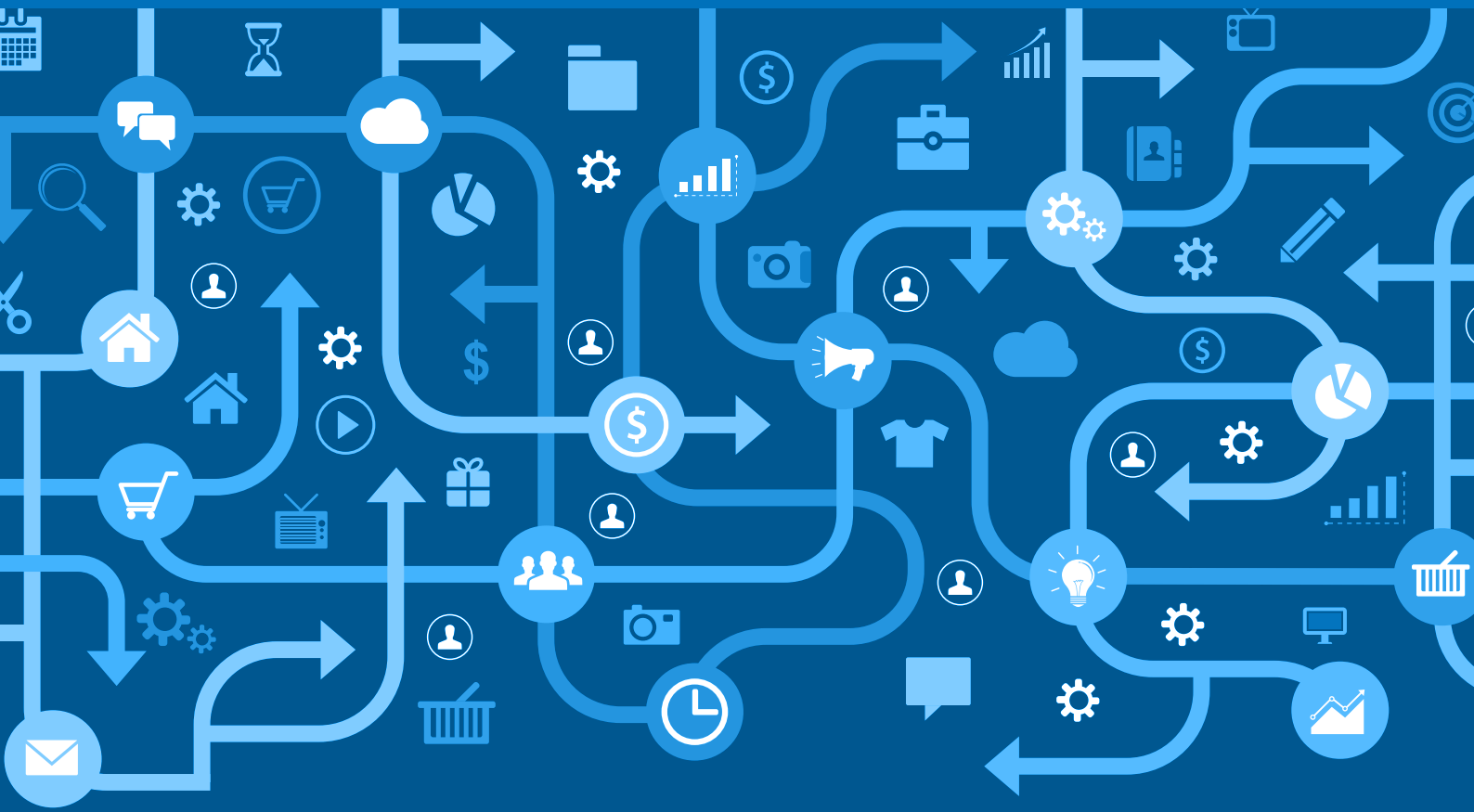
Putting information sharing at the heart of collaborative working.

Information sharing between the police and health services for prevention, early intervention and care purposes.



Introduction and case studies

Centre of Excellence for Information Sharing

Home Office

UKCGC
The United Kingdom Caldicott Guardian Council

www.informationsharing.org.uk/healthandpolice

Contents

This resource (including the case studies) was written prior to the introduction of the General Data Protection Regulations (GDPR) and will be updated in May 2018.

Christopher Fincken: Chairman of the UK Caldicott Guardian Council 2012-2017

Data sharing is vitally important. Organisations must work together, to effectively and efficiently deliver services. People need to be able to trust organisations with "their" data, and be confident that it is being used, and looked after; safely and securely. Trust underpins all these relationships, but it is fragile, and once damaged can be difficult, or in some cases impossible to repair.

Where trust exists, there are many examples of excellent data sharing between the Police and health and care services. These illustrate how, by working together, using accurate and relevant data to deliver services, efficiencies are gained and services enhanced.

Measures (sometimes called "Information Governance (IG)") are in place to protect trust, by ensuring that organisations can demonstrate that; the data they hold is used both legally and ethically. IG is not an obstruction to legitimate innovation and service delivery, but a safeguard; supporting and enabling the lawful and ethical sharing of data. It is sometimes said that Caldicott and IG are a barrier to data sharing and service improvement. This should not be the case!

The case studies in this document, demonstrate how IG can enable and support health services and the Police to work effectively together, developing new ways of improving care and delivering services. Each example illustrates not only the legal basis for their work, but also how "ethics" have been considered, by the application of the Caldicott Principles.

The full legal obligations of information governance are often highly complex and may also have to be balanced against fulfilling requirements under "the common law duty of care". Although the "gold standard" for IG remains full legal compliance with ALL legislation, and professional guidance, there may be some cases where the degree to which Information Governance "rules" are applied is modified by the obligation or desirability of delivering an immediate or vital service to an individual. Whilst adherence to the law is crucial , it should not place individuals in preventable danger. It is important not to allow perceived obstacles or difficulties to get in the way of achieving the right outcomes – particularly around safeguarding individuals. Each of the case studies illustrate the transformative possibilities of working together to overcome barriers and deliver improved services to some of the most vulnerable people in society.

