NDG National Data Guardian
for health and social care

The importance of maintaining trust in data use – and the conditions that create trust

Dr Nicola Byrne
National Data Guardian for Health and Social Care

Digital Health Rewired 2022
Design Business Centre, London
15 March 2022

Today’s presentation will cover:

- Importance of trust in a confidential health and care service
- Why it matters, and what happens when trust is damaged
- Public attitudes research: what do people think?
- What are the components of public trust

What are we talking about when we talk about trust?

- Maintaining trust in a **confidential health and care service**
- Encouraging **demonstrably trustworthy systems and processes** for data use (the cornerstone of the NDG role)
- Speaking up for the public and **reminding data decision makers whose confidential information it is** – who the most important stakeholders are
- Public *and* professional trust matters for **individuals' care** and the **social license for secondary uses**, if we are to maximise the benefits of data use for our health and the sustainability of our publicly funded system

What happens when trust is lost?

- Trust is hard to earn and very easy to lose
- When trust is lost, the consequences are considerable:

— Damage to the patient - clinician relationship of trust

— Loss of social licence to use people’s data for secondary purposes

Damage to the patient clinician relationship

- People need to be able to trust they can share information without worrying how it will be used subsequently within, or beyond, the health and care system
- Health and care professionals need reassurances around data use too, for them to support, and enable, its collection and use
- Data used in ways that people may not expect (or support) undermines both
- It may deter people from seeking treatment or telling the truth to their clinicians
- It may deter clinicians from fully and accurately documenting information shared
- For example – recent consideration of the proposed health and care data sharing in the Police, Crime, Sentencing and Courts Bill, now amended

Loss of social license

- When patients and professionals are not engaged and informed we risk losing their support
- General Practice Data for Planning and Research programme illustrates this - good intentions alone are not enough
- The system must listen to what matters to people: meet the conditions necessary for public and professional support – or else trust will be lost
- Thankfully, we already know a lot about what people think needs to be considered – what they worry about, and what's required to earn their trust and support

What do people worry about? (1)

- Our opinions are frequently based upon hearsay and anecdote, not fact
- The stories we share are often protective - focus on risks and concerns
- Media holds a mirror to, and in turn shapes, our shared conversations - focus often on the negative, using emotive language
- Case in point – GPDPR, media discourse around ‘data grab’, not benefits

What do people worry about? (2)

- Hacking and cyber crime
- Unintentional data leakage or loss
- Unauthorised access / access without explicit consent
- Reidentification risks – will people know it's me?
- Data aggregated to a group's disadvantage
- Consequences for employment, pension eligibility, insurance, visas
- The use of data for marketing, or to further political agendas
- Third parties using of data for financial gain

How do organisations build and maintain trust?

- **Caldicott Principle 8**: inform patients and service users about how their confidential information is used – ensure no surprises
- **Clear communications and authentic engagement**: holding honest conversations with the public– explain what you are doing, dispel any '*nothing to see here*' attitude: we know people are much more likely to support a data initiative once it's explained and they've had a chance to ask questions
- **Inclusivity**: ensure diversity of views, take steps to reach seldom-heard communities
- **Don't forget to engage with professionals** as systems must work for, and be trusted by, them too

....but when we communicate, what do people want to know?

Demonstrating a data system is trustworthy (1)

- **Be clear about purpose** – potential benefits, and who will seem them?
- **Engage with potential risks and harms –** what are the safeguards; how is data kept safe and secure; how will any incidents be learnt from?
- **Governance** – who holds responsibility and how are decisions made; what are the sanctions for any improper use, and how would they be enforced?
- **Transparency** – **who** is accessing **what** data, **how** do they get it and **why** - what will they do with it, then what are the **outcomes** from use? *Both our citizens' jury and public benefits dialogue work has reinforced this*
- **Clarity of choice** – what choices do individuals have? What data use can they opt out of, and how?

Demonstrating a data system is trustworthy (2)

- **Public involvement in decision making** – lay representation e.g. in data access committees; involve people in decisions about 3rd party access and open up to the 'fresh air and challenge' of public oversight - otherwise suspicion grows about motives, vested interests and 'what's going on behind closed doors'
- **Reassurance** – what will *not* be done with the data (e.g. not shared or sold for insurance and marketing purposes), and evidence that data partnerships are principally motivated by improving patient outcomes; the public must be satisfied that public benefit will outweigh potential commercial profit

National Data Guardian contact information

Website
https://www.gov.uk/government/organisations/national-data-guardian

Twitter
@ndgoffice

Email
ndgoffice@nhs.net