Rescon Ltd
Data Protection Impact Assessment (DPIA)

Revision History

Version	Revision Date	Summary of Changes	Author
1.0	23/08/2018	Document creation	Tom Dawson
1.1	14/03/2019	DPIA	Tom Dawson

Table of Contents

1. Introduction 1
2. Scope 2
3. Responsibilities 2
4. DPIA 2
5. Review & Monitoring 3
6. Approval 3
Appendix A: DPIA 3
Basic DPIA 3
Full DPIA 4

1. Introduction

Data Protection Impact Assessments (DPIA) help to identify and minimise the data protection risks of a project. DPIAs must be completed for all processing that is likely to result in a high risk to individuals including:

- Use systematic and extensive profiling with significant effects;
- Process special category or criminal offence data on a large scale; or
- Systematically monitor publicly accessible places on a large scale.
- Use new technologies;
- Use profiling or special category data to decide on access to services;
- Profile individuals on a large scale;
- Process biometric data;
- Process genetic data;
- Match data or combine datasets from different sources;
- Collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- Track individuals' location or behaviour;
- Profile children or target marketing or online services at them; or
- Process data that might endanger the individual's physical health or safety in the event of a security breach.

Failure to embed appropriate data protection measures may breach data security and protection laws.

This document will help to identify and address data protection concerns at the design and development stage and details the process for conducting a DPIA to ensure risks are identified and mitigated appropriately.

2. Scope

This document sets out the DPIA process which is required for all processing that is likely to result in a high risk to individuals, with the aim to identify new risks that may not have an associated mitigation.

3. Responsibilities

The person responsible for delivering the proposed project or change to the system is response for completing the DPIA.

The Data Protection Officer (DPO) must be involved and consulted when a DPIA is carried out.

The Information Governance Committee are responsible for overseeing the completion, assessment and outcomes of the DPIA.

4. DPIA

A basic DPIA must be completed to identify whether there may be a high risk to individuals. If the basic DPIA identifies a potential area of risk, a full DPIA must be completed.

The basic DPIA involves initial screening questions and must be completed by the person responsible for delivering the proposed project or change to the system (see Appendix). The basic DPIA will be reviewed and will result in one of the following:

1. The screening process has not identified any DPIA concerns – the process is complete
2. If the answer to any question if 'yes', a full DPIA must be completed

The full DPIA helps to identify and address data protection concerns and ensure risks are identified, assessed, mitigated and of acceptable risk. There are seven stages to the full DPIA (see Appendix). All stages must be completed.

The DPO must be consulted as a matter of routine when a data protection impact assessment is carried out.

www.rescontechnologies.com
info@rescontechnologies.com
penn croft farm – the carthouse, farnham, surrey GU10 5PX

The Information Commissioners Office (ICO) must be consulted where a DPIA indicates high risk to individual rights and freedoms that cannot be mitigated. The ICO will provide advice within eight weeks, or 14 weeks for complex cases.

DPIAs must be published as part of transparency material, with any sensitive information redacted prior to publication.

Completed DPIAs must be sent to adie@rescon.eu for filing.

5. Review & Monitoring

This policy must be reviewed and approved at least annually. Compliance with the DPIA will be monitored through audits and review by the Information Governance Committee.

6. Approval

This DPIA has been reviewed and approved by the Information Governance Lead.

Name: Tom Dawson

Position: Managing and Clinical Director

Date: 14 March 2019

Signature: 

Appendix A: DPIA

Basic DPIA

Answering yes to any of these questions represents a potential risk that requires full DPIA completion to ensure risks are identified, assessed, mitigated and of acceptable risk.

Stage 1 – Basic Assessment

Does this data processing activity:

	Yes	No
Use systematic and extensive profiling with significant effects		X
Process special category or criminal offence data on a large scale		X

www.rescontechnologies.com
info@rescontechnologies.com
penn croft farm – the carthouse, farnham, surrey GU10 5PX

Systematically monitor publicly accessible places on a large scale		X
Use new technologies	X	
Use profiling or special category data to decide on access to services		X
Profile individuals on a large scale		X
Process biometric data		X
Process genetic data		X
Match data or combine datasets from different sources	X	
Collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')		X
Track individuals' location or behaviour	X	
Profile children or target marketing or online services at them		X
Process data that might endanger the individual's physical health or safety in the event of a security breach	X	

If you have answered yes to any of these questions a full DPIA must be completed.

