Lincolnshire Community Health Services NHS Trust

Clinical Technology Standards Policy

(Clinical Photography and Video Recording, SMS Text Messaging for Service Users, Data Quality and NHS Number)

Reference No:	P_IG_29
Version:	1
Ratified by:	LCHS Trust Board
Date ratified:	14 August 2018
Name of originator/author:	Kaz Scott, Information Governance Lead
Name of responsible committee/individual:	Information Governance Management Assurance Group
Date issued:	August 2018
Review date:	August 2020
Target audience:	All staff and third party contractors employed by LCHS
Distributed via:	Website

Lincolnshire Community Health Services NHS Trust

Clinical Technology Standards Policy

Version Control Sheet

Version	Section/Para /Appendix	Version/Description of Amendments	Date	Author/ Amended by
1		Amalgamation of policies P_IG_16, 22, 24 content previously ratified and further content update to reflect GDPR.	June 2018	Kaz Scott
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Lincolnshire Community Health Services NHS Trust

Clinical Technology Standards Policy

Contents

Lincolnshire Community Health Services NHS Trust

Clinical Technology Standards Policy

Policy Statement

Background

Clinical Technology Standards plays an essential role within the Trust and this policy has been developed to ensure that all conform to current legislation and other Trust policies:

Consent to Treatment Policy
Records Management Policy
Data Protection Policy
Mental Capacity Act (2005)
Safeguarding Children Policy
Information Security Policy
Information Risk Policy
Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 11
Equality Act 2010
Care Act 2014

Statement

Staff working for the Trust will ensure that they comply with the requirements of the Data Protection legislation and safeguard personal confidential data (PCD) which is held.

Responsibilities

It is the responsibility of each member of staff who will be using clinical technology standards as part of a patient's care to be aware of this policy and work within its parameters.

Training

Training for the taking of digital images will be provided in line with the contents of this policy.

Dissemination

The policy will be published on the Trust website.

Resource Implication

Failure to obtain or record consent could lead to legal challenge.
Resource implications in the implementation of this policy are primarily in relation to training implications.

CLINICAL PHOTOGRAPHY AND VIDEO REDCORDING

Clinical photography and Video Recordings are a valuable part of assessing and evidencing a patient's condition. They are beneficial in areas such as tissue viability to demonstrate that the condition of a wound has improved, or in areas such as physiotherapy and speech and language therapy to demonstrate improvements of a particular condition over time. It also provides a quality transparent process to support complaints and investigations.

The term "recording" (or "recordings") is used to refer to photography (either conventional or digital) and video recordings (either conventional or digital) and voice recordings in Speech and Language Therapy. It refers to original and/or copies of images. It does not include pathology slides containing human tissue or CCTV recordings of public areas on the Trusts premises.

Recordings taken using cameras owned by the Trust which illustrates a patient's condition or an aspect of the treatment, form a part of that patient's health record and are protected in the same way as any other health record.

All research projects involving the recording of patients should contact the Research Team for further advice.

Copyright of all such recordings is held by the Trust.

Negatives, master transparencies, original digital camera files and videotapes must be logged and stored appropriately.

It is recognised that while digitally originated recordings are intrinsically no different to traditional recordings; they are easier to copy in electronic form and are therefore more at risk of both image manipulation and inappropriate distribution. Particular care must be taken to protect the image and maintain its integrity.

Confidentiality and Consent
This must be read in conjunction with the Consent Policy for further guidance on the general meaning and definition of consent.

Photographic and video recordings made for clinical purposes form part of a patient's record. Although consent to certain recordings, such as X-rays, is implicit in the patient's consent to the procedure, health professionals should always ensure that they make clear in advance if any photographic or video recording will result from that procedure.

Photographic and video recordings which are made for treating or assessing a patient must not be used for any purpose other than the patient's care or the audit of that care, without consent of the patient or a person with parental responsibility for the patient.

The one exception to this principle is set out in the paragraph below. If you wish to use such a recording for education, publication or research purposes, you must seek consent in writing, ensuring that the person giving consent is fully aware of the possible uses of the material. In particular, the person must be made aware that you may not be able to control future use of the material once it has been placed in the public domain. If a child is not willing for a recording to be used, you must not use it, even if a person with parental responsibility consents.

