UCL Information Governance Framework

Trevor Peacock
UCL School of Life and Medical Sciences

NHS-HE Forum, 28th November 2013

UCL IG Framework

- Where we've got to
- The IG Framework
- Services to support the IG Framework
- IG Toolkit submission process
- Next steps

UCL background

- Almost all of UCL's medical research takes place in the School of Life and Medical Sciences (SLMS)
- SLMS makes up ~55% of UCL (~3,500 staff)
- Working with four main NHS trusts plus others
- Significant number of projects come under ECC section 251
- Over 580 research DP registrations within SLMS for 2012-13
- SLMS Identifiable Data Handling Solution (IDHS) project began in 2012
- Presentation at Nov 2012 NHS-HE forum setting out our plan to address this
- IT for SLMS restructure in August 2013 provided dedicated resource for Information Governance

Where we've got to

- Senior Information Risk Owner (SIRO) appointed
- IG Lead appointed
- Information Governance structures in place
- Three services to support the IG framework:
  - IDHS (Technical infrastructure)
  - Training and Awareness
  - IG Advisory
- Services went live at the beginning of September

Some figures...

IG Toolkit submissions		
Published	6	Plus one scheduled for publication this week
In progress	11	Registered and submitting evidence
Engagement	10	Beginning the process of collecting evidence
Others	5	Registered outside of the process (historic)
Miscellaneous	1	Department for Education National Pupil Database: using IG Toolkit as framework for submission

Training and awareness		
Roadshows	5	Another scheduled: Feb 2014
Staff / students	191	Staff received training through roadshows
IT staff	66	Staff trained, one more session scheduled
IG Training tool	259	Passed the ‘Introduction to IG’ module

IDHS (technical environment)		
Groups migrated	7	Operating a ‘migrate then IG Toolkit’ policy

SLMS IG Framework

- SLMS IG framework consists of policy, procedures and guidance materials
- Using Hosted Secondary Use Team / Project as a standard for assurance
- Owned by SLMS SIRO
- Managed through Information Governance Steering Group
- Supported by IG Lead
- Provides standard answers for much of the IG Toolkit

SLMS IG Framework

Roles and responsibilities

Senior Information Risk Owner (SIRO)

Member of Senior Executive Group: responsibility for ensuring that information risk does not impact the strategic academic goals of the SLMS

Information Governance Steering Group (IGSG)

Supports and drives the broader IG agenda, ensuring effective management of information risk assurances that best practice mechanisms for IG are in place

Information Governance Lead

Coordinates IG work programme: ensures effective management, accountability, compliance and assurance for all aspects of IG

Information Asset Owners (IAOs)

Individual assigned ownership of a specific information asset and responsible for ensuring that it is properly protected and that its value to the organisation is realised. Typically the research study **Principal Investigator** in receipt of data obtained either directly from the research subjects or from a partner organisation (i.e. the NHS)

Documentation

Set of documents, approved by the IGSG, covering:

- Roles
  - SIRO, IG Lead, IGSG Terms of Reference
- Policies
  - SLMS IG Policy, Confidentiality Code of Conduct, Remote Access Policy
- Procedures and guidance
  - Pseudonymisation, Training Needs, Incident Reporting, Remote Working, Confidentiality Audit
- Contracts and agreement templates
  - NDA, Information Sharing Agreements, UCL Contracts Audit, Information Risk Assessment, Physical Risk Assessment

Services

Services to support the SLMS IG Framework:

