NHS
National Institute for
Health Research

Clinical Research Network

IG Statement of Compliance

CRNCC and University of Leeds

Supporting research to make patients, and the NHS, better

Introduction to IG and its relation to CRN

- IGSoC - a range of security related requirements which must be satisfied in order to provide assurances of safeguarding the N3 network and information assets
- IG Toolkit - compliance against the law and central guidance that information is handled correctly and protected from unauthorised access, loss, damage and destruction.
- Two can be run in parallel but IGSoC requires the IG Assurance statement from the IG Toolkit for approval
- Research Governance
  - IRAS
  - CSP

Context

- DH RD request for CRN to comply with IG Toolkit
- Dummy run through provided a baseline of CRN
- Gap analysis undertaken to identify necessary steps to achieve Level 2 of the IG Toolkit
- CRNCC in agreement with the University of Leeds to take part in a trial to achieve IGSoC as it was already on a path to comply with the IG Toolkit.

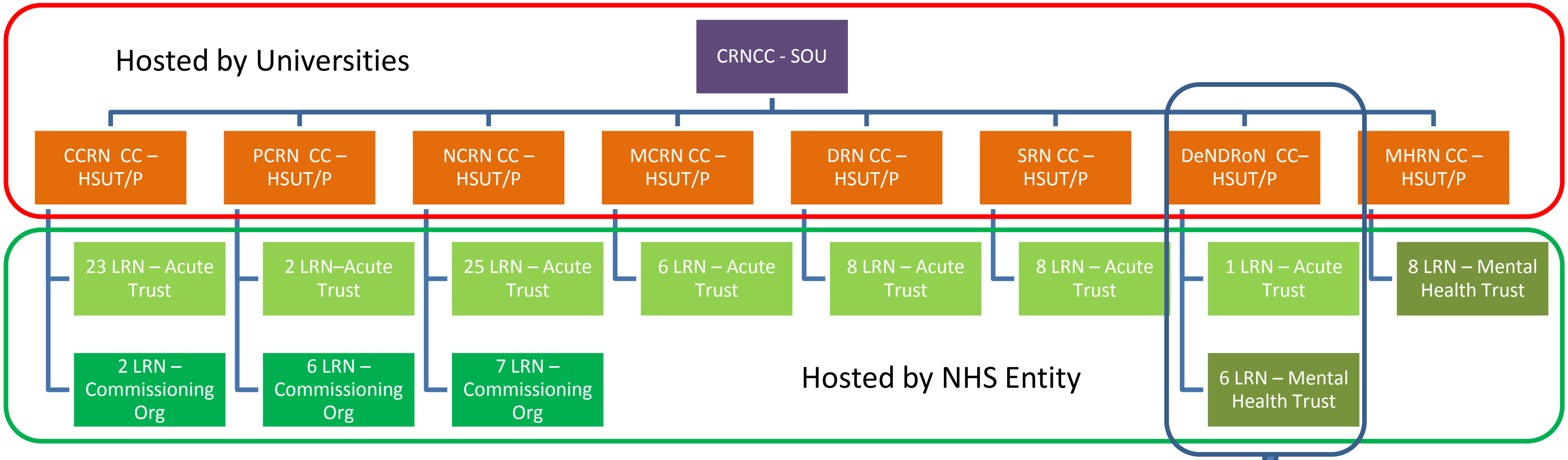
Challenges on the road to IG Toolkit

NHS
National Institute for Health Research
Clinical Research Network

- Most Universities will fall into the category ‘Hosted Secondary Use Team/Project’ (HSUT/P)
- Virtual Organisations such as CRN don’t fit into the Connecting for Health prescribed criteria of HSUT/P or Secondary Use Organisation
- CRN is hosted by Universities and Trusts and has in excess of 300 hosting arrangements
- Secondary Use Organisation - Mandates the use of in excess of 10 new policies - University Legal Service and ISS acceptance is required through a lengthy time consuming process
- Information Governance requires its own governance structure with new stated roles and responsibilities
- NHS IG Training Tool – Recommended for use by the IG Toolkit – different culture is not catered for although the training lessons can be adapted, the tests are NHS specific
- Risk - Manage large volumes of data shared with external stakeholders including Industry Partners