The importance of creating and maintaining trust between individuals and the organisations that provide their services is widely recognised, but trust also needs to exist between organisations, so that they can be confident in sharing the data they hold. Being confident in understanding both the legal and ethical basis for their work, underpins the ability of professionals, to reach out to others in partner organisations. The joint development of new ways of working, sometimes in complex situations, helps foster trust.

The case studies have been developed with the professionals involved to bring them to life as real examples. The seven "Caldicott Principles"[1] were applied and this structured approach is shown in each case in the format of a table. The case studies may differ in their use of language and style and this is intentional, as local initiatives quite often develop their own vocabulary but are unified by demonstrating the benefits of the Police and health services working collaboratively together.

I hope that this document will provide not just another "set of rules", but meaningful guidance to inspire and motivate others, to introduce, or develop, ways of working that are legal, ethical and deliver service improvements.

Chairman of the UK Caldicott Guardian Council 2012-2017

[1] Caldicott principles - www.igt.hscic.gov.uk/Caldicott2Principles.aspx

Putting information sharing at the heart of collaborative working

Information sharing between the Police and health services allows early intervention and preventative work, enables better care for patients, supports safeguarding and the promotion of welfare and improves public protection. It is important for the Police and health services to find new ways to work together. Effective information sharing improves services for members of the public, particularly in emergencies or when someone is near crisis.

This document provides case studies from across England that show how different approaches to innovation have been developed cost effectively. They illustrate what is possible whilst recognising and respecting both the legal and ethical frameworks. All of the case studies covered in this resource are the results of local and national initiatives where information sharing was identified as a 'root cause' of problems within local practice.

While this document focuses on information sharing between police and health services - the case studies also include examples of sharing between these agencies and voluntary organisations.

The purpose of this document

The Home Office (HO),[2] Information Governance Alliance (IGA),[3] the Centre of Excellence for Information Sharing (CoE)[4] and the UK Caldicott Guardian Council (UKCGC)[5] have prepared this document to support collaborations between Police and health services that involve the sharing of information for individuals for their care. This document is prepared for:

Police

- police chief officer team;
- police information officers;
- local police training leads;
- local police mental health officers;
- local police lead for custody; and
- police and crime commissioners.

Health

- clinical commissioner's groups (CCG's);
- local government commissioners for mental health;
- general practitioners (GP's);
- senior information risk officer;
- local health information governance leads; and
- Caldicott Guardians.

[2] The Home Office - www.gov.uk/government/organisations/home-office

[3] Information Governance Alliance - https://digital.nhs.uk/information-governance-alliance

[4] Centre of Excellence for Information Sharing - http://informationsharing.org.uk/

[5] UK Caldicott Guardian Council - www.gov.uk/government/groups/uk-caldicott-guardian-council

Better information sharing can help to improve services for members of the public. This document illustrates what is possible within existing parameters and is intended to act as a focus for local discussion of how to overcome perceived barriers. It does not replace or contradict current legislative provisions or guidance on information sharing. In all cases information sharing must be;

- lawful;
- limited to that data or information which is necessary for the purpose for which it is being shared;
- shared only with those individuals who need to have it;
- based on information which is accurate and as up to date as possible; and
- timely.

Detail of the legal basis for information sharing between the Police and health services is provided on page ten.

Although the teams described in these case studies regularly deal with safeguarding issues and incidents, this document does not directly address this challenge or replace existing guidance on this subject. In this document the phrase "service users" means members of the public that use the services of all organisations mentioned and "patients" when it's a health service.

Cultural issues affecting information sharing

Every organisation will have an existing information sharing culture that influences how staff behave and 'feel' about information they hold about individuals.

In some situations, staff are very protective of maintaining the confidentiality of the information that has been entrusted to them and are rightly reticent about sharing it. The Common Law Duty of Confidentiality[6] means that information provided in confidence must remain confidential unless there are overriding considerations (e.g. child safeguarding or public protection). In addition, information that is recorded will also be covered by the provisions of the Data Protection Act 1998 (DPA).[6]

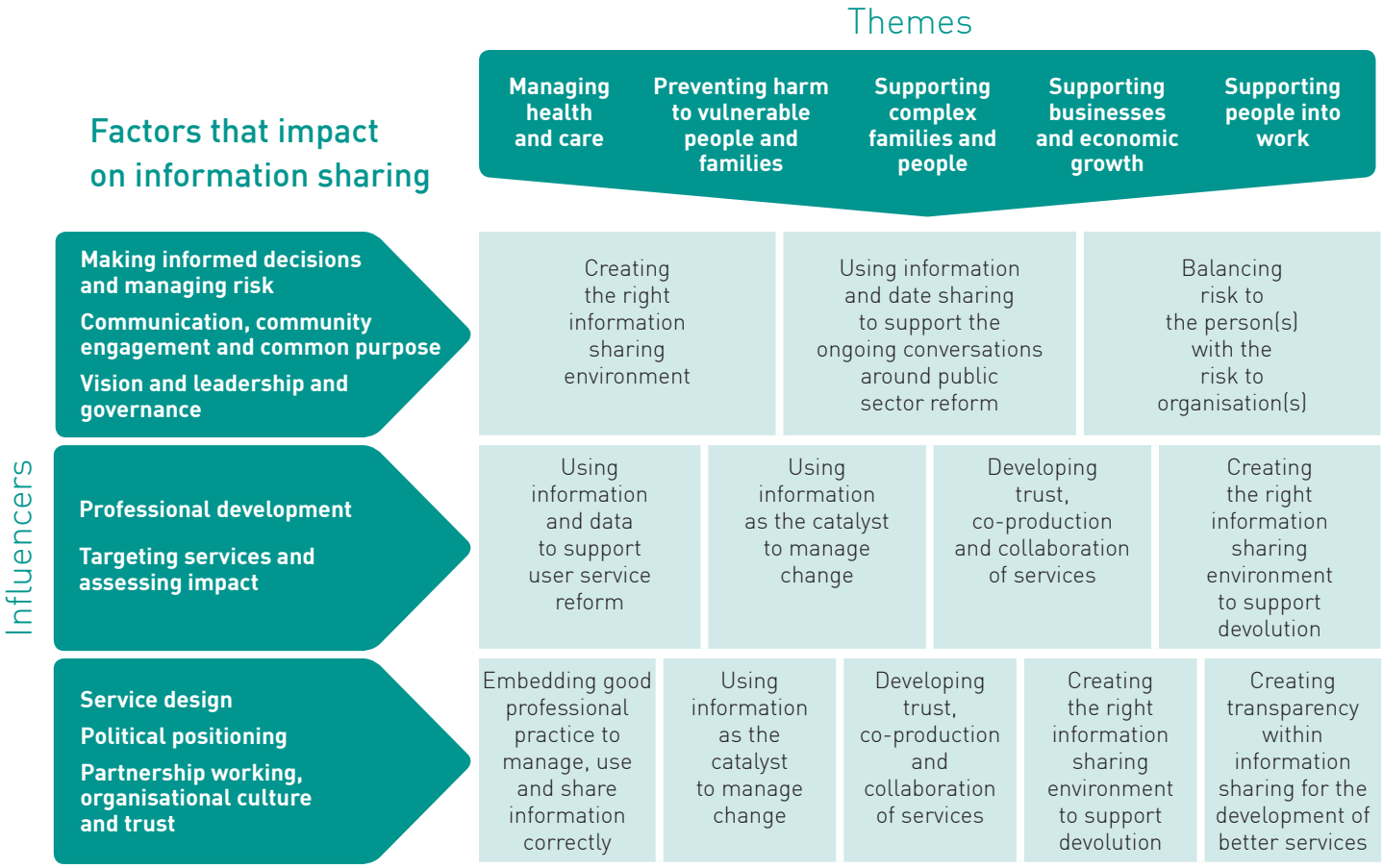
Within organisations and partnerships there can be a lack of understanding about how these two legal considerations can enable and support information sharing, combined with existing cultures of protecting information, this can create a misinformed perception that information may or should not be shared. Individual members of staff are also often strongly influenced by their own ethical views. The view of what is ethically acceptable evolves over time and the second Caldicott Review[8] - Information, to share or not to share 2013, considered ethical as well as legal aspects of information sharing. This included looking at the consequences of not sharing information.

