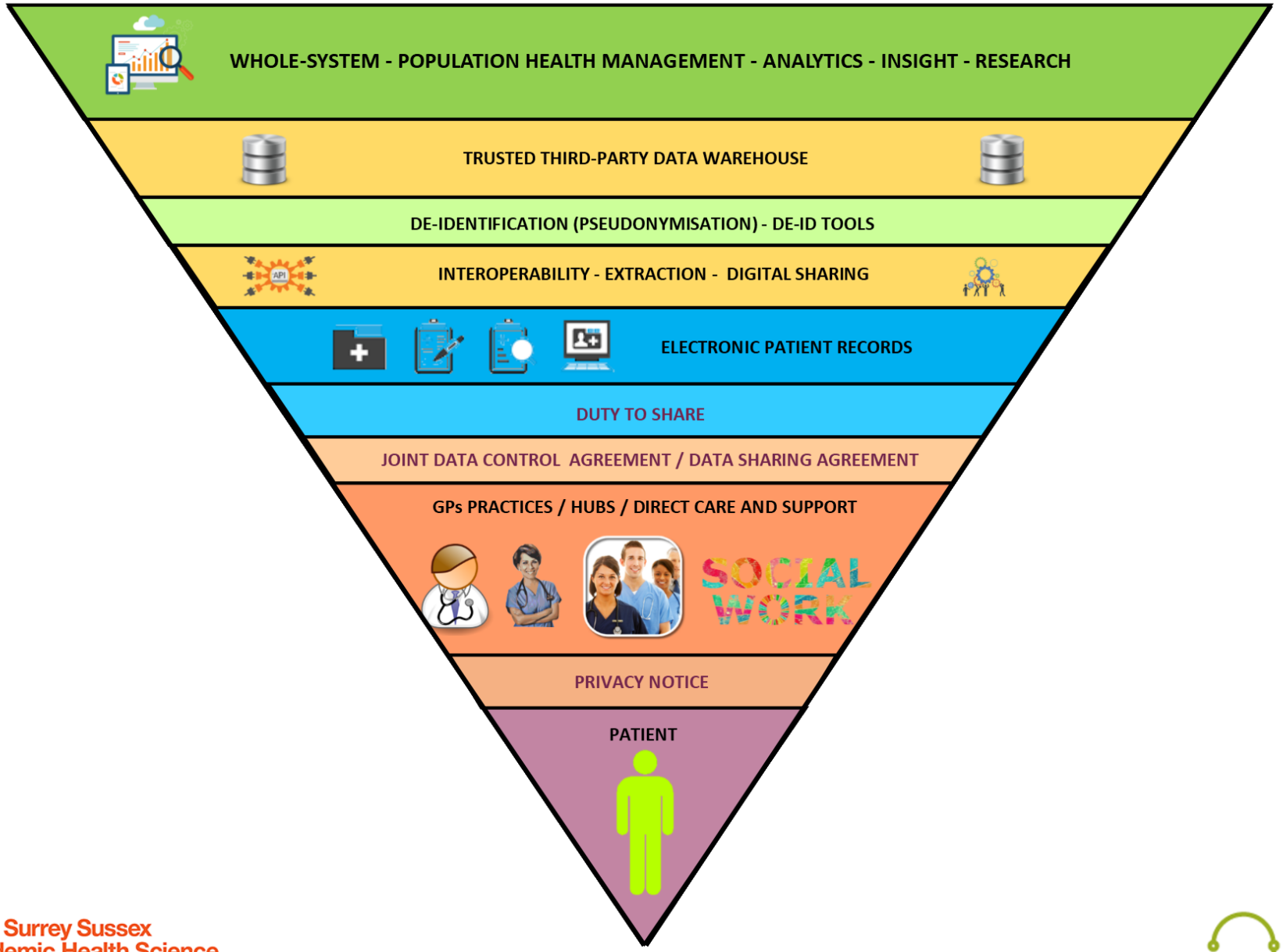
# IG: A PLAYBOOK

ALAN DAY


Kent Surrey Sussex
Academic Health Science
Network

BEAUTIFUL
INFORMATION




Kent Surrey Sussex Academic Health Science Network

www.beautifulinformation.org

# GDPR / DPA 2018

- Health and social care purposes now set out in law.
- Lawful basis for processing has changed.
  - **Consent**[1] – No longer required, replaced with a **Right to Object**[3]
  - **Public Task**[2] – Most Public Authorities expected to use.
  - **Legitimate Interest** - no longer a lawful basis for public authorities[4].
- **Transparency** – statutory content in Privacy (Fair Processing) Notices.
- **Data Protection Impact Assessments** – statutory (i.e. no screening)
- **Indirect Acquisition** - additional obligations must be met by recipient[5]
- **Contractors** – no processing without instruction[6]
- **Records of Processing** - Duty to document processing[7]

1. Art.6(1)(a) 2. Art.6(1)(e) 3. Art 21(1) if Public Task purpose 4. Art. 6(1) 5. Art. 14 6. Art. 28 7. Art. 30

# CONTROL

## Controller[1]

"Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"

## Joint Controllers[2]

"Where two or more controllers jointly determine the **purposes and means** of processing, **they shall be joint controllers**"

1. Art. 4(7)
2. Art. 26

# RESPONSIBILITY

Processing of personal data relating to an individual's health or social care data must be "under the responsibility of"[1] "… a health professional or a social work professional …"[2]

- List of professionals can be found in DPA2018
- Health professional includes '… scientist employed by a health service body as head of department'[3].
- This 'responsibility' holds the professional and individually accountable for their actions to their professional body.