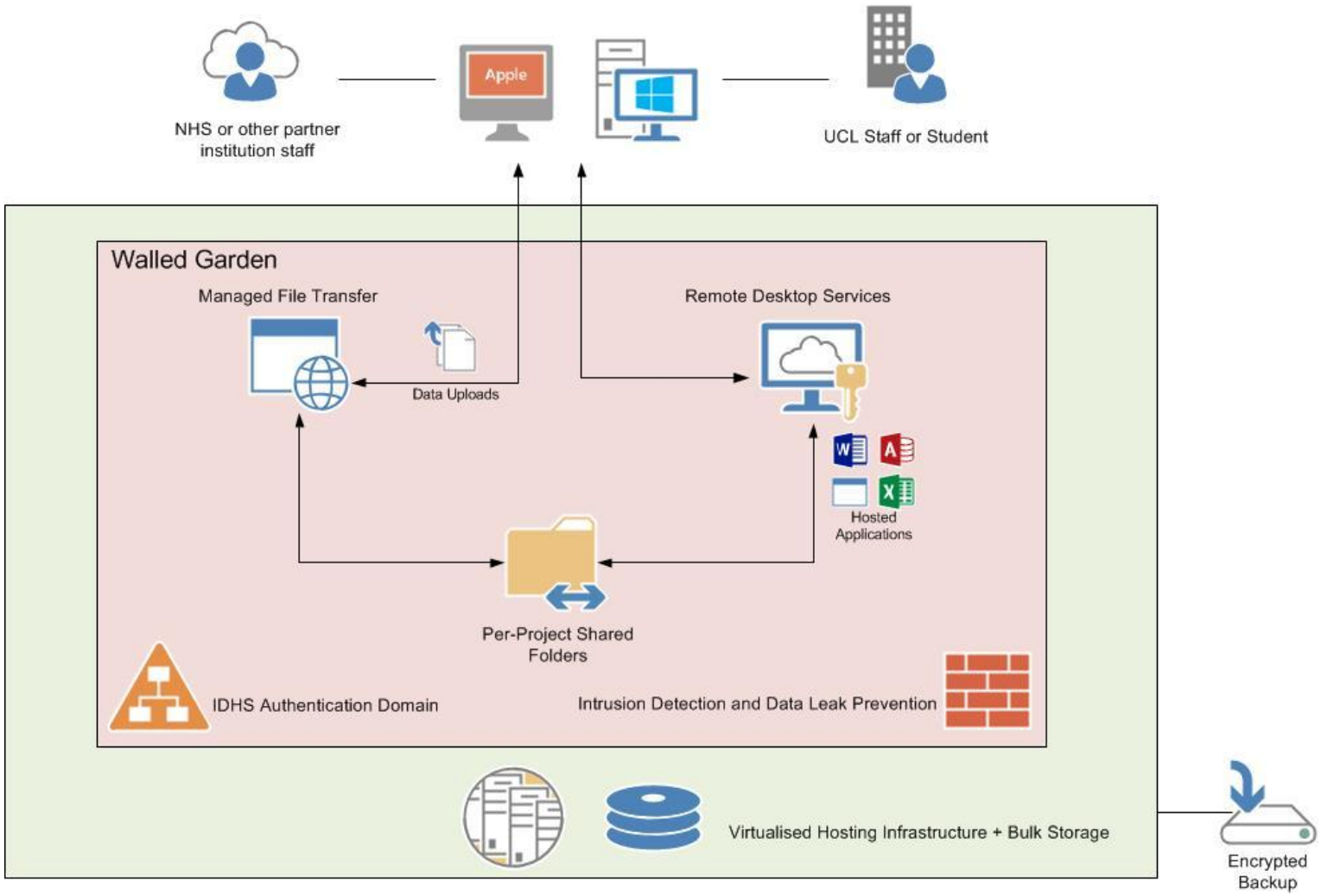
- IDHS – technical infrastructure
- Training and awareness
- IG Advisory service

Service: IDHS environment

IDHS key features

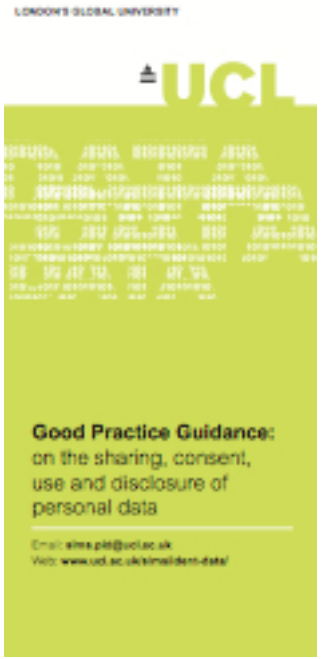
- 'Walled garden' model, separate from other systems
  - own data centre with physical access limited to small group of systems administration staff
- Penetration tested by external company
- 2-factor authentication (token or smartphone app)
- Thin client
  - no copy and paste between environment and local PC
  - no file transfer between environment and local PC
- Secure file transfer system
  - file dropped to staging area
  - automatic process moves file from staging area to internal filesystem
  - all outbound transfers need to authorised by PI or delegate
- Audit trail for all file operations
- Encrypted backups stored off-site

