North West London Collaboration of Clinical Commissioning Groups

Digital North West London

Summary of Caldicott 3 Review by North West London Digital IG Governance Group: 1st September 2016

Background

North West London Digital IG Governance Group (NWL Digital IG GG) was established in January 2015 and is made up of IG experts from across health and social care.

The group oversees and supports the NWL Digital Information Sharing Agreement, maintaining the secure sharing of information for all partner providers and the programmes noted within, supporting the established governance model of data controllers in common.

This group also drives the digital information governance agenda locally and provides assurance to the NWL provider partners by working collaboratively to implement information governance best practice mechanisms across organisational boundaries.

Members

- Imperial College Healthcare NHS trust
- Chelsea and Westminster Hospital NHS Foundations Trust
- The Hillingdon Hospitals NHS Foundation Trust
- London North West Healthcare NHS Trust
- West Middlesex University Hospital
- Central and North West London NHS Foundation Trust
- Central London Community Healthcare NHS Trust
- Hounslow and Richmond communities
- West London Mental Health Trust
- Brent Council
- Hounslow Council
- Harrow Council
- Ealing Council

- Westminster City Council
- Hammersmith & Fulham Council
- Royal borough of Kensington and Chelsea Council
- GP representation, Hammersmith & Fulham Network
- GP representation, Hounslow Network
- GP representation Harness , Network (Brent)
- GP representation, Kilburn Network (Brent)
- GP Representation, Hillingdon Early Adopter
- GP Representation, Harrow
- Patient representatives: John Norton and Angeleca Silverside
- North West London Collaboration of CCG's
- NWL Digital Programme
- Kaleidoscope Consultants

Summary and Main themes

I. Clear definition of what constitutes direct care for care providers; what does it include i.e. health marketing, case finding purposes.
II. Ability of Opt Out; difficult for all systems to align opt outs. Needs to be more clarity and definition across the care settings and systems, specifically using the same coding
III. When data sharing, it is important to look at patient pathways and how they access care across their journey, needs to be less focus on the areas of care.
IV. Definition and guidance is needed on the various layers of proportionality needed in multidisciplinary care.
V. Inability of current clinical systems to provide functionality to effectively support data controllers and multidisciplinary care.
VI. Further definition of Role Based Access control, which also includes bringing social care into the NHS family and further defining roles within social care that need access but are not registered social workers.
VII. Support for the model of opting out of anonymous use of information for secondary purposes.

Cyber Security Standards

Security Standards	NWL Digital IG Group Response
1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.	Agree, however more consideration is needed for those organisations that have already gone completely paperless. More support and guidance needed specifically around where a citizen's preference is paper and also management and handling of legacy records and paper.
2. All staff understand their responsibilities under the National Data Guardian's Data Security Standards including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.	Proportional training for care professionals is needed, however this is not just about the NHS family and social care, needs to be extended to private companies/third party suppliers (include those IT suppliers). There is a need to support the development of the growing trend of commissioning charities and companies to provide services and health and well-being intervention to the population, keeping people well for longer in their local communities and homes. Whilst this should be a minimum requirement to staff to who work within healthcare, not all 98% of staff (IG Toolkit requirement) can be trained, should be a more sensible approach that is based on their role and access to information and job role, specifically there needs to be more training for Analysts and supporting functions (i.e care coordinators) handling volumes of data for BI and Case finding.
3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.	There will be a significant resource implications for this, cannot guarantee that all staff can be trained. Training courses for both information security and data protection need to be accredited by the HSCIC for both health and social care organisations and even those private and 3rd sector organisations providing care. All of the training courses need to be based on role and the information they are using, training must be proportional and universally consistent. In most organisations all staff do mandatory training however due to resource implications some of the larger organisation felt that not all staff need training necessary up to the IG Toolkit training level (98%) as the courses were not proportionate to the roles of their staff members, therefore the long tests are a big

	resource and time implication for all parties and not a good indicator of security within an organisation.
4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.	Agree, needs to be more alignment with health and social care systems, more accredited standards that both can adhere to support interoperability. Granularity of systems also needs to improve for affective RBAC and proportionality of records shared and viewed. This should be clearly stipulated as part of new or renewed contracts with IT suppliers.
5. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.	Agree
6. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.	Agree, but there are inconsistencies in clinical systems, all need to have standard capabilities, especially as records are opened to patients and their next of kin, carers, guardians etc. Need to increase funding to update systems so all are able to meet present and future requirements.
7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.	Agree, penetration testing should be enforced as standard for all organisations that are storing or processing information. However GP's will struggle to do this locally as private respires; more funding for GP's is needed to support them as budgets for primary care centrally are being reduced, or, NHS England's GPSOC needs to pick this up on their behalf as commissioners of GP systems.
8. No unsupported operating systems, software or internet browsers are used within the IT estate.	Agree, needs security standards
9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.	Cyber Essentials; define framework further, what does that mean to organisations? More direction and support is needed.

10. Suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standard.	Agree, we already a standard for sub-data processors subject to Digital ISA to adhere to set of ISO standards, with a liability clause within Data Processing Agreements that cover the providers/Data Controllers from accountability as part of a breach. There is a need to impose standards on private 'partners' as more care organisations partner with private industry for research etc. There is ambiguity and lack of clarity on the responsibilities of the procurement process through GPSOC. NHS England need to enforce standards in GPSOC and other national contracts enable these to be fit for purpose for both care professionals, organisations and the public. **In addition to the above the national team should set out clear standards for all contractual arrangements, new or to be renewed, for all IT suppliers to safeguard data controllers. This is been an approach that has been encouraged by our LLMC and has proven helpful in accelerating the delivery of some of our local plans.**

Proposed Consent/Opt Out Model

Proposed Consent/Opt Out Model	NWL Digital IG Group response
1.You are protected by the law. Your personal confidential information will only ever be used where allowed by law. It will never be used for marketing or insurance purposes, without your consent.	Agree in principle, consent needs to be explicit consent for marketing and insurance companies. However the term marketing needs to further defined, 'Health marketing' to citizens can provide interventions from both a patient centred and public health level.
2. Information is essential for high quality care. Doctors, nurses and others providing your care need to have some information about you to ensure that your care is safe and effective. However, you can ask your health care professional not to pass on particular information to others involved in providing your care.	Needs to be defined further, currently there is an all or nothing approach which is not fit for purpose when sharing across care settings. Current system suppliers need to be encouraged to develop this capability. Should be a requirement for any new suppliers and there is also a need for universal clinical coding to support the delivery of integrated care across the system.

	We need to be able to define the wider care team, 'Care Professionals' also need to include social care staff that are not registered social workers but do the same/similar roles and need access to a portion of a medical record. Care pathway is managed by more than just care professionals, should be more patient centred, look at how and where they access care based on need and condition, better to co-defy types of data. Paper records still in use, cannot exclude information, more funding is needed for a paperless by 2020 target.
3. Information is essential for other beneficial purposes. Information about you is needed to maintain and improve the quality of care for you and for the whole community. It helps the NHS and social care organisations to provide the right care in the right places and it enables research to develop better care and treatment.	Agree as long as information is Anonymous, needs to have opt out process built in for patients. 'Use of data' is a broad term that means many things, should be split up into sharing, processing and viewing, for secondary purposes this should all be done with anonymous information and bulk should be done within accredited safe heavens in safe areas or black box environments. Support for longitudinal local care populations, and supports population analytics with anonymous information.
4A. You have the right to opt-out. You have the right to opt-out of your personal confidential information being used for these other purposes beyond your direct care. This opt-out covers: a. Personal confidential information being used to provide local services and run the NHS and social care system.	Clearer definition is needed for purposes beyond your direct care and should always have an option to opt out to respect the persons' wishes. The basis that PCD will only be used on a need to know basis, need to make sure that all other avenues of processing are addressed before using identifiable information for secondary purposes. For anonymous information for these purposes, we would suggest an opt-out model.

4b. You have the right to opt-out. Personal confidential information being used to support research and improve treatment and care. For example: • a university researching the effectiveness of the NHS Bowel Cancer Screening Programme • a researcher writing to an individual to invite them to participate in a specific approved research project This choice could be presented as two separate opt-outs. Or there could be a single opt-out covering personal confidential information being used both in running the health and social care system and to support research and improve treatment and care.	Disagree with this, opt out model should be used for local longitudinal studies, however at the point of they require PCD information, they should contact patients to get explicit consent, furthermore these citizens should only be contacted on their explicit consent, on the proviso that information used by research is annonlymous. The citizen should choose whether or not they wish to be contacted and again to take part in the trial, screening or research process.
5. This opt-out will be respected by all organisations that use health and social care information. You only have to state your preference once, and it will be applied across the health and social care system. You can change your mind, and this new preference will be honoured.	Agree, however there will be resource and software implications therefore more funding is needed for all to link into national consent database. North West London health and social care organisations are currently developing their own local solution as part of the Care Information Exchange.
6. Explicit consent will continue to be possible. Even if you opt-out, you can continue to give your explicit consent to share your personal confidential information if you wish, for example for a specific research study.	Agree, important to adhere to personal preferences, unless break glass is needed.

7. The opt-out will not apply to anonymised information. The Information Commissioner's Office (ICO) has a Code of Practice that establishes how data may be sufficiently anonymised that it may be used in controlled circumstances without breaching anyone's privacy. The ICO independently monitors the Code. The Health and Social Care Information Centre (HSCIC), as the statutory safe haven for the health and social care system, will anonymise personal confidential information it holds and share it with those that are authorised to use it. By using anonymised data, NHS managers and researchers will have less need to use people's personal confidential information and less justification for doing so.	Agree, however this is depend on the HSCIC on the readiness to fully service and support local requirements. dependency requirement for the HSCIC, therefore an initial shutting off of local processing could cause paralysis in the system unless HSCIC systems are fully capable. This approach needs to transitioned over safe period of year, with an acceptance process by local areas and user acceptance arrangements. More information and clarification is needed about deceased patient data.
8. The opt-out will not apply in certain exceptional circumstances. The opt-out will not apply where there is an overriding public interest, such as preventing and responding to natural disaster; monitoring and control of important diseases in humans such as TB and diseases of epidemic potential such as Ebola; infections that pass between animals and humans such as the Zika virus; and for chemical, biological, radiological and nuclear events. It would also include personal confidential data for monitoring and control of communicable diseases and other risks to public health. The opt-out will not apply where there is a mandatory legal requirement. This includes: • the Care Quality Commission, which has powers of inspection and entry to require documents, information and records;	Needs further work in defining where, when and what can be shared, specifically focusing around guidelines for the appropriate justification for sharing information without explicit consent.