1. Art.9(3)
2. DPA2018 s11(1)
3. DPA2018 s204(1) and (2) respectively.
4. DPA2018 s204(1)(k)

# ROLES

- Health or Social Work Professional.
- Caldicott Guardian - ‘necessity and proportionality’
- Senior Information Risk Owner (SIRO) - ‘safety and security’
- Data Protection Officer ‘ - inform, advise and monitor’

# DUTY OF CONFIDENCE

GDPR makes sense of reality, i.e. there is no realistic court remedy - requires a general tort of breach of confidence (without legal aid).

Of the few cases, complaints are made to the professional and their professional body (ICO doesn't handle breach of confidence, only breach of data protection principles).

Professional body can sanction which is usually a pre-requisite for settlement against an individual or their NHS employer.

Few end up in court.

# LAWFUL ANALYTICS PURPOSES

- Management (Health or Social Care Systems / Services)
- Public Health
- Scientific Research
- Approved Medical Research
- Statistics
- Archiving

# DATA TYPES - RAG

| RED | Confidential information containing identifiers |
|---|---|
| AMBER | De-identified (pseudonymised) row-level data held in a controlled environment |
| GREEN | Large groups or completely anonymous data |

# PSEUDONYMISATION

ICO Anonymisation: managing data protection risk code of practice. Ch.7 recognises processing of row-level pseudonymised data without consent provided access and dissemination is restricted to those processing.

Pseudonymisation typically replaces NHS Number with a ‘digest’ using an algorithm e.g. 123 234 3456 might become

15e2b0d3c33891ebb0f1ef609ec419420c20e320ce94c65fbc8c3312448eb225

SALT – adding a secret word to NHS No. to prevent reverse engineering.