Full DPIA

Stage 1 – Identify need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. Summarise the need for a full DPIA.
Lincus, is digital health and care tool for the monitoring and management of health and wellbeing. It helps deliver best practice care provision, providing an evidence driven platform that can be used by individuals, and/or their support network. Connectivity is a feature of Lincus with person to person to group connections through multiway video and chat. Lincus uses Open Standards and connects with any system supporting these standards for efficient and secure sharing of data. Lincus also connects to multiple IoT enabled devices and platforms including FitBit, Apple Health and Google Fit. Lincus has multiple UK and EU certifications, accreditations and endorsements. Importantly Lincus: 1.) Integrates new technologies on an ongoing basis including those relating to artificial intelligence, other new ways of data processing, and data visualisation all of which may impact on the health and wellbeing on data subjects; 2.) Lincus matches and combines data from different sources with a view to extending those sources. The permissions and legal bases for the data

combination are gained from either a data subject or an organisation that provides a service to them and is legally bound under the terms of our service level agreement to ensure that the legal basis for data processing has been addressed;

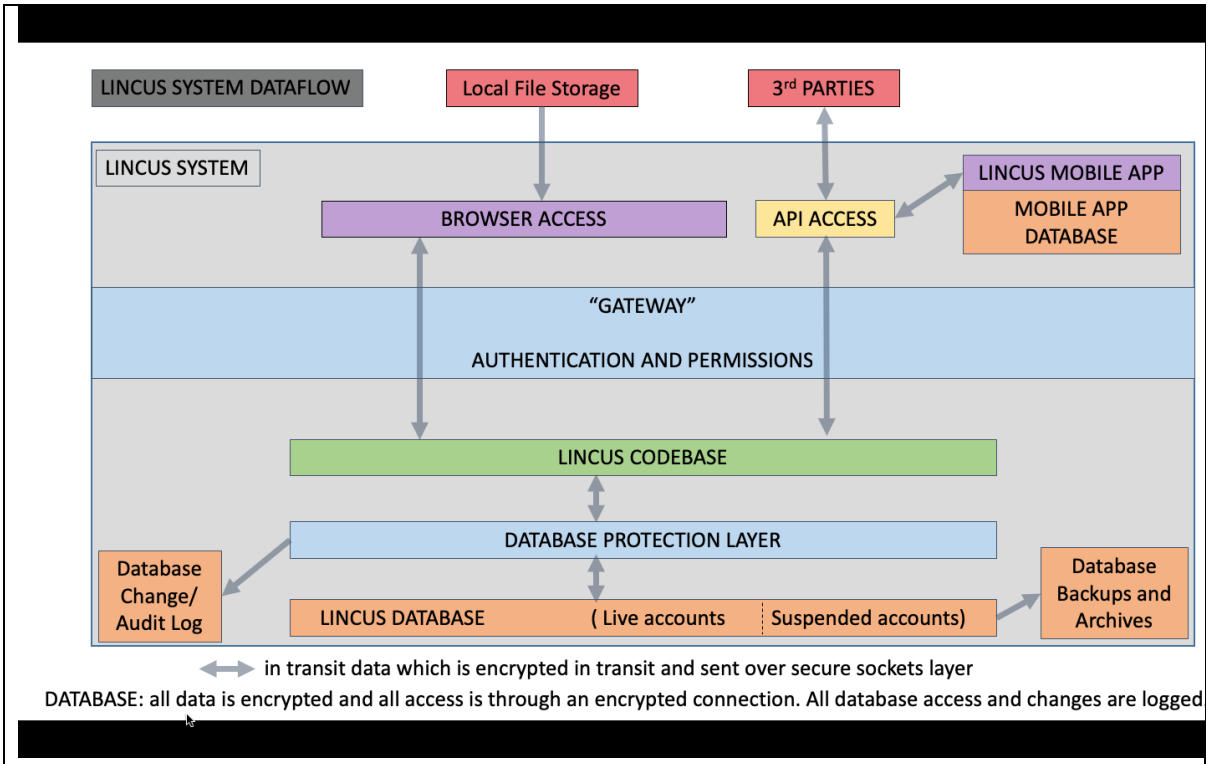
3.) We record the location and behavior patterns of individuals using Lincus. This information is accessible by individuals and organisations delivering their health and social care. This again is controlled through our service level agreements or terms and conditions of use which are explicitly laid out for data subjects.

