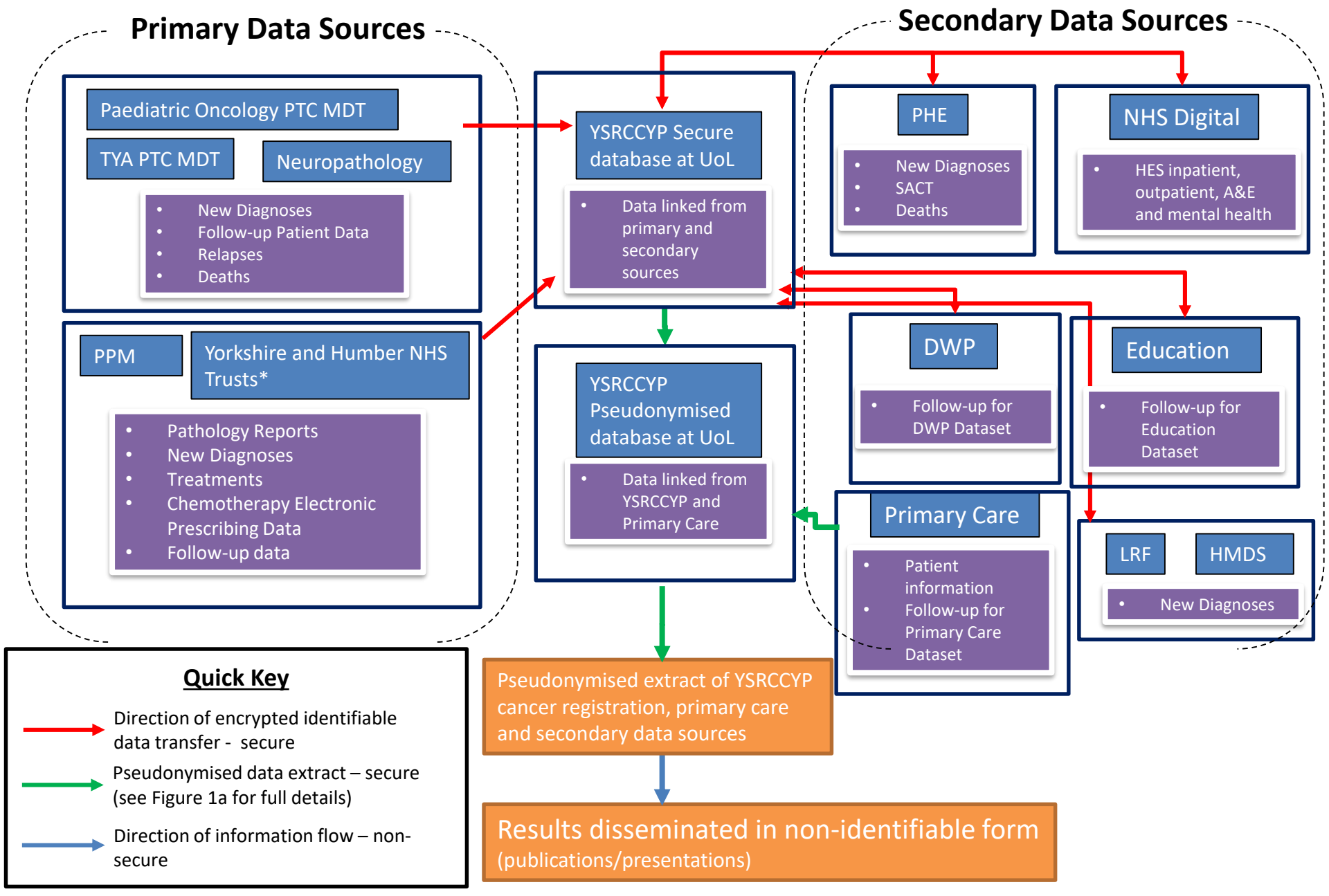
Figure 1: Yorkshire Specialist Register of Cancer in Children and Young People (YSRCCYP) Data Collection Flow overview (Oct 2019)



Appendix:

LTH – Leeds Teaching Hospitals
PTC – Principal Treatment Centre
MDT- Multidisciplinary Team
PPM/PPM+ - Patient Pathway Manager – LTH electronic patient information database
TYA – Teenage and Young Adult
HMDS – Haematological Malignancy Diagnostic Service
PHE – Public Health England
HES – Hospital Episode Statistics
SACT – Systemic anti-cancer therapies dataset
LRF – Leukaemia Research Fund
DWP – Department for Work and Pensions
Primary Care – Data that is taken from ResearchOne (a research database held by The Phoenix Partnership, TPP), EMIS Health, and other primary care IT providers.