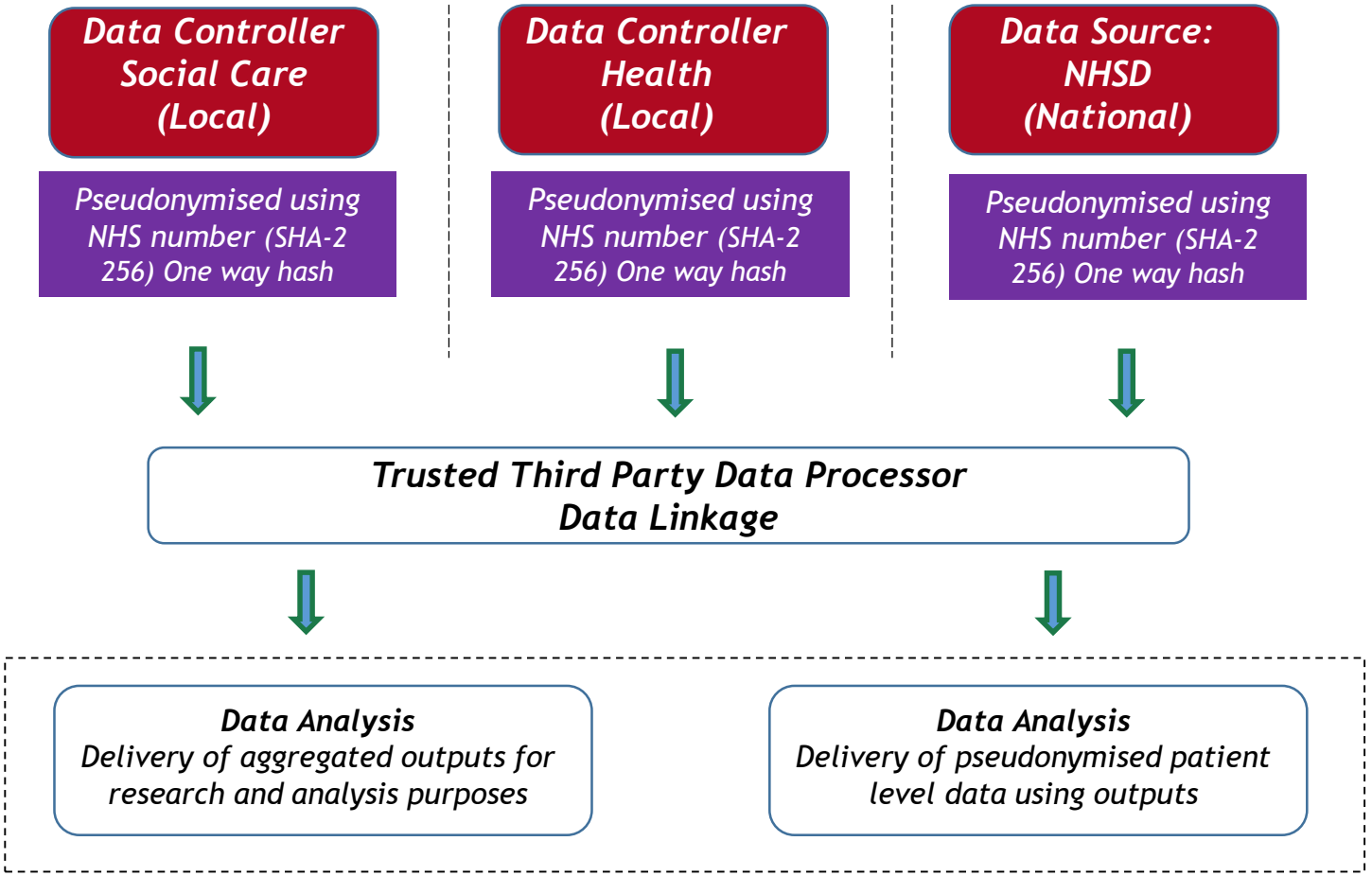
Enables data linkage without identifying individuals.

Technical skills thin on the ground.

Various tools, some free (e.g. Open Pseudonymiser).

Pseudonymise-at-source wherever possible.

# Trusted Third Party Model



# IG PLAYBOOK

GOVERNANCE

CONTROL

PURPOSE

PATTERNS

PRODUCTS

COMMUNICATIONS AND ENGAGEMENT

# IG PLAYBOOK - GOVERNANCE

## Terms of Reference

- If Board or Partnership; ensure it adequately represents controllers.
- Data-items held in should be attributable to an owner (generally the data provider for acquired data).
- Operating Model and overarching DPIA.