4.) We process health and social care data. Security breaches that may corrupt, intercept or delete data may endanger the physical and mental health of a data subject.

Stage 2 – Describe the processing

Describe the nature of the processing. How will it be collected, used, stored and deleted? What is the source of the data? Will the data be shared with anyone? Use a data flow diagram where possible. What types of processing are identified as high risk?
Data is collected from several sources including self-input from data subjects, observations from individuals providing direct health or social care utilising Lincus or other care recording management systems, measurement data from a variety of sources including wearable devices such as activity trackers, home healthcare devices such as weighing scales, medical devices such as glucometers, laboratory tests such as blood and urine analysis and imaging technologies such as X-ray or MRI scans. Once the data enters the Lincus system it is encrypted both at rest and during transit. The data is shared with organisations and individuals who provide direct health and social care services for the data subject. As we are dealing with health and social care data we assumed all personal linked data that is processed is high risk.

www.rescontechnologies.com
info@rescontechnologies.com
penn croft farm – the carthouse, farnham, surrey GU10 5PX



Describe the scope of the processing. What is the nature of the data, and does it include special category or criminal offence data? How much data will be collected and used? How often? How long will it be kept? How many individuals are affected? What geographical area does it cover?
Lincus is used by individuals and organisations as a means of storing any data that is relevant to the health and social care needs of data subjects. Therefore any special category data including criminal offence data would potentially be stored and processed by the platform. Lincus commonly processes data relating to race and ethnic origin, biometric data and health data though it is not limited to those data types. There is no limit of the amount of data collection or use within the scope that it applies to the delivery of the health and care needs of a data subject or subjects. The data may be collected continuously or intermittently. Data is kept according to service level agreements or in the case of an agreement with a data subject for seven years post the confirmed death of a data subject or 150 years post date of birth, whichever is the soonest. At the time of this DPIA there are 4000 individuals registered with Lincus covering all geographical regions. Most of the individuals registered with Lincus as resident in the United Kingdom.

www.rescontechnologies.com
info@rescontechnologies.com
penn croft farm – the carthouse, farnham, surrey GU10 5PX

Describe the context of the processing. What is the nature of the relationship with the individuals? How much control will they have? Would they expect the data to be used in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that should be factored in? Are there any approved code of conduct or certification schemes that have been applied to?
There are two types of relationship with data subjects. The first is a service relationship where individuals subscribe to using the platform and agree to the explicit and transparent terms and conditions including how the data will be used. The second is a through a service agreement with an organisation that provides a service for the data subject. In this situation the onus is on that organisation to inform the data subject how the data is going to be used. The data processing and context of processing is not novel. There are no issues of public concern. The data within Lincus is processed according to the UK national health service Information Governance and Security Toolkit, the UK Information Commissioners Office and the Medicines and Health Regulations Authority as a Class 1 Medical Device.

Describe the purposes of the processing. What do we want to achieve? What is the intended effect on individuals? What are the benefits of the processing?
The processing is for the purposes of improving the physical, mental, social and emotional health of data subjects and also those that support them. This also covers the intended effect and benefits.

Stage 3 – Consider consultation

Consider how to consult with relevant stakeholders. Describe when and how to seek individuals views – or justify why it is not appropriate to do so. Who else needs to be involved? Do processors need to assist? Do information security experts or any other experts need to be consulted?
The Lincus platform development process integrates data subject and other stakeholder views. We regularly consult with other data processors and security experts and are an active part of the community looking to improve the information and clinical governance processes for data subjects and populations. Our platform development release protocol is in Appendix 1 of this document.

