to identify vulnerable areas
- Provides a detailed report with recommendations for mitigating discovered risks
- Knowledge that we adopt best practice from globally recognised standards/benchmarks and we have access to the most recent vulnerability and threat research information

London based CCG Case Study

IGspectrum
IT for Health

IGpseudo

A London CCG project, led by a London Council and involving three London Trusts, a third party health analytics company and IGspectrum:

Objective: Meet the challenge of reducing hospital readmissions (within 30 days) for the older people’s cohort

- Risk stratification was the chosen approach - primary issue was meeting IG requirements and accessing data in a timely manner (HSCIC data was deemed not current enough)
- Chosen approach was to pseudonymise the PCD and sent to the health analytics company for Risk stratification
- GPs receive reports showing at risk patients and service users
- Interventions are then planned and managed

Return to IGpseudo

Risk Stratification

The way it works:

- All 3 hospitals and Adult Social Care use the same pseudonymisation tool (IGpseudo) to send their data to the health analytics company (via N3 to the companies portal) twice a month in an Excel or CSV file.

- To minimise the work involved, data extracts tie in with when SUS data is sent to the HSCIC.

- GPs will send identifiable data to the health analytics company who pseudonymise it on receipt using IGpseudo.

  - It is legal for the company to access identifiable patient data because they are doing so as a data processor under contract to the CCG.

Return to IGpseudo

- GPs have also signed DSAs with the CCG.

Risk Stratification

The way it works:

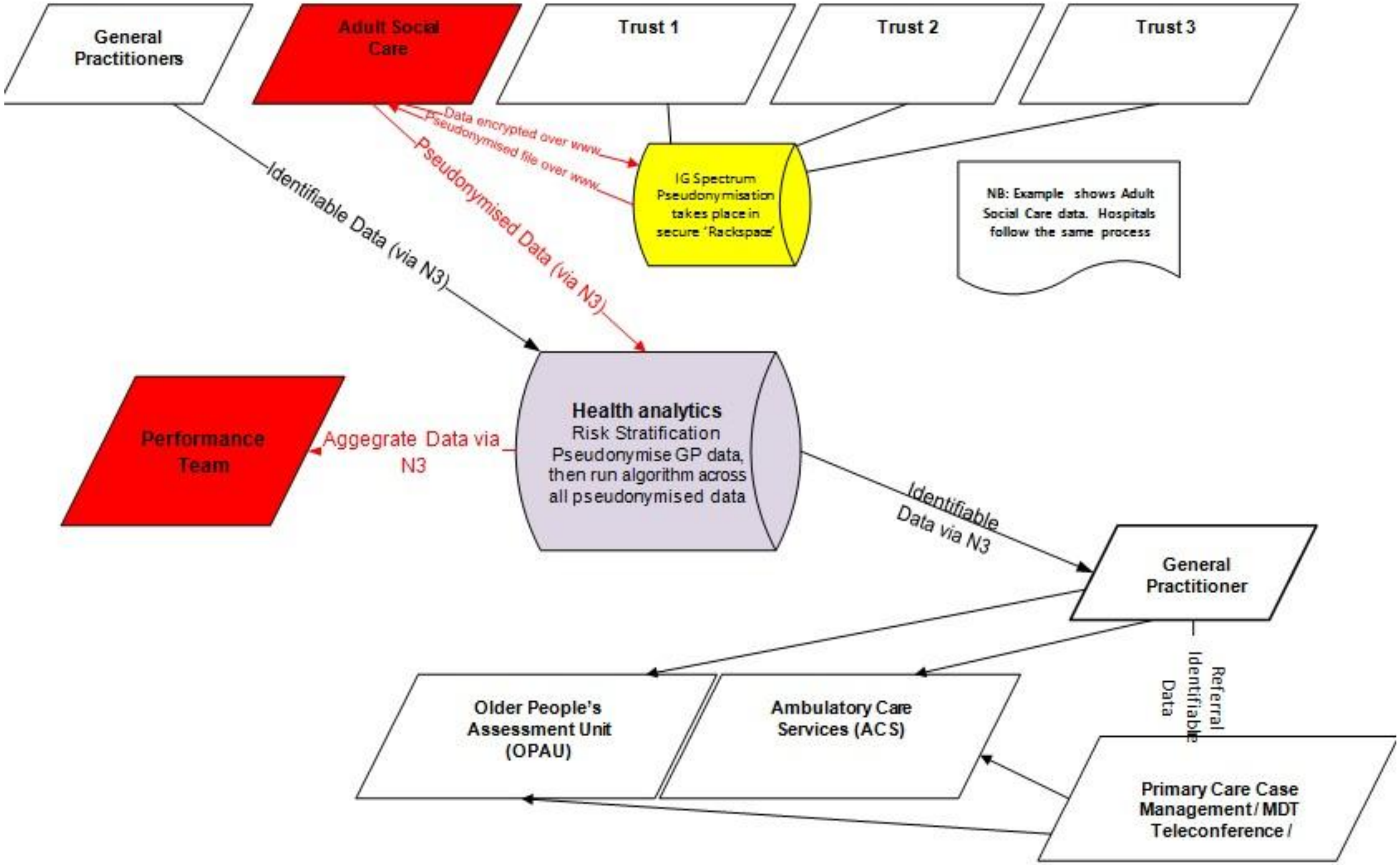
- Output is sent from the health analytics company (via N3) to GPs in identifiable format.
- GPs will only have access to identifiable data about their own patients.
- GPs will then make referrals to the MDT (and Older People’s Assessment Unit, a trust Ambulatory Service for Older People).
- All partners will be able to request pseudonymised reports fromthe health analytics company
- All partners can request variations of algorithms and reports to berun for a variety of purposes
- All IG requirements are met

Return to IGpseudo

Data Flow

IGspectrum
IT for Health

IGpseudo



General Practitioners

Adult Social Care

Trust 1

Trust 2

Trust 3

Data encrypted over www

Pseudonymised file over www

IG Spectrum Pseudonymisation takes place in secure 'Rackspace'

NB: Example shows Adult Social Care data. Hospitals follow the same process

Identifiable Data (via N3)

Pseudonymised Data (via N3)

Health analytics
Risk Stratification
Pseudonymise GP data, then run algorithm across all pseudonymised data

Performance Team

Aggregate Data via N3

Identifiable Data via N3

General Practitioner

Referral Identifiable Data

Older People's Assessment Unit (OPAU)

Ambulatory Care Services (ACS)

Primary Care Case Management/ MDT Teleconference /

Return to IGpseudo