Where patients who appear to lack capacity to give informed consent need clinical photography, the Trusts Mental Capacity Act (2005) and Procedures must be followed. One of the key principles is that any act done for, or any decision made on behalf of the person who lacks capacity must be done, or made in that persons best interest.

Photographic and video recordings, made for treating or assessing a patient and from which there is no possibility that the patient might be recognised, may be used within the clinical setting for teaching purposes without consent from the patient, as long as this is well publicised. However, consent must be sought for any form of publication.

If you wish to make a photographic or video recording of a patient specifically for education, publication or research purposes, you must first seek their written consent (or where appropriate that of a person with parental responsibility) to make the recording, and then seek their consent to use it. Patients must know that they are free to stop the recording at any time and that they are entitled to view it if they wish, before deciding whether to give consent to its use.

If the patient decides that they are not happy for any recording to be used, it must be destroyed. As with recordings made with therapeutic intent, patients must receive full information on the possible future uses of the recording, including the fact that it may not be possible to withdraw it once it is in the public domain.

The situation may sometimes arise where you wish to make a recording specifically for education, publication or research purposes, but the patient is temporarily unable to give or withhold consent because, for example, they are unconscious. In such cases, you may make such a recording, but you must seek consent as soon as the patient regains capacity. You must not use the recording until you have received consent for its use, and if the patient does not consent to any form of use, the recording must be destroyed.

In the case of minors, the person with parental responsibility must sign the consent form for education, publication or research purpose unless the minor reaches the age of 16 or is judged to be capable of consenting in his own right during the course of treatment, when new consent is required. Please refer to the Mental Capacity Act (2005). If a child is not willing for a recording to be used it must not be used, even if the person with parental responsibility consents.

In regards to Safeguarding Children a child would need to be assessed as competent to give consent using Gillick Competence.

If the patient is likely to be permanently unable to give or withhold consent for a recording to be made for education, publication or research purposes:

Research covered by the Act cannot include people who lack capacity to consent to the research unless:

- It has approval of “the appropriate body” (in England, the appropriate body must be a research ethics committee recognised by the Secretary of State.
- It follows other requirements of the Act to:
- Consider the views of carers and other relevant people.
- Treat the person’s interests as more important than those of science and society
- Respect any objections a person who lacks capacity makes during the research.

You must not make any use of the recording, which might be against the interests of the patient. You should also not make, or use, any such recording if the purpose of the recording could equally well be met by recording patients who are able to give or withhold consent (refer to MCA Code of Practice 2005).

Staff should seek appropriate consent to make the recordings listed below, but you do not need explicit consent to use them for any purpose, provided that, before use, the recordings are effectively anonymised by the removal of any identifying marks:

- X-rays (including dental x-rays), Images taken from pathology slides or Ultrasound images

Such recordings will not identify the patient. It may still be appropriate to explain to the patient, as part of the process of obtaining consent to the treatment or assessment procedure, that a recording will be made.

There is a tick box available on templates which should be used to record patient consent. These may be in the Wound Template or TV Assessment.

Confidentiality is the patient's right and may usually only be waived by the patient or someone legally entitled to do so on his/her behalf e.g. Power of Attorney.

Photographs of unconscious patients may only be taken with consent from the next of kin. Once the patient has regained consciousness they must be informed that a photograph has been taken and if they object to the use of the photograph it must be destroyed. This must all be documented in the patient's health record (refer to MCA Code of Practice 2005).

Where a Practitioner suspects there are concerns related to Child Protection, guidance is available in the Safeguarding Children Board Policy via www.lincolnshire.gov.uk/lscb as it is not deemed appropriate for Practitioners to be taking recordings for suspected Child Protection concerns.

A person with parental responsibility should be informed of the reasons for clinical photography and must be given the opportunity to consent. The parents' responses should be documented. The agreement of the child, if of sufficient understanding, should also be sought. In the absence of parental consent, photography should only be authorised by the senior child protection practitioner with responsibility for the case. Recordings taken in these cases may be required as evidence in criminal or public proceedings and no absolute guarantees of confidentiality in this respect can be given.