Stage 4 – Access necessity and proportionality

www.rescontechnologies.com
info@rescontechnologies.com
penn croft farm – the carthouse, farnham, surrey GU10 5PX

Describe compliance and proportionality measures. What is the lawful basis for processing? Does the processing achieve the purpose? Is there another way to achieve the same outcome? How will function creep be prevented? How will data quality and data minimization be ensured? What information will be given to individuals? How will we help to support their rights? What measures will be taken to ensure processors comply? How will international transfers be safeguarded?
The lawful basis of processing is to deliver a service being a managed health and care record. The primary reason that processing is necessary is for the purposes of medical diagnosis or the provision of health or social care treatment (Article 17 – 3c) and secondary reasons of retention for: compliance with legal obligation (Article 17 – 3b); the establishment, exercise or defence of legal claims (Article 17 – 3e). Data that is no longer required for processing is securely archived. Pseudonymised and anonymized data is held indefinitely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 17 – 3d). There is no other way to achieve the outcome as Lincus is a managed health and care record by definition. Function creep is limited through ongoing and continuous monitoring, consultation with stakeholders and quarterly information governance meetings. We constantly refine our processes to assure data quality and minimization. All information apart from that which may be considered potentially harmful from a safeguarding perspective on behalf of an organisation deliver direct health or social care is available to data subjects. Rights are supported by ongoing attention to processes and collaborative consultation with the clinical, healthcare and information security community. All processors are bound under service level agreements. This does not guarantee compliance so we continue to review the utility and robustness of emerging compliance technologies such as distributed ledgers technologies (Block Chain). The only case we have for international transfers would be through a data subject who would need to access the browser portal and physically download their data to a local device in another international region. This type of transfer is protected by our usual security processes including 256 bit encryption during transit.

Stage 5 – Identify and assess risks

Please refer to our full information governance risk assessment and mitigation documentation available here and clinical safety case available here

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant, severe	**Overall risk** Low, medium, high

www.rescontechnologies.com
info@rescontechnologies.com
penn croft farm – the carthouse, farnham, surrey GU10 5PX

See above			

Stage 6 – Identify measures to mitigate risk

Please refer to our full information governance risk assessment and mitigation documentation available here and clinical safety case available here

Identify additional measures that could be taken to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated, reduced, accepted	**Residual risk** Low, medium, high	**Measure approved?** Yes/No
See above				

Stage 7 – Sign off and record outcomes

Item	**Name/Date**	**Notes**
Measures approved by:	Tom Dawson	*Integrate actions into project plan with date and responsibility for completion*
Residual risks approved by:	Tom Dawson No residual high risk	*If accepting any residual high risk, consult the ICO before going ahead*
DPI advice provided:	Yes	*DPO must advise on compliance, step 6 measures and whether processing can proceed*
Summary of DPO advice: No residual high risk – processing can proceed.		
DPO advice accepted or overruled by:	Laura Gilbert	*If overruled, explain reasons why*
Comments:		

www.rescontechnologies.com
info@rescontechnologies.com
penn croft farm – the carthouse, farnham, surrey GU10 5PX