= Data Source

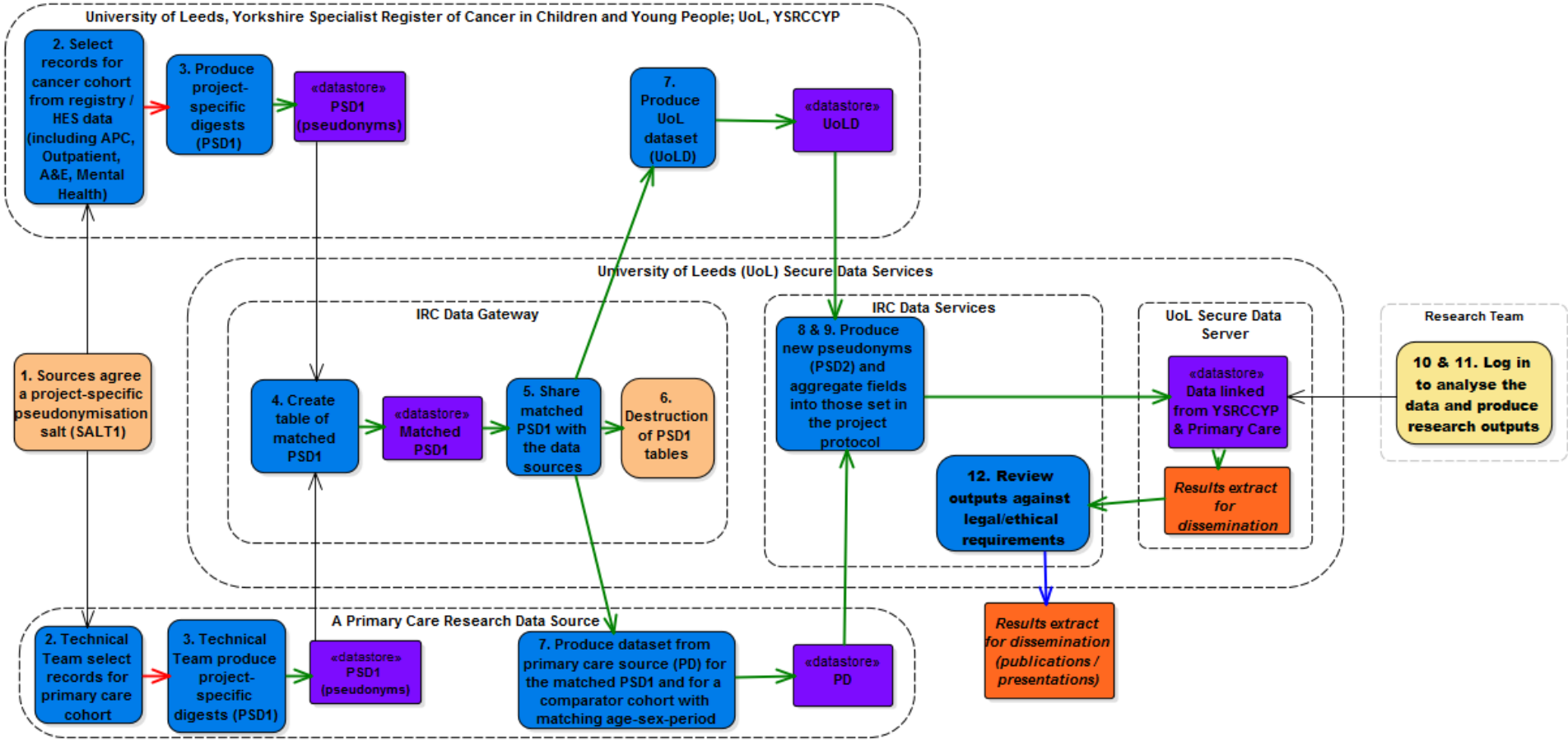

= Data Type


= Output

Yorkshire and Humber NHS Trusts*

- Airedale NHS Foundation Trust
- Bradford Teaching Hospitals NHS Foundation Trust
- Calderdale and Huddersfield NHS Foundation Trust
- Harrogate and District NHS Foundation Trust
- Hull and East Yorkshire Hospitals NHS Trust
- Mid Yorkshire Hospitals NHS Trust
- North Lincolnshire and Goole NHS Foundation Trust
- Sheffield Teaching Hospitals NHS Foundation Trust
- South Tees Hospitals NHS Foundation Trust
- York Teaching Hospital NHS Foundation Trust

Figure 1a: Yorkshire Specialist Register of Cancer in Children and Young People (YSRCCYP) Primary Care Data Flow (Oct 2019)



SEED Technical Data Storage Overview

The Secure Electronic Environment for Data (SEED) facility is a secure data management infrastructure run centrally by IT. This allows for safe storage and access to personal identifiable sensitive data, subject to individual consent or the relevant approval to set aside consent in the case of medical research. The facility allows secure remote data entry and reporting over the web and a safe environment for data processing and analysis. Data in the facility is clustered for resilience, backed-up nightly and can be encrypted if required.