In all cases of recording, care must be taken to respect the dignity, ethnicity and religious beliefs of the patient.

A patients' image may not be altered in any way to achieve anonymity and so avoid the need for consent.

Blacking out the eyes in a facial photograph is not an acceptable means of anonymising the image and the patient may still be identified by other distinguishing features such as a tattoo or scar.

If a patient dies before a retrospective consent can be obtained, material by which the patient is identifiable can only be released with the consent of the deceased person's representatives.
In addition wherever possible the consent of the next of kin or near relatives should be obtained, particularly where the personal representatives of the deceased are not relatives. Staff are reminded that the duty of confidentiality survives death of the patient.

If a consenting patient subsequently dies, permission should be sought for any new use outside the terms of the existing consent. In this instance the consent of either the personal representative or the next of kin is required.

Non Clinical Photography
In cases where the patient is incidental to a recording, e.g. where the picture is to illustrate a particular piece of equipment set-up, consent to appear in the recording is still required from any patient or member of the public.

Accidental recording of patients who have not given appropriate consent must be avoided. Images of a patient that inadvertently include an image of another patient or patients who have not consented must not be published under any circumstances. Unless deleterious, causing harm or damage to the care of the patient, they should be destroyed.

Freelance professional photographers are sometimes employed to make this sort of recording. They may only be used by the Trust by prior arrangement with the Head of Communications.

Contracts with outside photographers must ensure that they waive ownership of copyright and moral rights in the recordings they prepare, although they may still be allowed to reproduce the recording or image providing permission has been given from the Trust on each occasion.

Copyright

The Trust holds the copyright for all recordings made of its patients.

It is important that in any contract for publication the copyright of the recording remains with the Trust and does not pass automatically to the publishers on first publication, otherwise the Trust might well find it is unable to protect the patient's interests by exercising control over further publication of the recording.

Those signing contracts with book or other publishers have a responsibility to delete from the contract any suggestion that the copyright will pass to the publishers.

Any member of staff acquiring copies of recordings in the course of their duties may retain these for teaching purposes but must undertake to use them only within the terms of the original consent. Copyright and reproduction rights must at all times remain with the Trust.

Copies of recordings must not be excessive and must be discussed with the Information Governance Lead. Decisions will be made on a case by case basis.

Security and Storage

Since any health record has to be available for disclosure under the Access to Health Records Process if required, it is essential that every recording is logged and properly recorded in the record and in accordance with the Data Protection legislation.

All recordings of patients must be stored on Trust premises. Information Security is paramount. Digital images must be stored securely on the Trusts server or in the clinical system and should never be stored on a standalone desktop computer where it is only possible to store data locally. Images can be stored temporarily on an encrypted laptop.

Images may be stored **temporarily** on digital cameras as an exception to normal policy before being uploaded to a secure area of the network or in the clinical system. Ideally all digital images should be uploaded immediately where possible and deleted from the camera to prevent any loss of personal data and security incidents. All images must be transferred from the camera to the laptop at the end of each day, in the patient's home or immediately upon return to base. This process only applies to digital camera images and not to video or any other recording.

Once the data has been transferred, all traces of the data should be immediately removed from the removable storage device.

Personally owned storage devices (USB or data sticks), mobile phones, personal digital cameras or MP3 players must **never** be used to store images or recordings.

Data in transit on removable media **must** be encrypted, handled and stored appropriately and afforded the utmost security and protection **at all times**.

It has been accepted however that until we can satisfactorily provide an encryption solution to digital images in transit that this poses a risk in case of loss or theft. Staff are advised therefore to take extreme care with cameras at all times. This exception only applies to digital cameras and not to any other video or other recordings which must be encrypted immediately.

Any image or recordings should be named with the NHS Number using the recommended format of 3 3 4 e.g. 123 456 7890 (NPSA Safer Practice Notice: Sep 2008 No NPSA/2008/SPN001) of the patient and the date the image or recording was made. It is noted that some electronic systems are only set up to record a full 10 digit number with no spaces.

In the case of a digital picture file, the original file must be written to disc and stored securely and appropriate measures taken to back up the images. For later retrieval purposes, each image should be assigned a file name by which it can clearly be identified, incorporating the patient's NHS number and the date of the recording.