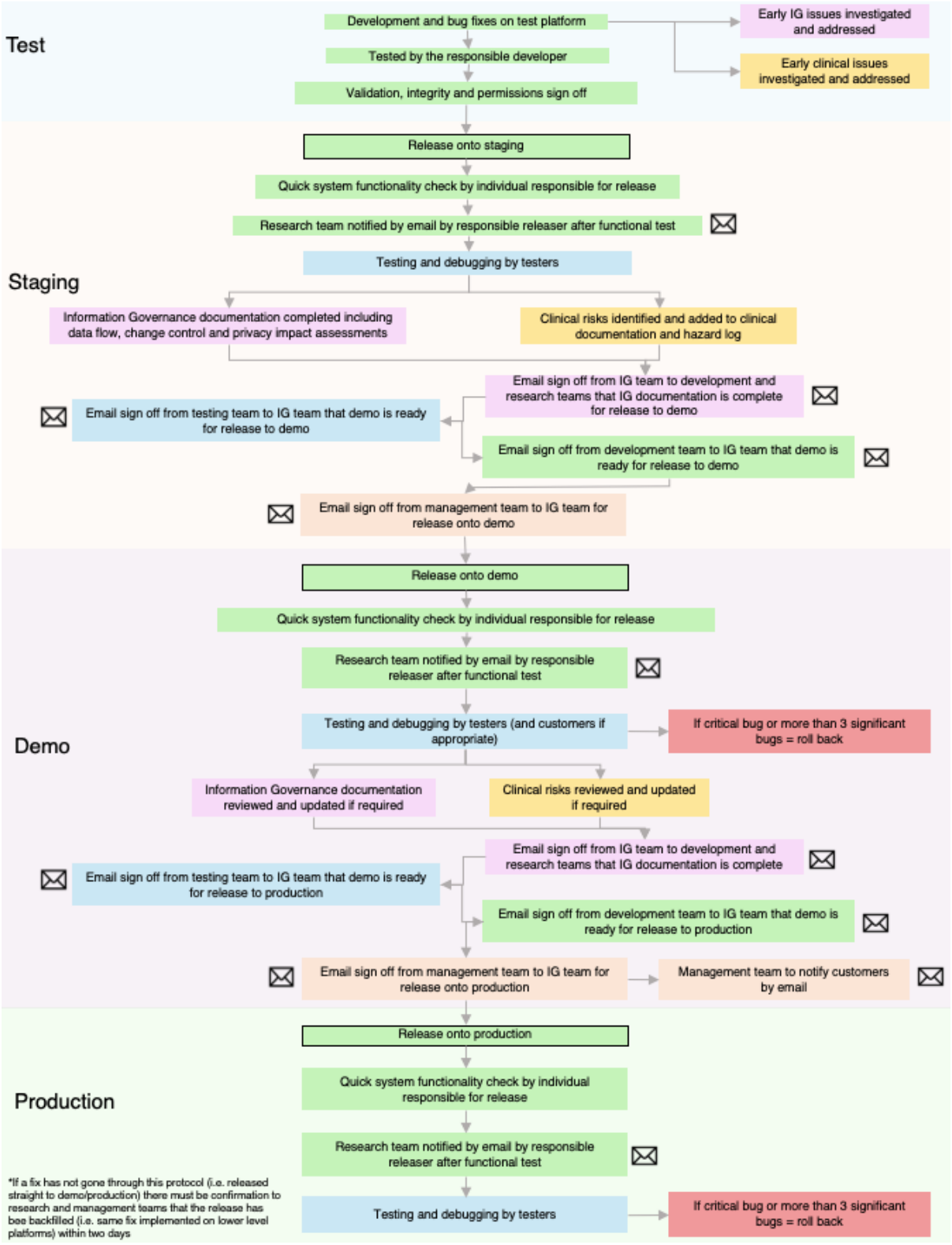
Consultation responses reviewed by:	Tom Dawson	*If your decision departs from individuals' views, you must explain your reasons*
Comments:		
This DPIA will be kept under review by:	Tom Dawson and Adie Blanchard	*The DPO must also review ongoing compliance with DPIA*

Please send the completed DPIA to adie@rescon.eu

Appendix 1: Release Protocol

www.rescontechnologies.com
info@rescontechnologies.com
penn croft farm – the carthouse, farnham, surrey GU10 5PX

Lincus Release Protocol



www.rescontechnologies.com
info@rescontechnologies.com
penn croft farm – the carthouse, farnham, surrey GU10 5PX