IG Toolkit Organisation Types for CRN as a Virtual Organisation with current status

NHS
National Institute for Health Research
Clinical Research Network

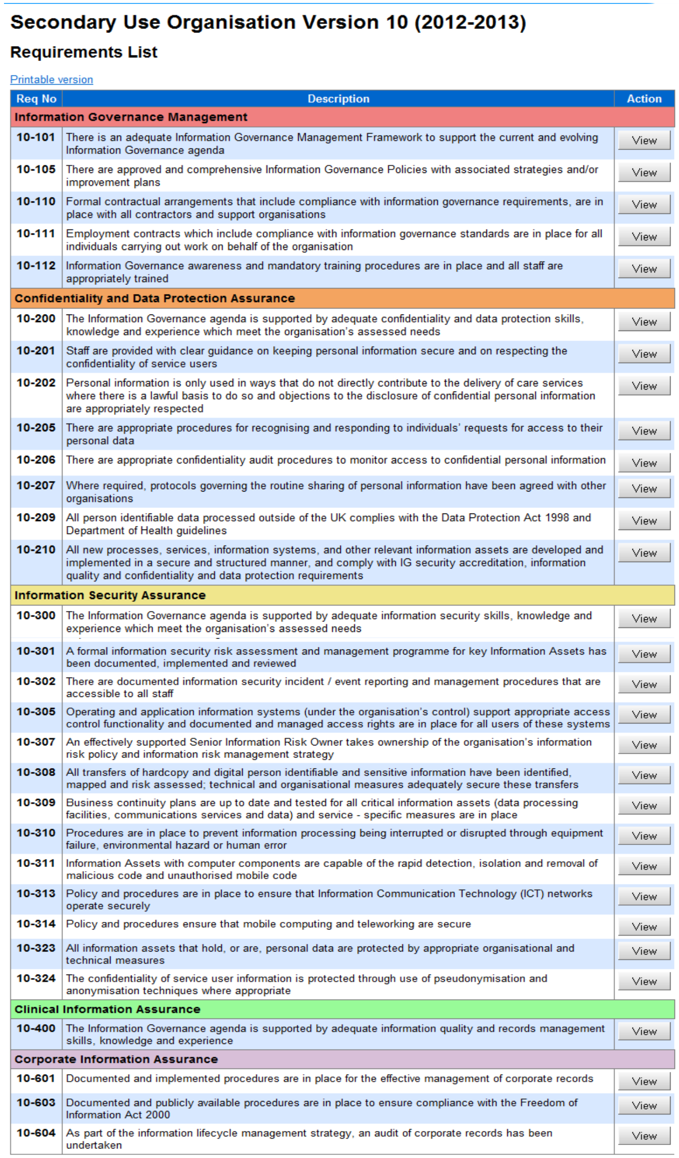


CRN Governance	Hosted by	IG Toolkit Org Type
Clinical Research Network CC	University of Leeds	Secondary Use Org (SOU)
DeNDRoN Coordinating Centre	Kings College London	Hosted Secondary Use Team/Project (HSUT/P)
DeNDRoN Thames Valley	Oxford University Hospitals Trust	Acute Trust
DeNDRoN East Anglia	Norfolk and Suffolk NHS Foundation Trust	Mental Health Trust

IG Toolkit Modules

NHS
National Institute for Health Research

Clinical Research Network

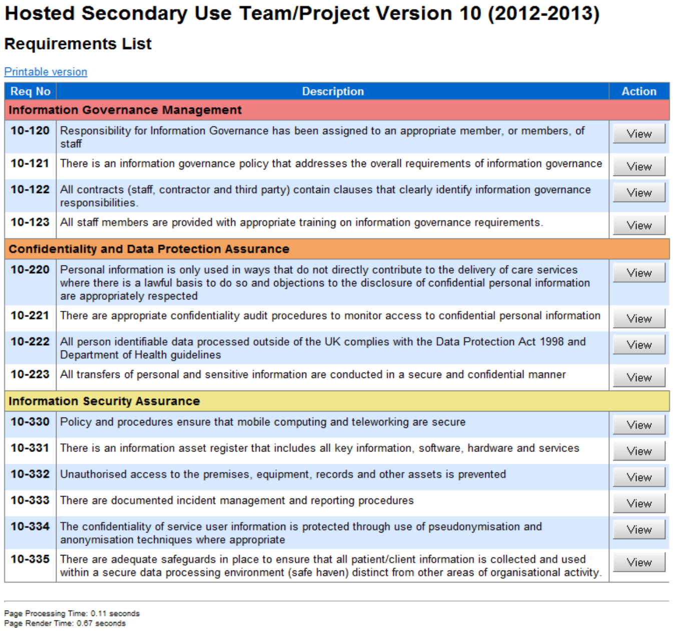


Secondary Use Organisation Version 10 (2012-2013)