The review affirmed the validity of the existing six Caldicott Principles but also recommended the introduction of a new seventh Caldicott Principle: "The duty to share information can be as important as the duty to protect patient confidentiality". There is sometimes a lack of clarity about what information should, or may be shared and this lack of confidence is a barrier to legitimate information sharing. Although the Common Law Duty of Confidentiality remains important, it needs to be recognised that there is also a duty of care and the underlying importance of 'trust' must also be protected. Cultural issues discussed within the case studies highlight:

[6] The Common Law of Confidentiality - www.health-ni.gov.uk/articles/common-law-duty-confidentiality

[7] Data Protection Act 1998 - www.legislation.gov.uk/ukpga/1998/29/contents

[8] Second Caldicott review - www.gov.uk/government/publications/the-information-governance-review



Managing informed decisions and managing risk

Information sharing plays a pivotal role for partnerships and organisations to better manage risk. Risk within information sharing comes in three main categories:

1. Risk to service users
   The misuse of personal data or untimely sharing of data can in some cases have catastrophic outcomes.
2. Organisational risk
   There is reputational risk to organisations who misuse data or personal information or who fail to share information and data in a timely, lawful way. There is also a financial risk to organisations through misuse or improper use of the data.
3. Practitioner risk
   Practitioners are often acutely aware of the risks around sharing information. This creates risk aversity and will often be a barrier to effective working for the client and in serious cases have severe consequences for clients and adverse effects to them personally.

Communication, community engagement and common purpose

The importance of effective communication is of paramount importance for information sharing. Creating a space to communicate aims and objectives of sharing information creates a collective understanding and leads to the creation of a shared language for information sharing. Understanding the 'why', 'how' and 'what' information is shared also supports positive engagement with other organisations and can be used in the engagement with service user groups within a partnership to foster trust and further understanding; as emphasised in Caldicott Three, in which it is recommended that citizens can make informed choices, by providing simple consent models.

Vision, leadership and governance

A strong vision for transformational change is vitally important to communicating about and sharing information and data. In turn this supports informed leadership. This collaborative way of working and shared governance can create the momentum for developing new, and innovative information sharing processes and therefore improving services. Providing a catalyst for public sector reform.

Professional development

It is important to ensure the professional development of practitioners and management teams to support a mutual understanding of sharing information, this organisational understanding supports the development of a responsible 'culture to share'. It ensures; better understanding of governance, the importance of conversations with service users and the use of informed consent and confidentiality. A mature organisational development of a thriving information sharing culture will ensure that confidence and trust are built with partner organisations and agencies, which will directly lead to better outcomes for people.

Targeting services and assessing impact

Supporting service reform requires a cultural shift to help service providers to understand and articulate what information they need and the purpose it is needed for. Targeting services to support better delivery outcomes identifies at which level services require change, how that service understands the outcomes they desire or require and how they analyse, assess and monitor those changes to show impact for the service user, professionals delivering those services across organisations.

Service design

The process of good service design engages with its service users and reflects on their experience and needs to refine, improve, or re-imagine what is delivered, and this relies on the availability of information and data. However, often the process or framework for information sharing is considered too late and becomes a barrier to making progress. Starting a conversation about information sharing at the beginning of the service design process helps build confidence in partnerships, improve awareness in the customers role, and provides a mechanism for change, that encourages greater transparency and accountability in the new service.

Political positioning

To future proof, high quality, sustainable services it is important to consider the political landscape in which a partnership functions. Partners may be working towards different end-goals (in the short and long-term), so their agenda's might differ, as well as the way in which they organise and deliver services. It is therefore important for partnerships to acknowledge and understand the changes they are working towards with this in mind, so they can overcome political-organisational barriers to information sharing.

Partnership working, organisational culture and trust

Through the development of joint information processes and protocols information sharing offers; improved partnership relations, the creation of joint information sharing training provision, collaborative thinking and can be the foundation for improved partnership working. Information sharing can be the foundations for public service reform and support the long-term aspirations of partnerships.