Staff undertaking storage and retrieval of digital images must work at all times within this policy and procedure.

Staff are to ensure the digital camera is stored securely when taken away from premises or locked away appropriately and to remain vigilant at **all times** regarding the security and handling of the equipment.

Standards of Digital Photography/Video Recording of Patients
Where digital photography is to be used to record images of patients, due care must be given before the start to ensure that the quality of the image (in terms of both resolution and colour depth) is adequate for purpose.

Staff should use the 'Softdrape Measurement' details on the dressing pack / or other type when taking clinical photographs to identify the patient.

In order to maintain the integrity of the image, manipulation may only be carried out to the whole image and must be limited to simple sharpening, adjustment of contrast and brightness and correction of colour balance.

Due to the speed in which it may take to upload the image a resolution of 3 mega pixels has been tested and deemed acceptable. The quality of the image is not compromised when photographing or viewing wound assessments.

Before leaving the employment, staff must seek specific permission to retain images for teaching purposes from the Trust who may grant such permission subject to the retention of copyright and all reproduction rights.

All recordings for projects/research must be discussed with the Research Department.

On some occasions parents/guardians may request a copy of a video recording that has been made of their child during treatment. In these cases, parents/guardians must be directed to make their request using the Access to Health Records Process.

Use of SKYPE / E-Consultations
The Trust is now using SKYPE to undertake consultations and any team wishing to pursue the use should contact the IMT Team for further information.

There is a standard process and allocation of use which will only be approved through IMT in conjunction with ICT Services who will arrange the installation of any software.

Smartphones
Smartphones may be used for taking clinical images. These **must** have an 8-digit pin applied or encryption to meet the information security standard. Any smartphone which have a 4-digit pin are **NOT** approved for use.

Changing the 8-digit pin to a pattern is against Trust policy and must remain as a pin code. IMT can offer guidance and support.

Any images should have the 'Softdrape Measurement details' with the NHS Number clearly recorded, Name and DoB is not sufficient and should be uploaded within 24 hours.

Patient Photographs – Residential Homes Only
A photo is often placed on the patient's folder in a residential home so the patient can be identified accurately against other demographic details. The image may be uploaded into the record to support mobile working and is to be removed from the electronic record when the care is ended.

Linked documents

- Records Management Code of Practice for Health and Social Care 2016
- LSCB Guidance via www.lincolnshire.gov.uk/lscb.
- Mental Capacity Act Code of Practice
- http://www.gmc-uk.org/Making_and_using_visual_and_audio_recordings_of_patients.pdf_58838365.pdf
- http://www.hra.nhs.uk/about-the-hra/our-plans-and-projects/assessment-approval/

References
Acknowledgements are given to Salisbury NHS FT and Royal Cornwall Hospitals NHST whose information has been used and adapted to produce this as an example of good practice.

NHS
Lincolnshire Community Health Services
NHS Trust

Consent Form for Video Recordings / Voice Recordings

Visual and audio recordings can be a useful resource for patient experience, consultations, medical teaching, research or supporting complaints and investigations.

This allows us to:

- Have a record of how a condition changes and to assist in treatment
- Help train staff, including supervising staff who are treating you
- Provide a quality transparent process to support complaints and investigations

A member of staff will explain the purpose and how the recording is to be used before you read and sign this consent form. You may ask for a relative, friend or Staff member to be present during the recording.

Consent may be withdrawn at any time and the standard of care will not be affected, however, if published the withdrawal of consent may not be possible. **No fees are paid for publication or broadcast.** Copyright and reproduction rights will remain with the Trust.

Consent to Visual and Audio Recording

I agree to the Trust using the photographs/videos/voice recordings for the following purpose:

To assist in treatment or health condition changes	☐ Yes	☐ No
To support a complaint or investigation (To provide a high quality and transparent service)	☐ Yes	☐ No
For Information and exhibition purposes (May be used in articles seen by the general public or in medical textbooks on public sale)	☐ Yes	☐ No

By signing this form, I have read, understood and accept the Trust, its agents, subsidiaries, and associates, shall not be held liable for any grievance, incident or legal matter arising from my appearance in any Video, Audio and/or Photography productions, subject to its reasonable and ethical use and I confirm that this consent form has been explained to me in terms which I understand

Signed _____ Print name _____
Patient /Parent /Guardian

Date _____

Description of Recording

Consent obtained by:

Staff Name _____ Role _____

Date _____

SMS TEXT MESSAGING FOR SERVICE USERS

The Trust supports the use of Text Messaging (or SMS - Short Message Service) as a means of communication.