Requirements List

Printable version

Req No	Description	Action
Information Governance Management		
10-101	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda	View
10-105	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans	View
10-110	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations	View
10-111	Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation	View
10-112	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained	View
Confidentiality and Data Protection Assurance		
10-200	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs	View
10-201	Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users	View
10-202	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	View
10-205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data	View
10-206	There are appropriate confidentiality audit procedures to monitor access to confidential personal information	View
10-207	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations	View
10-209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	View
10-210	All new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements	View
Information Security Assurance		
10-300	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs	View
10-301	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed	View
10-302	There are documented information security incident / event reporting and management procedures that are accessible to all staff	View
10-305	Operating and application information systems (under the organisation's control) support appropriate access control functionality and documented and managed access rights are in place for all users of these systems	View
10-307	An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy	View
10-308	All transfers of hardcopy and digital person identifiable and sensitive information have been identified, mapped and risk assessed; technical and organisational measures adequately secure these transfers	View
10-309	Business continuity plans are up to date and tested for all critical information assets (data processing facilities, communications services and data) and service - specific measures are in place	View
10-310	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error	View
10-311	Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code	View
10-313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	View
10-314	Policy and procedures ensure that mobile computing and teleworking are secure	View
10-323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	View
10-324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	View
Clinical Information Assurance		
10-400	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience	View
Corporate Information Assurance		
10-601	Documented and implemented procedures are in place for the effective management of corporate records	View
10-603	Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000	View
10-604	As part of the information lifecycle management strategy, an audit of corporate records has been undertaken	View



Hosted Secondary Use Team/Project Version 10 (2012-2013)

Requirements List

Printable version

Req No	Description	Action
Information Governance Management		
10-120	Responsibility for Information Governance has been assigned to an appropriate member, or members, of staff	View
10-121	There is an information governance policy that addresses the overall requirements of information governance	View
10-122	All contracts (staff, contractor and third party) contain clauses that clearly identify information governance responsibilities.	View
10-123	All staff members are provided with appropriate training on information governance requirements.	View
Confidentiality and Data Protection Assurance		
10-220	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	View
10-221	There are appropriate confidentiality audit procedures to monitor access to confidential personal information	View
10-222	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	View
10-223	All transfers of personal and sensitive information are conducted in a secure and confidential manner	View
Information Security Assurance		
10-330	Policy and procedures ensure that mobile computing and teleworking are secure	View
10-331	There is an information asset register that includes all key information, software, hardware and services	View
10-332	Unauthorised access to the premises, equipment, records and other assets is prevented	View
10-333	There are documented incident management and reporting procedures	View
10-334	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	View
10-335	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.	View