The barriers and enablers to information sharing

The case studies in this publication illustrate that outcomes can be transformed when organisations and partnerships start to recognise the cultural barriers and enablers to information sharing. Recognising these barriers and enablers allows individuals and organisations to understand and develop ways of working and supports the introduction of new working practices to overcome them. This can in turn lead to better use of the data. These new working arrangements can provide robust assurance, both to the organisations concerned, as they are better able to understand requirement and to the public, through transparent governance processes and supported communication and interaction.

Cultural issues discussed within the case studies highlight:

- how strong vision, informed leadership and collaborative governance can create the momentum for developing new information sharing processes and a culture for improving services;
- the importance of effective communication and engagement with service user groups within a partnership to foster trust;
- that professional development of practitioners and management teams can gain a common understanding of sharing information;
- how partnerships and organisations are better able to manage the risk to their service users through information sharing; and
- that the development of joint information, including joint training provision, can be a foundation for improved partnership working.

The case studies illustrate that outcomes can be transformed when organisations and partnerships start to recognise the barriers and introduce new working practices to overcome them. These new working arrangements need to be able to provide robust assurance, both to the organisations concerned and to the public through transparent governance processes.

Key information strands

Between health services and the Police there are three main categories of information sharing:

1. Proactive: The exchange of specific information about an Individual/person that is used in multi-agency arenas to plan support - for example work around troubled families.
2. Reactive: The exchange of information about an individual in response to an incident when they present with immediate needs - for example potential suicide or missing person.
3. Anonymised data from which an individual cannot be identified: A controlled exchange for explicit purpose - for example analysing trends/patterns and areas of need and to aid with service design and commissioning such as the prevalence of drug misuse.

This document focuses on "proactive" and "reactive" information sharing and does not cover information sharing of anonymised data from which an individual can be identified.

The General Data Protection Regulations

The General Data Protection Regulation (GDPR) is a regulation introduced by the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).

From 25 May 2018 the GDPR will replace the DPA meaning that all companies which are currently governed by the act will need to update their processes to ensure they remain compliant with the new, tougher legislation.

The introduction of new legislation can cause lots of concern and confusion, which can in turn limit information sharing, or programmes seeking to develop data sharing. The changes which the GDPR bring, are predominately about firming up data management practices (i.e. recording things more and bettering how you record them, improving the content of your privacy notices, and the way you ask people for consent), rather than a total overhaul of your systems and processes.

The purpose of Police sharing information

Information sharing is a vital element of policing and protecting the public. Police forces across England are looking to work more collaboratively with health services and other public and private sector organisations to improve the delivery of services. Such sharing is essential for early intervention and preventative work, for safeguarding and promoting welfare and for public protection.

The sharing of information between the Police and other organisations, still has to have a legal basis, respecting, the Common Law Duty of Confidentiality and complying with the DPA[9] and all other legislation. Sharing Police information also has to satisfy a policing purpose. These purposes are presented in the management of police information (MoPI) code of practice and listed[10] as:

- protection of life and property;
- preservation of order;
- prevention and detection of offences;
- bringing offenders to justice; and
- any duty or responsibility arising from common or statute law.

Please see further details at www.app.college.police.uk/management-of-police-information

Many of the initiatives in the case studies are focused on the protection of life. In this context not sharing information may have a significant negative impact for the individual. Professionals recognise the importance of maintaining the trust of service users and patients as well as their legal obligations in relation to confidentiality. In those cases, where it may not be possible to follow the wishes of patients and service users, there should normally still be an explanation of how and why the information has been shared – for example a legal requirement to share information in relation to child safeguarding under the provisions of the Children's Act.[11]

The purpose of health sharing information

Health services are committed to working jointly with Police and other local authority services, public sector and a wide range of private and voluntary sector organisations to deliver improvements in health and wellbeing. Commissioning partnerships agree local priorities which include improvement to emergency care and better management of chronic illness. The case studies in this resource show how cost effective funding enables the improvement of information sharing, which directly leads to improvements in direct care and financial efficiency.

[9] Data Protection Act 1998 - www.legislation.gov.uk/ukpga/1998/29/contents

[10] Management of police information cade of practice - http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf

[11] Children's Act 2014 - www.legislation.gov.uk/ukpga/2004/31

How Police and health services share information

Both the Police and the health services use a structured approach to information sharing within a compliance framework - key components of this framework include:

- ensuring patients and service users are informed about how their information is held and shared. This needs to be done in a way that can be understood by the individual and include the opportunity to contact someone if they have further questions. Simply making such "privacy notices" available is not enough, all patients and service users should know and understand how their information is used. There should never be any surprises! The use of "privacy notices", usually in the form of a statement on the organisations web page, with posters and leaflets being available may not be effective in communicating to all.

  It is important that the information produced should be in a format that communicates with the individual patient, it should not be assumed that all patients speak English or will be familiar with the type of words frequently used by those working in information governance or found in the DPA. For the NHS, privacy notices[12] are the responsibilities of each care organisation and for the Police; these are typically managed at force level.

- for partnership innovations a consultation process is often completed;
- registration and compliance with the DPA including clarity on the legal basis for processing and sharing personal and sensitive information of individuals;
- for the NHS, Subject Access Requests (SARs)[13] and Freedom of Information (FOI)[14] obligations are met by each provider organisation. For the Police, SAR and FOI services are provided by each force and there is also a central referral unit based within the National Police Chief Council[15] to ensure a consistent approach to all requests across the Police service;
- training of staff in the importance of balancing the need to respect confidentiality with information sharing and security;
- how to effectively use the information tools provided to best effect;
- security of information systems and access control; and
- accountability for the correct handling of personal and sensitive information for both Police and health services rests on NHS providers and Police organisations and also on individual health care professionals and police officers.

In terms of innovative information sharing, this framework includes:

- undertaking a Privacy Impact Assessment (PIA)[16] to understand the prospective information flows, technologies and the associated risks to identify the controls required;
- privacy notices to be edited to reflect changes to sharing information for service users and patients;
- use of secure channels and systems for communication; and
- an Information Sharing Agreement (ISA)[17] which summarises the purpose and legal basis for sharing, what is shared and how it is managed between the partners.

To ensure there is a legal basis for sharing, the DPA and the Common Law Duty of Confidentiality must be satisfied. For such innovations, ISA cover the detail of how requirements of the DPA schedules two and three are met. There are also other legal gateways that, although not central to the case studies, may occasionally be relevant - see page 11 for information sharing section.