## Project Management

- DPIA for each project.
- Operating Procedures for assurance and sign-off.
- Transparency, communications and engagement.

# IG PLAYBOOK - CONTROL

## CONTROL

If you have a Board or Partnership, do they independently decide purposes and means on a project-by-project basis (i.e. no business-as-usual activity)? If so, they retain individual control.

If business-as-usual reports are produced from pseudonymised and linked data, it is likely to be Joint Control (i.e. joint purpose and means) unless access is restricted to TTP staff only.

# IG PLAYBOOK - PURPOSE

STATE YOUR PURPOSE(S) IN TERMS OF THE LEGAL BASIS

- Management (systems and services) - ????
- Public Health - ????
- Scientific Research - ????
- Statistics - ????

Avoid waffle and don't invent 'novel' purposes.

Purpose statements – short, pithy, not more that a short paragraph.

# IG PLAYBOOK - PATTERNS

The concept of Patterns comes from Enterprise Architecture and equally apply to Data Architecture. They are standard ways of doing things.

Create a catalogue of Patterns for:

- Methods of extracting data (e.g. ODBC/API etc.)
- Pseudonymisation techniques (SHA256 forward #) + Salt
- Transport (e.g. via HSCN, VPN, SSL etc.)
- Quarantining on landing.
- Information Risk Assessments Etc.

# IG PLAYBOOK - PRODUCTS

**Privacy Notices**

Model clauses for controllers

Links to standard explanations etc.

If research, use the links to HRA standard resources.

Machine-readable registry of controller Privacy Notices.

**DPIAs** – re-usable boilerplates designed for the relevant purpose and lawful basis (ICO advice).

**Patterns** – if you use the same 'means' re-use patterns.

**Contacts** - List of controllers: DPO; SIRO; CG; IG Lead.

**Process** - Use online forms for consulting IG contacts.

# IG PLAYBOOK - COMMS

## Publish

- Purpose(s) clearly and unambiguously.
- Principles that underpin how projects are ranked and pipelined.
- Candidate and current projects – show the pipeline.
- DPIAs

## Articulate Benefits.

- To individuals (e.g. prevention / risk stratification)
- To the public
- To public service organisations.