A 'user' is an NHS employee or any other person working for or on behalf of the Trust.

Although the basic principles of SMS have been available for a number of years, it is recognised that it is an ever-growing technology. Accordingly, this will be reviewed at least annually and users should ensure they follow the most recent version of the policy, which will available on the Trust Website.

Purpose
This sets out the circumstances in which service users may be contacted by SMS / Text Messaging and the procedures that must be followed when using this method of communication.

Services must individually agree the need/benefit of using SMS and formally approve and document the implementation of the service. Individual users must not use SMS for health-related purposes without formal documented approval.

Local/departmental procedures for the use of SMS, which comply with this, must be documented and cover the following topics –

- Identification of the need or justification for the use of SMS
- Identification of the service or facility to be provided
- The agreement to the use of the service by its intended beneficiaries/recipients
- Clear identification of the associated risks and of the means by which these risks are managed
- Storage and retention procedures (in particular, patient messages or important messages

Use of SMS
SMS can be used for a number of purposes –

- to send individual clients/patients appointment reminders
- to broadcast messages to a wide-ranging audience, for example, as a health promotion exercise
- to support a lone worker
- messages to Staff and Team Members to assist staff movements/shifts

Advantages of using SMS to communicate with service users are:

- Quick and easy communication without delays
- Reduced postage costs
- Reduced possibility of communications going astray through incorrect postal addresses, changing addresses of service users etc
- Ability to send appointment reminders to reduce DNAs

Key Points
SMS or text messaging is an attractive technology for quick communication of short messages and is a widely accepted form of communication. Service users therefore increasingly expect the Trust to communicate with them in this way for simple transactions such as appointment reminders.

The Trust endorses the use of SMS to communicate with service users provided this is for simple communications such as appointment reminders, and provided strict Trust protocol is followed when sending messages.

- Only e-mail accounts must be used when sending out appointments or reminders. This means that teams / services must either set up a generic (team account) or operational e-mail account prior to sending SMS messages to service users
- A generic email account is one that refers to a service or function rather than an individual
- Consent should be gained from service users prior to any SMS messaging taking place
- It must be used only for appointments and other non-sensitive information. Any test results should have an agreed message from the service e.g. Sexual Health Services
- Under NO circumstances should any type of PCD be transmitted via SMS or confidential business information

Consent
Where patients or members of the public are the intended recipients/beneficiaries of a health-related service, they must consent to this. Consent is gained from the service user prior to the commencement of SMS messaging and potential benefits and risks should be explained before deciding on whether or not to participate.

This could be achieved at the time of recording a mobile phone number. Retrospectively, this must be done by making contact with the intended recipient before initiating the service for that person.

Consent should be recorded electronically within the clinical system and templates exist where an option can be selected to confirm patient has consented to receive SMS Text Messages. Service Users may withdraw their consent to SMS messages at any time by informing their Health Professional.

Risks
The risks associated with this technology will vary according to the outcome.

The following risks must always be taken into account -
Confidentiality risks can be mitigated to a large extent by only sending non-confidential messages and by never sending sensitive data such as - “your next ante-natal appointment is...”

The following points must be addressed –

- Ensuring delivery to the correct recipient (i.e. the ‘safe haven’ principle; the sender must be sure that the phone number being used is that of the intended recipient – being aware that phones are regularly changed, exchanged or sold)
- Theft of the recipient’s phone

The SMS Service is used with an external provider of SMS Text Messaging which is managed through a Portal. Information Governance and all contractual and security measures are in place.

Equality Assessment
Text messaging can undoubtedly be of benefit to recipients, for example, those with hearing impairment or those who would benefit from appointment reminders. However, this Trust cannot resolve every issue that may arise from the use of SMS.