[12] Privacy notices - https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

[13] Subject access requests - https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/

[14] Freedom of Information act - www.legislation.gov.uk/ukpga/2000/36/contents

[15] National Police Chief Council - www.npcc.police.uk/

[16] Privacy Impact Assessment - https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

[17] Information sharing agreement - https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

The General Data Protection Regulations

The GDPR acknowledges that technology has revolutionised both the extent to, and way in which data has transformed the economy and people's private lives. The GDPR, in response to this offers 'greater transparency, enhanced rights for citizens and increased accountability. The United Kingdom will be adopting the GDPR from the Council of the European Union and European Commission, and from 25 May 2018 the GDPR will replace the Data Protection Act (1998).

The introduction of this new legislation has the potential to cause concern, confusion, and misconception resulting in nervousness amongst professionals around communicating about information and data sharing.

Many organisations are gearing up to implement the requirements of the GDPR. And we have a new Data Protection Bill on the horizon. In the context of all this change, it is all the more important that we communicate more about why information sharing is important. We should consider how we engage with our people and communities about why we need to share information and data, and place this firmly at the heart of improved and transformed services.

Legal annex

Most statute law is written in language that can be difficult for many people to understand. Statute law starts life as a written "bill" before being debated by both the House of Commons and the House of Lords. When the bill has been approved it becomes an "Act" of Parliament and a "Statute". In addition to statute law there is common law, which has developed in many situations over centuries, it is not written down in one document but individual cases may come to court and establish a legal "precedence", or "case law". It may be necessary in some situations to comply with several pieces of legislation or common law, and legal opinion may need to be sought as to which piece may be considered to have "precedence" (e.g The Children's Act usually has precedence over the Common Law Duty of Confidentiality).

The law does not provide a barrier to legitimate information sharing but it is important to establish what the legal basis is for any information sharing. A PIA should be conducted before any information sharing takes place to look at what the purposes are of any proposed information sharing, what the legal basis is and what potential objections or challenges there might be. It is likely to involve the participation of key stakeholders which may include other agencies, organisations or individuals, it may also include the representatives of patient or service user groups. Although the prospect of conducting a PIA may seem onerous; it will provide assurance of the legal and ethical basis for the proposal, and is time very well spent! If a complaint is made about the legality of sharing information it may go to court, and legal argument will ensue. The two opposing legal teams will try and persuade the jury or judge of the validity of their view as to how statute or common law should be interpreted. This adversarial process will result in a judgement being made in the specific case which may then also be applied in other similar cases.

The following legal basis gives a flavor of some of the major legal considerations:

For the purpose of clarity, information sharing is the disclosure of information from one or more organisations to a third party organisation(s). In this context it may include the processing of information either on a one-off or an on-going basis between partners for the purpose of achieving a common or joint aim.

Legal basis for information sharing

This information will be reviewed from May 2018 in line with GDPR. For more information about the new regulations, please see the previous page.

The DPA makes provision for the regulation of the processing of information relating to individuals, including; obtaining, holding, use or disclosure of such information. For all case studies the legal basis for information sharing will be covered by the following:

1. **DPA schedule two**
   This is satisfied as the sharing that is necessary to comply with the common law duty of care and to enable the exercise of police and health services functions to act in the public interest. In exceptional circumstances the vital interests of the individual or the administration of justice may also apply. When processing personal data, the DPA requires that at least one of the conditions for processing in schedule two is met, and that where the processing includes sensitive personal data, at least one of the schedule three conditions is also met. For all case studies at least one of the following conditions for processing are relevant:
   - to comply with a legal obligation, e.g. common law duty of care;
   - to protect the vital interests of the individual concerned (must be risk of death or serious harm);
   - for the administration of justice;
   - to discharge a function imposed by statute; and
   - to enable the exercise of a function of a public nature exercised in the public interest.
2. **DPA schedule three**
   This is satisfied as the sharing by both parties supporting a medical purpose. In exceptional cases the vital interests[18] of individuals or the administration of justice may also apply. The points below are needed to satisfy the schedule:
   - to protect the vital interests of any individual where obtaining consent is difficult or cannot be obtained; or
   - for the administration of justice; or
   - for medical purposes – a broad category including all aspects of managing and delivering care and treatment, including social care – where those involved have a strict duty of confidentiality.
3. **The common law duty of confidentiality**
   This satisfied because the public interest in sharing is sufficient to support the limited information sharing involved. Any further sharing within health services, e.g. to support a referral, is subject to normal NHS information sharing practice. The common law duty of confidentiality will be satisfied when information is shared:
   - where there is a clear statutory obligation to share confidential information; or
   - with the consent of the individual concerned; or
   - where it is in the best interests of an individual who lacks the capacity to consent to the sharing; or
   - where the public interest served by sharing the minimum information needed to satisfy a purpose outweighs both the duty of confidentiality owed to an individual and the public interest in services being seen to be provided on a confidential basis.

In addition there are a number of legal gateways that enable sharing of information.

Court orders

These include coroners' investigations (Coroners and Justice Act 2009).

Safeguarding

Information must be shared for child or vulnerable adult safeguarding purposes (e.g. s.47 Children Act 1989).[20]

[18] Vital interest in DPA 1998

(a) in order to protect the vital interests of the data subject or another person, in a case where -

(i) consent cannot be given by or on behalf of the data subject, or

(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

[20] Children's Act 1989 - www.legislation.gov.uk/ukpga/1989/41/contents

In addition, for the Police:

In addition, the police can sometimes rely on DPA 29(3) or 35(2). In this context the DPA allows but does not compel sharing where the specified criteria are met.

DPA Section 29(3)

Crime and taxation - personal data processed for any of the following purposes:

- the prevention and detection of crime;
- the apprehension or prosecution of offenders; and
- the assessment or collection of any tax or duty or of any imposition of a similar nature.

DPA Section 35(2)

Disclosures required by law or made in connection with legal proceedings:

- personal data is exempt from the non-disclosure provisions where the disclosure is required by or under any enactment, by any rule of law or by the order of a court; and
- personal data is exempt from the non-disclosure provisions where the disclosure is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings).