## Engage

- Patient Participation and Advisory Groups
- Healthwatch
- Other

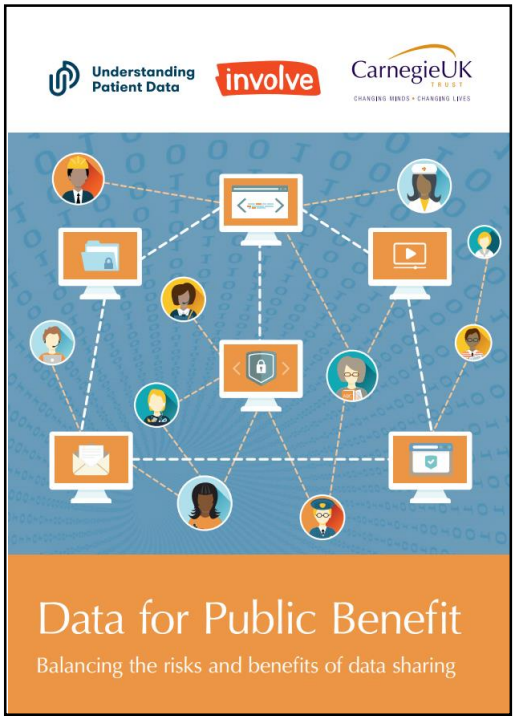
# INVOLVE

## Data for Public Benefit

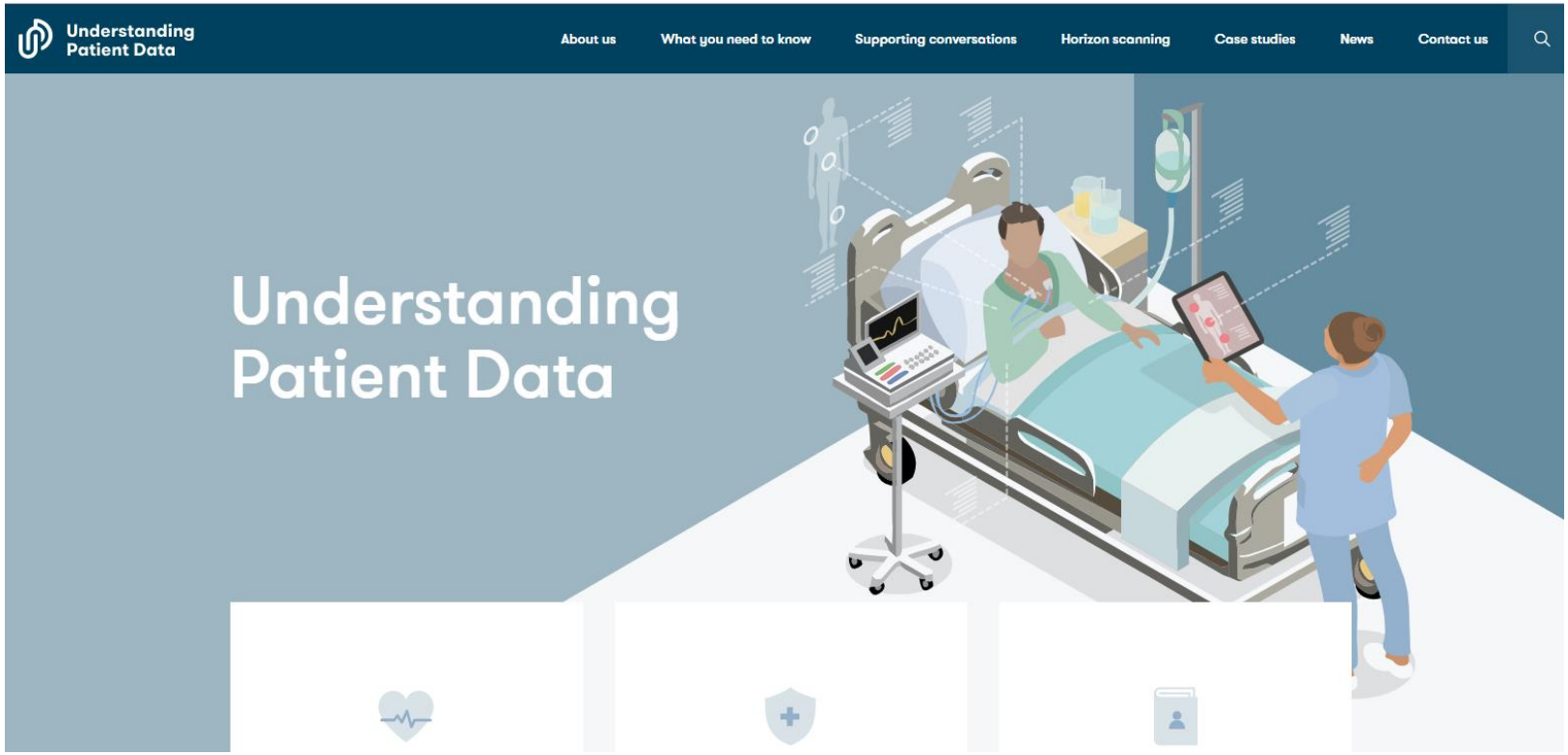
Three conditions for effective data use.

- Purposeful.
- Proportionate.
- Responsible.

Includes a framework for assessing the merit of a data sharing activity to deliver public benefit.



# UNDERSTANDING PATIENT DATA




Kent Surrey Sussex Academic Health Science Network

www.beautifulinformation.org

# QUESTIONS