Audit and Monitoring
Auditing procedures will be established by IG, in collaboration with the Information Governance Management Assurance Group (IGMAG), to ensure;

- The service does not create problems or difficulties for the Trust or for patients
- An Owner or Local Organisation Administrator (LOA) of the e-mail account should monitor activity, assess risks and audit the effectiveness of the service
- Risks are identified, regularly re-assessed and adequately addressed
- The service is providing good value to the Trust and to users
- Confidentiality is not put at risk

DATA QUALITY AND NHS NUMBER

Reliable information is a fundamental requirement for the Trust to conduct its business efficiently and effectively. This applies in all areas of activity including the delivery of care to service users, service management, performance management, corporate governance, internal and external accountability and communication. Data Quality (DQ) is a crucial pre-requisite to information that is complete, relevant, accurate and timely.

Rationale
Ever-increasing use of computerised systems provides greater opportunities to store and access many types and large volumes of data but also increases the risk of misinformation if the data from which information is derived is not of good quality. This risk applies both to the Trust's internal use of information and to information conveyed in the form of statutory returns to the national databases;

- Data Warehouse
- Secondary Uses Service (SUS)
- Child Health Information System (CHIS)

For information to have value, it is essential that the data that underlies it is consistent and complies with national standards. NHS Trusts are assessed and judged on the quality of the data they produce. National performance indicators and audit assessments depend on good quality data for their accuracy and indeed include DQ amongst them.

Compliance with high DQ Assurance standards is an implicit requirement for Foundation Trust status.

Scope
This is intended to cover all data that is entered onto computerised systems within the Trust and should be read in conjunction with the other Trust Policies or Operational Guidance relating to the system.

It covers primarily data relating to individuals (staff, service-users or third-parties) and the delivery of care but also includes other data that relates to financial management, service management, performance management, corporate governance and communications. '

Service-user' data is held on clinical information systems owned by the Trust or accessed under SLA with host organisations. The Trust also operates a range of non-clinical information systems that support its business processes. This applies to all staff that use, or supply data that is input to, those systems. It outlines good practice and identifies the roles and responsibilities of both the Trust and its staff in terms of DQ.

Core Principles
The Data Protection Act 2018 requires, amongst other things, that information held on computer systems is accurate and up to date.

There will be identified individuals within the Trust, including those in the areas of informatics, health records, clinical coding, data protection, and Caldicott, with particular responsibility for DQ issues in those areas. Their specific responsibility in this respect will be explicitly stated in their job descriptions.

Responsibility for the strategic management of DQ in the Trust lies with the I&P Team.

Responsibility for the operational management of DQ will lie with the operational managers of all services to which this applies.

All data collection and input processes will have an audit trail that operates continuously. Any training and development issues identified in the course of auditing will be addressed promptly.

All users will be made aware of their individual and the Trust's corporate responsibility for confidentiality and security of data through the Trust's relevant policies.

Common Standards
The common standards of good quality data are:

Accuracy
The data recorded must accurately reflect the actual state that is being described. In particular, every opportunity will be taken to check demographic details with the service user and update their record to avoid inaccurate demographic data resulting in correspondence being misdirected, or service users misidentified.

Validity
All data items held on Trust computer and other record systems must be valid and contextually logical. Where possible free-text fields will be avoided and standard codes or options used which comply with national standards or map to national values. Wherever possible, computer systems will be programmed to only accept valid entries. In particular, steps will be taken to ensure that service user details are validated for changes and accuracy throughout the duration of care received from the Trust.

Consistency
Data items will be populated in an internally consistent fashion. All reference tables and codes will be audited and updated regularly with reference to national and local data sources.

Completeness
Every effort will be made to ensure that data in a record is complete, such that all relevant items are populated. It is required that all mandatory data items within a dataset are populated. Use of default codes will only be permitted where appropriate, and not as a substitute for real data. If it is necessary to bypass a data item in order to progress the delivery of care to a service user, such an event will be notified to the appropriate authority immediately for corrective action.

Coverage
Every effort will be made to ensure that recorded data reflects all of the Trust's activity. Systems and processes will be reviewed to ensure complete data capture. Audit procedures will be developed and routinely applied to identify missing data.