For the purpose of obtaining legal advice, or is otherwise necessary) for the establishing, exercising or defending legal rights. Also the following can be relevant:

- Civil Evidence Act 1995[20];
- Crime and Disorder Act 1998[21];
- Police Reform Act 2002[22]; and
- Rehabilitation of Offenders Act 1974[23].

[20] Civil Evidence Act 1995 - www.legislation.gov.uk/ukpga/1995/38/contents

[21] Crime and Disorder Act 1998 - www.legislation.gov.uk/ukpga/1998/37/contents

[22] Police Reform Act 2002 - www.legislation.gov.uk/ukpga/2002/30/contents

[23] Rehabilitation of Offenders Act 1974 - www.legislation.gov.uk/ukpga/1974/53

[24] Prevention of Terrorism Act 1989 - www.legislation.gov.uk/ukpga/1989/4/contents

[25] Road Traffic Act 1988 - www.legislation.gov.uk/ukpga/1988/52/contents

[26] Female Genital Mutilation Act 2003 - www.legislation.gov.uk/ukpga/2003/31/contents

[27] Care Quality Commission - www.cqc.org.uk/

[28] Health and Social Care Act 2008 - www.legislation.gov.uk/ukpga/2008/14/contents

[29] Health and Social Care Act 2012 - www.legislation.gov.uk/ukpga/2012/7/contents/enacted

[30] Control of Disease Act 1984 - www.legislation.gov.uk/ukpga/1984/22/section/46

[31] Health Protection Regulations 2010 - http://legislation.data.gov.uk/uksi/2010/657/made/data.htm?wrap=true

In addition, for the NHS:

- Prevention of Terrorism Act (1989)[24] and Terrorism Act (2000). NHS staff must inform the Police if they have information that may assist them in preventing an act of terrorism, or help in apprehending or prosecuting a terrorist;
- Road Traffic Act (1988)[25]. There is a statutory duty to inform the Police, when asked, of any information that might identify any driver who is alleged to have committed an offence under the Act. NHS staff are not required to disclose clinical or other confidential information;
- Female Genital Mutilation Act (2003)[26]. Staff have a statutory duty to report to the police under section 5B of this act where it appears that a girl under the age of 18 has been subject to genital mutilation;
- Care Quality Commission[27], which has powers of inspection and entry to require documents, information and records – a code of practice sets out how the CQC can use these powers (Health and Social Care Act 2008[28];
- Health and Social Care Information Centre, the statutory safe haven, which has powers to collect information when directed by the Secretary of State or NHS England (Health and Social Care Act 2012)[29]; and
- health professionals must report notifiable diseases, including food poisoning (The Public Health (Control of Disease Act 1984) and the Health Protection (notification) Regulations 2010)[30].

The NHS uses a common reference number, the NHS number, across all care delivery organisations for patient safety reasons. The expectation is that this number is not held routinely on Police information systems. However, in the context of an episode of emergency care, it may be used to support identification. This framework may appear complicated. To help, questions are presented in the conclusion of this document to support local partnership think through new ways of sharing information - things to consider when sharing information on page 35.

A separate guide is available for disclosure of personal information to Police for purposes other than care and is available from the IGA website (www.systems.digital.nhs.uk/infogov/iga[31]).

The Caldicott Principles

In 1997, following concerns about how patients' information was being used in the NHS, a committee was established under the chairmanship of Dame Fiona Caldicott to investigate. In the resulting report six Caldicott Principles were identified and the "advisory" role of Caldicott Guardians was established. A further review followed in 2012 and a "sharing" principle was added. All seven principles were republished in 2016 in the National Data Guardian for Health and Care Review of Data Security Consent and Opt Outs. Caldicott Principles are widely recognised as providing an acceptable ethical basis for the use of patient and service user information but do not themselves provide a legal basis for sharing.

CP1 Justify the purpose(s)

Every proposed use or transfer of personal-confidential data within or from an organisation should be clearly defined, scrutinised and documented with continuing uses regularly reviewed, by an appropriate guardian.

CP2 Don't use personable identifiable information unless it is absolutely necessary

Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

CP3 Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a function to be carried out.

CP4 Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

CP5 Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff are made fully aware of their responsibilities and obligations to respect patient confidentiality.

CP6 Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

CP7 The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

In the case studies later in this resource, a note is given against each of the Caldicott Principles to summarise the approach taken. If you have any questions about any principles highlighted in the case studies, please use the contact details below:

- On cultural issues to sharing information contact the Centre of Excellence for Information Sharing at: Info@informationsharing.org.uk

If you would like to contact any of the case study teams directly you will find the contact details at the end of the individual case studies.

Data sharing between the Police and health services for care purposes

Case Study

The Leicestershire triage car: reducing the number of people detained under section 136

CP1 CP2 CP3 CP4 CP5 CP6 CP7

Caldicott Principles covered

The example within this case study is governed by the Data Protection Act (1998) but will be updated from May 2018 to reference any changes made to comply with the introduction of the General Data Protection Regulation (GDPR).

Overview

Local statistics for Leicestershire showed a high number of people in mental health crisis being detained by the Police under Section 136 of the Mental Health Act because of insufficient access to the support they needed.

Leicestershire Police felt their officers' time was being taken up at the accident and emergency department, getting mental health assessments and that the lack of understanding between the services and ways that they shared information was having a negative impact on the people they were trying to support.

View at www.informationsharing.org.uk/healthandpolice

The solution was a combined initiative, between Leicestershire Police and Leicestershire Partnership NHS trust mental health crisis services. The approach enabled mental health practitioners access to individuals at their first point of contact with the Police, to assess if their situation was due to poor mental health and determine the most appropriate treatment. Since being developed, this process has become business as usual for the police and health commissioners from the local clinical commissioning groups (CCGs).

The Leicestershire approach

At the Euston Street custody suite, in Leicester, a police officer and mental health nurse are co-located and operate alongside the liaison and diversion service. This gives opportunities for police officers responding to a callout to receive information and advice through the mental health triage nurse who has access to the trust's electronic patient record. If the individual has engaged with mental health services previously, or has a current mental health care plan in place, the nurse is able to discuss relevant information and work with the police officer to ensure a better outcome. The approach also allows for mobile assessment - police officers and triage nurses attend incidents, making assessments and referrals based upon the immediate needs of the individual. The nurse, following an assessment of the person's mental health, can arrange for hospital admission, refer to the mental health crisis team or pass care back to the GP or community health team.