• the HSCIC, the statutory safe haven, which has powers to collect information when directed by the Secretary of State or NHS England; • the NHS Counter Fraud Service, which has powers to prevent, detect and prosecute fraud in the NHS; • investigations by regulators of professionals; • coroners' investigations into the circumstances of a death, i.e. if the death occurred in a violent manner or in custody; • health professionals must report notifiable diseases, including food poisoning; • the Chief Medical Officer must be notified of termination of pregnancy; • employers must report deaths, major injuries and accidents to the Health and Safety Executive; • information must be provided to the police when requested to help identify a driver alleged to have committed a traffic offence; or to help prevent an act of terrorism or prosecuting a terrorist; • information must be shared for child or vulnerable adult safeguarding purposes; and • health professionals must report known cases of female genital mutilation to police. In addition the Review also sets out that the following should not be part of the opt-out: • some forms of invoice validation where there is no alternative solution, such as the use of anonymised data; • demographic information flows (e.g. NHS number, address) into the Office of National Statistics (ONS) for the production of official statistics e.g. to look at internal migration; • national registers of disease including cancer where there will be a new approach to informing patients about registration.	

8. The opt-out will not apply in certain exceptional circumstances. The opt-out will not apply where there is an overriding public interest, such as preventing and responding to natural disaster; monitoring and control of important diseases in humans such as TB and diseases of epidemic potential such as Ebola; infections that pass between animals and humans such as the Zika virus; and for chemical, biological, radiological and nuclear events. It would also include personal confidential data for monitoring and control of communicable diseases and other risks to public health. The opt-out will not apply where there is a mandatory legal requirement. This includes: • the Care Quality Commission, which has powers of inspection and entry to require documents, information and records; • the HSCIC, the statutory safe haven, which has powers to collect information when directed by the Secretary of State or NHS England; • the NHS Counter Fraud Service, which has powers to prevent, detect and prosecute fraud in the NHS; • investigations by regulators of professionals; • coroners' investigations into the circumstances of a death, i.e. if the death occurred in a violent manner or in custody; • health professionals must report notifiable diseases, including food poisoning; • the Chief Medical Officer must be notified of termination of pregnancy; • employers must report deaths, major injuries and accidents to the Health and Safety Executive; • information must be provided to the police when requested to help identify a driver alleged to have committed a traffic offence; or to help prevent an act of terrorism or prosecuting a terrorist;	Agree that national registers of patients are beneficial to both patients and the health and care economy however; there are concerns around the standards of these registered and the systems they are being held on. There is a need to enforce the same ISO standards on those systems/system providers that hold registers as there is for NHS organisations. There are concerns about making data available in relation to traffic offences.

• information must be shared for child or vulnerable adult safeguarding purposes; and • health professionals must report known cases of female genital mutilation to police. In addition the Review also sets out that the following should not be part of the opt-out: • some forms of invoice validation where there is no alternative solution, such as the use of anonymised data; • demographic information flows (e.g. NHS number, address) into the Office of National Statistics (ONS) for the production of official statistics e.g. to look at internal migration; • national registers of disease including cancer where there will be a new approach to informing patients about registration.	

Appendix A: Specific Concerns voiced in relation to Primary Care

1. Standards and agreement across general practice on record keeping and Coding will directly affect clinician's ability to share data and obtain meaningful consent:

- practices have very different approaches to what is Coded and what Codes are used, which impedes digital integration and raises clinical risk
- There is no agreed reference on standards. 'Good Practice Guidelines for GP electronic patient records - version 4' contains generic principles only. It is now 5 years old and.
- This topic is largely absent from the undergraduate & GP training curricula.
- There is a need for a combination of guidance, agreement and training materials for all primary care staff members, not just GP's so that they are able to deal with patients queries when asked.
- Introduction of SNOMED-CT (affecting future workforce) may be an opportunity for health and social care organisation to standardise consent and align consent but this agenda will require a significant resource.

2. Need further clarity about change to ability to dissent from two specific uses, as we (and the intention to abolish the right to Type 1 and 2 objections)

- the consent/dissent model (as described in the Public Consultation) will influence how GP records are kept and the information patients are prepared to divulge
- there is an assurance that, in sharing for direct care, the patient can tell the doctor not to share some bits of information, leading to:-
    - patient safety issues if information missing but record thought to be complete
    - technical problems in implementing the same functionality across different systems
    - Maintenance of trust when patients registering Type 1/2 objectors are told that plans have changed. What guarantee there will not be other changes?
- There is a paucity of information about the form in which linked data will be accessed by those approved by the HSCIC/NHS Digital