Timeliness
The timely recording of data is essential to the efficient and effective operation of processes, including the delivery of care. Data needs to be present at the time that processes require it, for both service delivery and reporting purposes. To that end key-staff need to be aware of relevant deadlines. These requirements will not be allowed to compromise the urgent treatment of service users.

Documented Procedures
In order to minimise errors and achieve good quality data, appropriate written procedures and guidance must exist so that staff can be supported in their work and have access to up to date training materials and sources.

Details of these procedures, training and processes will be held by the relevant System Administrator and made available to all system trained staff.

Each system will have a named Information Asset Owner (IAO) and a named Information Asset Administrator (IAA) (for smaller scale systems these may be the same person) who will be responsible for access, System use and maintenance and DQ Assurance (Some of these tasks may be completed by other departments).

Controls Assurance
DQ will be subject to internal control processes within the Trust and through external scrutiny**.**

Internal controls

- All information systems and processes will have routines developed and designed to systematically identify errors and other aspects of poor DQ
- Reports will be generated regularly and considered by the appropriate Business Units which will make recommendations regarding the improvement of DQ
- Reports will be routinely fed back to operational managers with advice as to corrective action to be taken such as improving processes and systems and staff training and development.
- Audit of case records and DQ by internal auditors.

System Utilisation Checks
The Information and Performance Team (I&P) will undertake additional checks to ensure that activity recorded is consistent with known or expected activty levels. The checks will give an early warning if activity is not reflective of the Trust.

Reporting Arrangements
DQ reports and findings will be presented to the appropriate departments responsible for performance as soon as they are available who will recommed re-checks or checks on systems not yet undertaken.

External controls

- DQ reports from SUS, CDS DQ indicators
- Queries from commissioners, queries from service user
- Audit of records and DQ by external auditors e.g. Care Quality Commission (CQC)

The Trust will aim to be significantly above average in all indicators and will strive for 100% accuracy and will act on all enquiries, recommendations and complaints from commissioners, service users and external auditors.

Use of the NHS Number
The NHS number is fundamental and is the common unique identifier to identify and link patient information that makes it possible to share patient information across the whole of the NHS safely, efficiently and accurately. It is a unique 10 digit number, the first nine are the identifier and the tenth is a check digit used to confirm the number's validity.

The NHS Number is the key to unlocking services such as the NHS Care Records Service, Choose and Book or the Electronic Prescription Service (EPS)

Staff have a vital role in ensuring it is used throughout the Trust.

NHS Number Targets and Standards
The Trust aims for 100% completeness of verified NHS numbers for patients and service users accessing its services.

- All electronic systems recording patient / service user information include the facility to capture the NHS number
- All relevant paper-based documents used to collect, store, transfer or amend patient / service user information can record the NHS Number.
- Set in place common procedures for the management, tracing and monitoring of the NHS number within the organisation
- Enable relevant, approved staff to have access to methods of tracing and verifying patient / service user NHS numbers.

The Trust will design and implement standard letters and documents for communication within the NHS that include the verified NHS Number and recommends that the NHS Number is, as a minimum, used on the following:

- Clinical records - detail and discharge summaries
- Referrals to other organisations-including electronic bookings
- Clinic appointment letters , test requests, samples and results
- All communications related to service users includes the NHS Number

Within the NHS and to non NHS organisations, wherever possible, PCD, (apart from the NHS number) should not be sent electronically or on paper. Where this is unavoidable then the data must be protected in accordance with the Information Security Policy, Caldicott Principles and the Data Protection requirements.

The Trust will require that other NHS organisation's include the patient's / service users' verified NHS number in all communications to the Trust.

The Trust will monitor and report on the recording of the NHS number on electronic systems on a regular basis through the DQ Reports.

All patient / service user case notes will include the verified NHS number, except where this is not applicable e.g. Sexual Health who use a Unique ID Number.

The Trust will arrange for regular external audit of its use of the NHS number. (This may be conducted as part of other broader DQ audits)

Responsibilities of all Staff
All staff are obliged to adhere to their responsibilities and Managers at all levels are responsible for ensuring that staff for whom they are responsible adhere to this ensuring changes are communicated to staff.