Relationships between Police and mental health workers have developed through the approach into a trusting and informed working partnership. This allows for advice and expertise to be shared and further meantal health training given to the Police. This has led to preparation of more informed assessments and more options for alternative care pathways, as well as lowering the risk for all involved.

Why is information sharing necessary?

By sharing information during a live situation, there are better outcomes for vulnerable people as a consequence of better informed decision making. The approach has also allowed for better partnership understanding and has led to further opportunities within this field.

What does this mean for vulnerable people?

Vulnerable people gain access to the right support in the right place, quickly. This means that there is a reduced chance of them spending time in a cell unnecessarily waiting to be assessed and possibly detained under a section 136.

How is information shared?

Information is shared through discussion between the police officer and mental health triage nurse. They are able to communicate with their own organisations and share relevant information with partner organisation as necessary. This builds up the specialist knowledge of team members and improves practice and positively affects the culture of both organisations to share information. There is no physical exchange of data and the Police are given only contextual clinical information necessary to understand risk and how a person may present. The mental health nurse has no access to Police records but again are given contextual information based on risk.

Information sharing barriers and how they were overcome

- a lack of understanding for the organisational cultures towards information sharing by both organisations; and
- a non-service user centred approach to information sharing.

These barriers were overcome by:

- strong and consistent leadership to co-locate police officers with a mental health triage nurse; and
- better understanding of other organisations' views on information sharing and provision of training.

Management of consent

Consent to share is dictated by the circumstance and seriousness of the incident. Where explicit consent is appropriate it is sought. In situations where there is a specific safety risk or it is impossible to seek consent, a judgement is made by the police officer and mental health nurse. In the absence of explicit consent, the nurse will need to judge the current capacity of the patient or service user to make decisions and act in their best interests where they lack this capacity. If the patient or service user is capable of making decisions but will not consent, then the nurse will need to determine whether the public good that would be provided by sharing proportional information outweighs the individual's right to confidentiality.

By following the Caldicott Principles and ensuring information sharing is necessary, proportionate, relevant, adequate, accurate, timely and secure - correct information sharing occurs.

What are the benefits of information sharing?

Health services

- practitioners are able to deal with more mental health crisis situations at an earlier stage to prevent hospital admissions;
- it reduces the number of patients being held inappropriately in police custody awaiting assessments; and
- it has reduced the amount of doctors' time needed, as there is less need for such assessments.

Police

- officers are no longer required to spend time waiting for vulnerable people to be assessed which removes them from other duties for considerable lengths of time; and
- police officers have access to advice and information from a mental health practitioner in order to support how they manage vulnerable people at the scene.

Joint benefits

- over a three-year period the number of people detained under the section 136 of the Mental Health Act[32] has reduced by around 80%; this indicates more appropriate outcomes have been achieved for people who are in crisis;
- in 2016, with a small increase in mental health related contacts, less than four people are detained by the police per month;
- an estimated reduction of 554 hours per week for officers spent involved with mental health related incidents; and
- both organisations have seen positive cultural change through joint working. Staff surveys of Leicestershire Police reveal an overwhelmingly positive support for the approach.

[32] Section 136 of the Mental Health Act - www.legislation.gov.uk/ukpga/1983/20/section/136

Governance of the work

The scheme is managed through a partnership between Leicestershire Police and the Leicestershire Partnership NHS Trust. An ISA supports detailed procedures and staff training. Outcomes are audited which enables the partnership to monitor performance.

Cultural issues affecting information sharing

Embedding information sharing across partnerships invariably highlights a number of cultural issues between organisations which need to be addressed. The main issue here was to enable practitioners to feel confident in sharing information. This was achieved through co-location, training and also strong governance. This approach has subsequently been adopted in other areas of England.

How the Caldicott Principles are applied in this case study

CP1 Justify the purpose(s)

Police are able to share with nurses in the triage team for purposes of early intervention, prevention and safeguarding and for the care of the individual. These arrangements are set out in the ISA between Leicestershire Police and Leicestershire Partnership NHS Trust.

CP2 Don't use personable identifiable information unless it is absolutely necessary

Service users are identified to see if they are known to either Police or the mental health team. The necessity to share information further is governed by the situation and the individual.

CP3 Use the minimum necessary personal confidential data

Sharing of information is based on the situation, the risks to the individual(s) and following advice from any existing mental health care plan or/and possible restrictions put in place by the criminal justice system; for example, bail conditions.

CP4 Access to personal confidential data should be on a strict need-to-know basis

As neither organisation can access the other's records all information is shared on a 'need to know' basis by each member of the team.

CP5 Everyone with access to personal confidential data should be aware of their responsibilities

Both police officers and mental health triage nurses are trained in the standing operating procedures which are based on the ISA.

CP6 Comply with the law

The team is aware that they are sharing highly confidential information. Depending on the situation, it could be of high or low importance to disclose information as there may or may not be a significant risk of harm to an individual(s). There is team training in the procedures based on the ISA and legal gateways.

CP7 The duty to share information can be as important as the duty to protect patient confidentiality

The sharing of information in appropriate ways is essential to the function of the triage team as they support individuals in crisis. For the professionals involved, an understanding of their duty of care to the individual enables them to decide whether, when and how to share.

Good practice

This case study is of a joint triage team of Police and mental health nurses set up to respond to the immediate needs of individuals in crisis. Good practice is illustrated in terms of:

- providing the best possible care to people in crisis as soon as practical;
- the triage team allows Police to share information for the purposes of early intervention, prevention and safeguarding and for nurses to share for care on the basis of consent, if there is a care plan, or best interests if the individual lacks capacity and otherwise on the basis of public interest; and
- privacy notices of both Police and health service organisations state how information is held and shared and an ISA summarises the arrangement.

