UCL INFORMATION SERVICES DIVISION
IT for SLMS

Developing a coordinated organisation-wide approach & tools for submitting research IGT applications

Trevor Peacock

2nd July 2014

Which approach suits your organisation?

- Secondary Use Organisation (SUO)
  - 30 requirements in 5 categories
  - covers the whole organisation

- Hosted Secondary Use Team / Project (HSUT/P)
  - 14 requirements in 3 categories
  - covers a team or study within a larger organisation
  - Can have local or centrally managed elements eg. governance, IT systems

Need to define the scope of the ‘organisation’: study, department or whole org

Each model has overheads for different parts of the organisation

The UCL model

- IG framework for the School of Life & Medical Sciences (SLMS)
  - Large organisation, SLMS is 60% of UCL 5,000-6,000 staff, ~3,000 honoraries
- Adopted the HSUT/P for studies within the SLMS
- Centralised governance structure
  - SIRO appointed
  - IG Steering group and IG Lead to manage the framework
  - Studies adopt the IG framework with IG responsibility delegated to PI
- Support services
  - Dedicated research IT infrastructure for sensitive data
  - Training and awareness – rolling programme of introductory training events
  - Advisory Service – supports studies in adopting the IG Framework and IGTK submissions

Supporting IG Toolkit submissions

- Aim to streamline the activities required to submit
  - Central management of the IG Framework
  - Develop multipurpose tools
    - Information Risk Assessment Tool covers risk, transfers, and asset register
    - Physical Risk Assessment covers physical security and working practices
  - Tie-in to existing policies and processes wherever possible
    - Information Security Team - incidents
    - Data Protection Office – incidents, non-EEA dataflows, contracts
    - Legal services - contracts
    - Estates Security – physical security
    - HR - contracts
  - Study Improvement Plan
    - Derived from Information and Physical Risk Assessments plus Confidentiality Audit

Activities

- IG Steering Group
  - Decision making
  - Monitoring of progress
  - Escalation route
- Training & awareness
  - Training delivery, record keeping and effectiveness monitoring
  - Induction and awareness materials
- Advisory Service
  - Guidance, assessment and assistance
- Technical Solution
  - Onboarding, monitoring, testing
- Incident management
  - Technical and information incidents: Confidentiality, Integrity and availability

Advisory Service: Tools

- Information Risk Assessment Tool
  - Information asset register
  - Records attributes of data and transfers
  - RAG risk assessment
  - Highlights improvement actions
- Physical Risk Assessment Tool
  - Physical risks
  - Operational risks
- Template letters from PI
  - Promote training, confidentiality audit, incident reporting, IG Policy etc
  - Confirm appropriate pseudonymisation, contracts, adherence to IG Policy
- Documents on intranet
  - NDA, pseudonymisation advice, remote access, policies and guidance
- Completion template
  - Standard responses for researchers to use

Shopping list

- Buy-in from senior management in the form of a SIRO
- Resources to support the process:
  - Training
  - Demonstrably fit-for-purpose IT
  - Someone to manage it all
  - Other parts of the organisation: HR, Data Protection, InfoSec, Estates
- Risk framework
  - Link in to organisational risk assessment framework, don't invent your own

What a UCL SLMS researcher submits

- The cut-and-paste-o-matic
  - a spreadsheet containing standard UCL responses to the IG Toolkit

Discussion

- Senior buy-in
- SUO or HSUT/P
- Resourcing it all!
- Audit - who performs this function?
- Local improvement plan
- Providing research-centred training (IGTT isn't ideal)
- People from within the organisation but outside of 'the organisation'
- Team IGTK submissions – ensuring IG is managed properly within that team
- Making it too much of a tickbox exercise for researchers
- Submitting IG Toolkit before receiving the data eg. S251
- ISO27001?