Platform	Release Stages	Responsible Individual	Additional Comments
Test	Development and bug fixes on test platform	LMG*	Early IG issues and clinical risks investigated and addressed at this stage.
Test	Tested by the responsible developer	LMG*	
Test	Validation, integrity and permissions sign off	CAM*	
Test	Developers email management (cc'ing testers, CSG and IG Committee) requesting approval for release to staging	CAM*	
Test	Management approve request for release	TD*	
Staging	Release onto staging platform after request has been approved. Bug fix **and** new updates can take place for two weeks from this date or until release to demo (whichever is sooner)	LMG*	
Staging	Quick system functionality check by individual responsible for release	LMG*	
Staging	Developers email management (cc'ing testers, CSG and IG Committee) confirming release and initial checks have taken place	LMG*	
Staging	Testing and debugging by testers	AB*	Testing must only take place once email confirmation of release from developers has been received. A full test must take place prior to release to demo (bug fix testing is not sufficient for a full release).
Staging	Testers to email developers (cc'ing management, CSG and	AB*	

www.rescontechnologies.com
info@rescontechnologies.com
penn croft farm – the carthouse, farnham, surrey GU10 5PX

	IG Committee) once testing and debugging has been completed (all critical bugs fixed and staging ready for release to demo)		
Staging	Information Governance documentation completed and filed with confirmation email sent to management, developers and testers	AB*	Software update assessment, data flows, change control, privacy impact assessment.
Staging	Clinical risks documentation completed and filed with confirmation email sent to management, developers and testers	TD*	Clinical impact assessment.
Staging	Developers email management (cc'ing testers, CSG and IG Committee) requesting approval for release to demo	LMG*	
Staging	Management approve request for release	TD*	
Demo	Release onto demo platform after request has been approved. Bug fix updates **only** can take place for two weeks from this date or until release to demo (whichever is sooner). New updates require further authorisation.	LMG*	Release to occur out of hours where possible. If a critical bug is found at any point or three significant new bugs found, the release is rolled back immediately.
Demo	Quick system functionality check by individual responsible for release	LMG*	
Demo	Developers email management (cc'ing testers, CSG and IG Committee) confirming release and initial checks have taken place	LMG*	
Demo	Testing and debugging by testers	AB*	Testing must only take place once email confirmation of release from developers has

www.rescontechnologies.com
info@rescontechnologies.com
penn croft farm – the carthouse, farnham, surrey GU10 5PX

			been received. A full test must take place prior to release to demo (bug fix testing is not sufficient for a full release).
Demo	Testers to email developers (cc'ing management, CSG and IG Committee) once testing and debugging has been completed (all critical bugs fixed and staging ready for release to production)	AB*	
Demo	Information Governance documentation reviewed and updated if required with confirmation email sent to management, developers and testers	AB*	Software update assessment, data flows, change control, privacy impact assessment.
Demo	Clinical risks documentation reviewed and updated with confirmation email sent to management, developers and testers	TD*	Clinical impact assessment.
Demo	Developers email management (cc'ing testers, CSG and IG Committee) requesting approval for release to production	LMG*	
Demo	Management approve request for release and notify customers	TD*	
Demo	Notify ISTB if there are any server changes that need to be implemented	LMG*	
Production	Out of hours' release onto production platform after request has been approved. Bug fix updates **only** can take place for two weeks from this date or until release to demo (whichever is sooner). New	LMG*	Release must occur out of hours. If a critical bug is found at any point or three significant new bugs found, the release is rolled back immediately.

www.rescontechnologies.com
info@rescontechnologies.com
penn croft farm – the carthouse, farnham, surrey GU10 5PX

	updates require further authorisation.		
Production	Quick system functionality check by individual responsible for release	LMG*	
Production	Developers email management (cc'ing testers, CSG and IG Committee) confirming release and initial checks have taken place	LMG*	
Production	Release email filed	AB*	
Production	Testing and debugging by testers	AB*	Testing must only take place once email confirmation of release from developers has been received. A full test must take place prior to release to demo (bug fix testing is not sufficient for a full release).
	Release manager to email management, developers, testers, IG committee and CSG with completed release protocol and confirmation of successful release. Release protocol is then reset.	AB*	

*or deputy

www.rescontechnologies.com
info@rescontechnologies.com
penn croft farm – the carthouse, farnham, surrey GU10 5PX