Title	Role	Responsibilities
Trust Board	Strategic	Strategic overview and final responsibility for setting the direction for data quality within the Trust
Audit Committee *(charged with ensuring data quality)*	Accountable	A sub-committee of the Trust Board has delegated responsibility for ensuring DQ is undertaken efficiently and effectively in accordance with the Board's Assurance Framework (BAF) and strategic priorities
Lead Director *[Senior Information Risk Owner (SIRO)]*	Executive Lead	Responsibility has been delegated by the Chief Executive to the SIRO: • responsible at Trust Board and Executive level for Trust strategic direction for DQ • Monitor performance against DQ ensuring corrective action is taken where necessary • Agreeing action plans to address DQ issues • Update the Trust Board regularly on DQ issues.
Information Governance Management Assurance Group *(IGMAG)*	Accountable	Responsibility for the IG Agenda and works alongside the Countywide IG Management Group (CWIMG) and the Quality and Risk Committee (Q&R). IGMAG signs off all elements of the IG Agenda of behalf of the Trust.
Head of Information & Performance – I&P	Operational Lead	Responsible for ensuring that this is implemented and that DQ management systems and processes are developed, co-ordinated and monitored in line with DQ standards.
Information Governance (IG)	Operational	Responsible for implementing and applying the legal framework governing the use of PCD in health and to comply with the NHS Act 2006, the Health and Social Care Act 2012, the Data Protection Act 2018, and the Human Rights Act.
Senior Managers & Service leads *[Information Asset Owners] - IAO*	Operational	IAO and Department Managers are responsible for ensuring that staff attend training in the use of information assets and standard operating procedures for data collection and recording are maintained for each operational area.
Information & Performance Staff	Operational	Interpret the requirements of the NHS Data Model and Dictionary for England to ensure compliance of all Trust data Monitor and disseminate changes to requirements as notified via Information Standards Notices (ISN's) / official channels Ensure that systems support robust data collection Produce or enable DQ exception reporting to monitor data quality Be aware of and comply with legislation and Trust policies and procedures Work in partnership with operational services to improve DQ
Clinical & Admin Staff (including Health Records , Clinical Coding and other relevant roles	Operational	The fundamental principle of DQ is data should be right first time, which means that the responsibility is held at the point at which it is collected and recorded, whether the person recording the information is clinical, technical or clerical. Therefore all staff are responsible and accountable for the quality of data they collate and record.

NHSLA Monitoring

Minimum requirement to be monitored	Process for monitoring e.g. audit	Responsible individuals/ group/ committee	Frequency of monitoring /audit	Responsible individuals/ group/ committee (multidisciplinary) for review of results	Responsible individuals/ group/ committee for development of action plan	Responsible individuals/ group/ committee for monitoring of action plan
DSP Toolkit Standards	Review / Audit / Reports	IG Lead	Annual	IG Lead / IGMAG	IG Lead / IGMAG	IG Lead / IGMAG

Equality Analysis

A.	Briefly give an outline of the key objectives of the policy; what it's intended outcome is and who the intended beneficiaries are expected to be	To provide clear and effective management and accountability structures, governance processes, documented policies and procedures, a comprehensive IG training programme and adequate resources to manage and embed IG throughout the Trust.		
B.	Does the policy have an impact on patients, carers or staff, or the wider community that we have links with? **Please give details**	All Staff and Service Users		
C.	Is there is any evidence that the policy\service relates to an area with known inequalities? **Please give details**	No		
D.	Will/Does the implementation of the policy\service result in different impacts for protected characteristics?	No		
		Yes	No	
	Disability		X	
	Sexual Orientation		X	
	Sex		X	
	Gender Reassignment		X	
	Race		X	
	Marriage/Civil Partnership		X	
	Maternity/Pregnancy		X	
	Age		X	
	Religion or Belief		X	
	Carers		X	
	If you have answered 'Yes' to any of the questions then you are required to carry out a full Equality Analysis which should be approved by the Equality and Human Rights Lead – please go to section 2			
The above named policy has been considered and does not require a full equality analysis				
Equality Analysis Carried out by:		Kaz Scott		
Date:		June 2018		