Page Processing Time: 0.11 seconds
Page Render Time: 0.67 seconds

Secondary Use Organisation:
30 complex modules

Hosted Secondary Use Team/Project:
14 modules

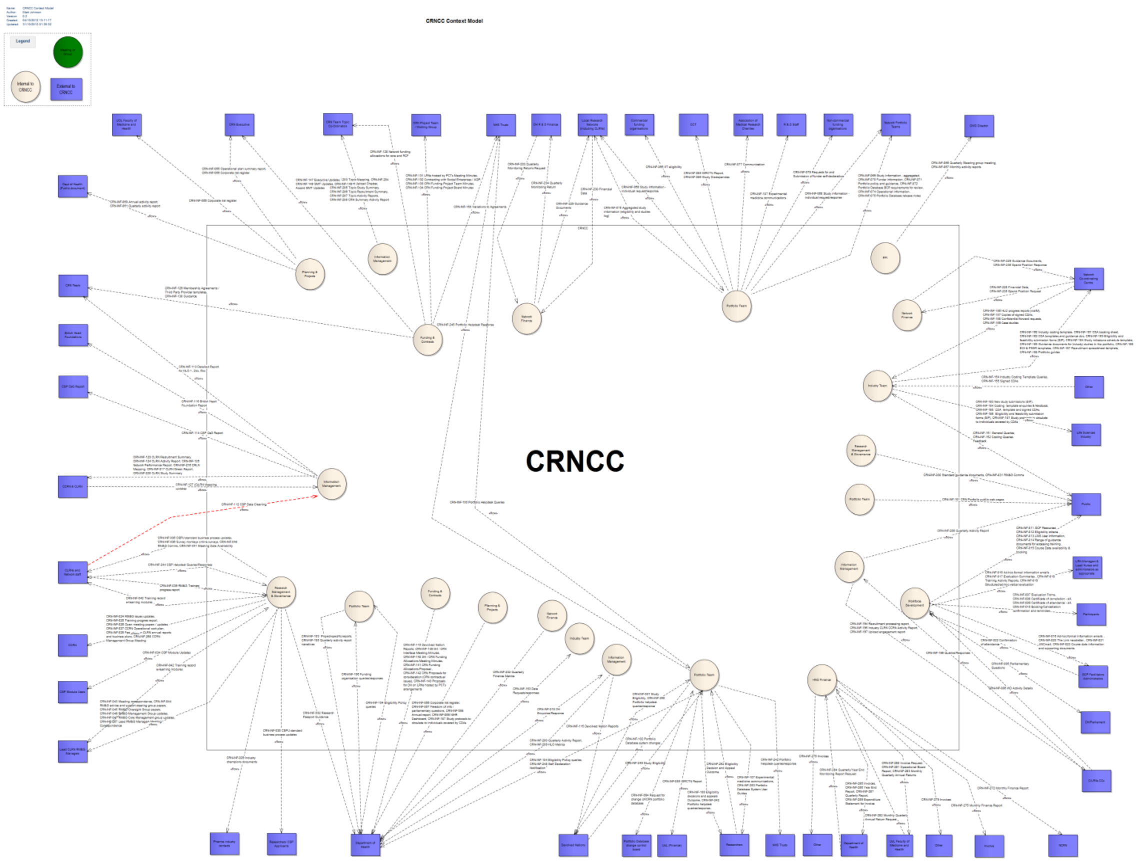
Success on the road to IG Toolkit

NHS
National Institute for Health Research

Clinical Research Network

- Expertise of the Information Security Forum to ensure compliance with ISO standards has assisted in identifying risks
- Raised the awareness of IG within the broader requirements of the University of Leeds including Section 251 of the NHS Act 2006 and Health Service (Control of Patient Information) Regulations 2002
- Developed our organisational information flows that has allowed us to develop:
  - Two corporate risks
  - Risk management of information and infrastructure
  - What our Records are and who our IAO are
  - Training needs analysis
  - CRN Executive buy-in
- IG Working Group and IG Steering Group
- Support and direction from CfH and HSC IC

CRNCC Information Flows


Name: CRNCC Context Model
Author: Mark Johnson
Version: 0.2
Created: 04/10/2012 13:11:17
Updated: 31/10/2012 01:30:32
CRNCC Context Model
Legend
Meeting or Group
Internal to CRNCC
External to CRNCC
UOL Faculty of Medicine and Health
CRN Executive
CRN Team Topic Co-Ordinators
CRN Project Team / Working Group
NHS Trusts
CRN-INF-128 Network funding allocations for core and RCF
CRN-INF-055 Operational plan summary report, CRN-INF-056 Corporate risk register
CRNCC

Internal to External flows has resolved the following:

- Information Asset Owners
- Identification of PII/PID
- Records
- Risk management
- Information storage
- Communication routes ie email, portal.

Future

- Achieve Level 2 IG Toolkit by April 13
- Gain IGSOC by April 13
- Access to N3 to introduce collaborative working across CRN whether hosted by University or Trusts
- Access to NHSMail and directory as an additional goal to N3
- CRN Open Data Platform (ODP) – shared data security
- Collaboration with NHS based ODPs
- CRN Service Improvement Plan - N3 benefit realisation