The SEED system is a firewall-protected private network containing database and file servers. The firewall blocks all network traffic from the University of Leeds campus network except from authorised users of the SEED system who connect from the University of Leeds network via a Virtual Private Network (VPN) connection. The VPN connection encrypts all network traffic between the authorised user's PC and the SEED system. The campus border firewall blocks all network traffic from the internet to the SEED system firewall. The device used to access the SEED system must be organisationally owned, managed and maintained.

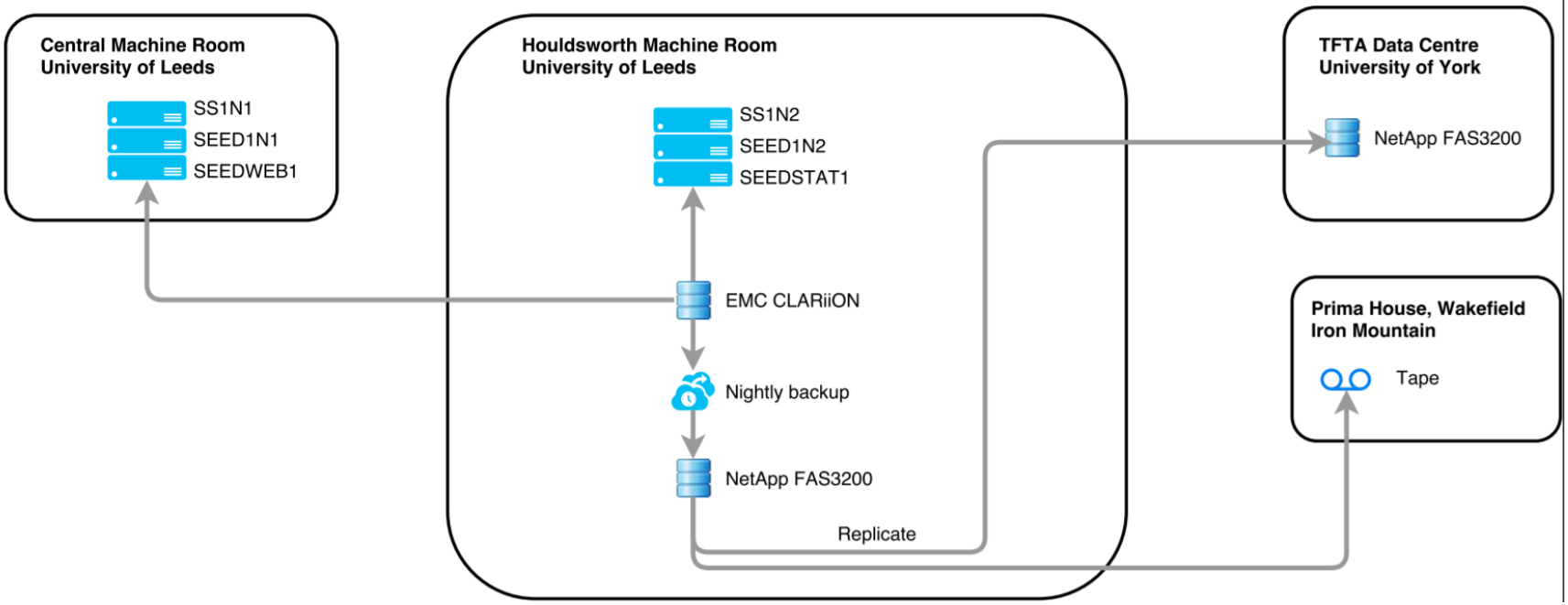
The SEED system is subject to, and its own Information Governance Policy extends operationally, both the Information Security Policy and the Information Protection Policy of the University, available online at http://it.leeds.ac.uk/info/116/policies. These policies, together with other related guidance materials, identify the actions, managerial responsibilities, confidentiality requirements and information security management measures for the SEED system.

Full data access policies and responsibilities are listed within the SEED Information Governance Policy, specifically sections 7.17.2 (Physical and Technical Security) and Appendix 4 (Summary of an individual's responsibilities). In summary, only those essential members of staff working on an information asset who require direct access will be granted authorisation. All users of the SEED system must sign a confidentiality agreement, which includes stipulating that security and confidentiality must be maintained.

Access to University of Leeds computing resources is controlled by the University's Microsoft Active Directory through login IDs and passwords. Access to information assets is authorised by the Responsible Owner of the asset (also known as the Information Guardian) and is granted by the Information Governance Lead (also known as the Data Custodian). All information assets require a credential check on log in. Identifiable data within the database are encrypted. All staff are fully trained in dealing with sensitive and confidential data, including their responsibilities to maintain patient confidentiality.

The SEED system has been assessed via the NHS Information Governance Toolkit, using the v11.0 requirements for a Hosted Secondary Use Team/Project. It has been judged satisfactory, at Level 2.

SEED Physical Architecture v1.0
Initial Version 26/11/2013



Key

Server

Database

Users with access to data (Oct 2019):

- Richard Feltbower
- Lesley Smith
- Benjamin Fox
- Nicola Hughes
- Amanda Friend