Service: IDHS environment



Service: Training and Awareness

- Roadshows, which include introductory IG awareness training
- Management of the CfH IG Training Tool for SLMS
- Record-keeping
- Outreach
- Leaflets and posters



Service: IG Advisory

Guiding PIs through:

- Assessing risks
- Identifying actions to mitigate those risks
- Internal audit
- IG Toolkit submissions

Aim is to make IG Toolkit submission a streamlined process – reducing workload for research teams

- Tools to:
  - capture information assets and risks
  - capture physical risks and mitigation procedures
- Templates:
  - Improvement plan
  - email from PI to team covering policies, procedures and need for training
  - email from PI to IG Lead confirming requirements met in terms of contracts, use of pseudonymisation etc

IG Toolkit submission: how it works

Information Governance Management		SLMS IG	IRAT	PRT	email to IG Lead	email to staff	Conf. audit
11-120	Responsibility for Information Governance has been assigned to an appropriate member, or members, of staff	✓					
11-121	There is an information governance policy that addresses the overall requirements of information governance	✓			✓		
11-122	All contracts (staff, contractor and third party) contain clauses that clearly identify information governance responsibilities	✓			✓		
11-123	All staff members are provided with appropriate training on information governance requirements	✓				✓	
Confidentiality and Data Protection Assurance							
11-220	Personal information is only used in ways that do not directly contribute to the delivery of care services where there is a lawful basis to do so and objections to the disclosure of confidential personal information are appropriately respected	✓				✓	
11-221	There are appropriate confidentiality audit procedures to monitor access to confidential personal information	✓				✓	✓
11-222	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	✓	✓				
11-223	All transfers of personal and sensitive information are conducted in a secure and confidential manner	✓	✓				
Information Security Assurance							
11-330	Policy and procedures ensure that mobile computing and teleworking are secure	✓					
11-331	There is an information asset register that includes all key information, software, hardware and services	✓	✓				
11-332	Unauthorised access to the premises, equipment, records and other assets is prevented	✓		✓		✓	
11-333	There are documented incident management and reporting procedures	✓				✓	
11-334	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	✓			✓		
11-335	There are adequate safeguards in place to ensure that all patient/client information is collected and used within a secure data processing environment (safe haven) distinct from other areas of organisational activity	✓					

IG Toolkit submission: how it works

Initial meeting with PI

- Establish facts about study
  - s251, non-UK data flows, 3rd party contracts
- Run-through of the risk assessment tools and emails
  - PI completes the assessments and sends emails
- Register study team to use the IDHS
- Register study ODS code for the IG Toolkit
- Populate most of the IG Toolkit, including actions for the PI
  - spreadsheet of standard responses, so can be passed to the PI to cut and paste
- IG Lead reviews risk assessment tools
  - requests additional information (eg 3rd party contracts)
  - amends / suggests actions for improvement

IG Toolkit submission: how it works

Follow-up meeting

- Review details in assessment tools
- Review IG Toolkit elements, updating as necessary
  - gaps or actions added to study improvement plan

Confidentiality Audit

- Covers:
  - staff awareness, recording of consent, storage and transfer of information (paper and electronic), physical access control etc
  - record outcome

IG Lead updates IG Toolkit with audit evidence

- IG Toolkit submission is published (takes 5-10 days)

IG Lead updates reports for IGSG

- non-UK data flows, Improvement plan, SIRI (if necessary)

Next steps

IDHS

- Expansion: capacity, capability and resilience
- ISO27001 accreditation

Training and Awareness

- Use of self-led material
- Looking at USB stick amnesty and encryption clinics

Advisory Service

- Better links with grant application process and Information Security team
- Liaising with Exeter Helpdesk to look at UCL ‘master set’ of evidence, with individual studies submitting differences

Summary

- Built a repeatable process that is flexible enough to cover all UCL IG Toolkit submissions
- Simplifies process for research teams, reduces their workload
- ‘Flat pack’ model could be used elsewhere
- For the scale of SLMS, dedicated resource was needed
- Governance structures needed strong backing by senior management
- ‘Fit for purpose’ IT environment simplifies matters

Questions?

https://www.ucl.ac.uk/isd/itforslms/services/handling-sens-data

t.peacock@ucl.ac.uk