If you have further questions on this case study, please contact:

Peter Jackson

Project Manager, Criminal Justice Liaison & Diversion, Leicestershire Partnership NHS Trust

Johnpeter.jackson@leicspart.nhs.uk

If you have found this resource useful and are planning to start work on improve information sharing between health and Police in your area, please let us know so we can track the impact of this work by emailing info@informationsharing.org.uk

Data sharing between the Police and health services for care purposes

Case Study

The Margate Task Force 999 frequent callers

CP1 CP2 CP3 CP4 CP5 CP6 CP7

Caldicott principles covered

The example within this case study is governed by the Data Protection Act (1998) but will be updated from May 2018 to reference any changes made to comply with the introduction of the General Data Protection Regulation (GDPR).

Overview

The Margate Task Force is a multi-disciplinary, co-located team working with local people to improve lives by tackling health and social issues. Focussing on the most deprived wards in Thanet, the team is made up of professionals from the Police, Community Safety, Fire, Health, Department for Work and Pensions (DWP), Early Help, Troubled Families and Housing. These wards have high caseloads for a number of these teams and engagement at street level has identified mental health as a priority.

View at www.informationsharing.org.uk/healthandpolice

In 2013 the Police, Turning Point (commissioned drug/alcohol treatment providers) and South East Coast Ambulance Service (SECAMB),[33] identified a number of frequent callers (five calls or more in a month to 999 or 101 services). These callers were effecting service delivery and draining resources. The majority were known to mental health services.

At the same time, relationships between mental health teams and the Police were poor due to a clash of organisational cultures. Police officers identified that they were ill equipped to deal with these individuals because there was little access to advice or to mental health triage workers. This resulted in vulnerable people being inappropriately detained in Police custody or not being referred.

In a pilot, details of a number of frequent callers were passed to the adult mental health team. If callers were a known patient, appropriate information from the care plan was shared with the Police and the patient's care co-ordinator was informed and:

1. a joint visit was made to the caller, led by their care co-ordinator.
2. the care plan for the patient was reviewed and additional support from other agencies was offered; reducing calls to emergency services was added to the objectives of the care plan.

If the caller was not a patient:

3. the adult mental health nurse visited with a police officer to discuss the reasons for the frequency of calls.
4. the services available through the Margate Task Force were offered to the individual.

Many of the callers were suffering from substance misuse, dementia and/or poor mental health. Providing appropriate packages of care proved effective in reducing the number of subsequent calls to emergency services. As a result, this approach became "business as usual" for the task force.

[33] South East Coast Ambulance Service - www.secamb.nhs.uk/

Why is information sharing necessary?

Information sharing allows better support for someone who is reaching crisis point. The task force is able to develop care packages through a holistic understanding of needs of the individual. With early identification and then assessment, people suffering with poor mental health are less likely to get to crisis point. Such intervention reduces the number of people detained under the Mental Health Act.

What does this mean for vulnerable people?

It means vulnerable people are able to access appropriate services and wider social care issues can be addressed through the multi-agency partnership.

How is the information shared?

A list of names and dates of birth of frequent callers are compiled monthly by Police and by ambulance call-handling teams. These lists are shared with the adult mental health worker to see if any of the callers are an existing patient and has a case worker.

Information concerning callers is recorded separately by each organisation; no detailed clinical information is recorded by the Police. Similarly, police information is not recorded on the clinical care record. However, if the caller is thought to pose a risk to staff then a warning marker is created on both Police and ambulance call-handling systems.

Information sharing barriers and how they were overcome

There were significant cultural barriers between the Police and the mental health crisis team, which prevented them from discussing cases effectively; these included:

- mistrust between the two services and also between practitioners;
- no understanding of joint working and resource pressures; and
- both services working at cross purposes, without a shared language.

These were addressed by:

- the creation of the Margate Task Force which is co-located and has shared objectives and procedures;
- developing a shared language through the work of an embedded adult mental health worker. This role is a conduit for the task force into the wider mental health team and other services;
- understanding of mutual organisational roles and responsibility at every level, helped by the shared experience of working with service users; and
- the creation of a partnership ISA and procedures for the task force.

Management of consent

There is clear evidence that repeated high levels of 999 and 101 calls by an individual is an indication of a need for care. Initial sharing of a list of frequent callers by the Police and also the ambulance service is on the basis of public interest. Once it is established that the frequent caller is an existing mental health patient, their case manager approaches them. If the callers are not known, a home visit is made by a police officer and a mental health nurse to offer help. Should the person agree to proceed, consent is sought as the basis for information sharing between the care agencies to develop a care package.

What are the benefits of information Sharing

Health services

- identification of frequent 999 and 101 callers to allow prevention strategies to be developed;
- assessment of frequent callers who can benefit from drug or alcohol related support; and
- fewer call outs for SECAMB.

Police

- fewer people inappropriately processed through the criminal justice system; and
- information on crimes committed against vulnerable people; this has led to arrests and other community issues resulting in referrals to other services within the task force.

Joint benefits

- less drain on emergency services both financially and also time spent;
- better access to local services for vulnerable people;
- a reduction in stress and anxiety for the frequent caller, and improved care plans;
- police officers and adult mental health crisis workers are able to draw on each other's experience and knowledge; and
- police officers are now better able to support people in difficulty.

Governance of the work

Kent and Medway partnership provides governance for the task force and there is an ISA for partnership and safeguarding. All staff are Police vetted and act as the designated officer (DOs) for their data. The two joint lead officers from the Police and Kent Fire and Rescue Service perform the function within the integrated services environment of primary designated officers (PDOs).

Cultural issues affecting information sharing

In Margate the formation of a co-located task force was crucial to tackling cultural factors. Strong leadership from the agencies meant clear outcomes were established within a clear governance structure. Joint working has allowed for the development of a high level of trust, shared understanding and awareness. Strong and balanced leadership and communication of a shared vision has enabled the task force to improve services and outcomes for service users.

How the Caldicott Principles are applied in this case study

CP1 Justify the purpose(s)

The purpose of sharing information is to provide appropriate care package to vulnerable, repeat callers to 999 or 101 service. For identification, the purpose for sharing information for the Police is early intervention, prevention and safeguarding and for the ambulance service, public interest.

CP2 Don't use personable identifiable information unless it is absolutely necessary

Great care is taken to ensure identification of frequent callers is systematic and justifiable.

CP3 Use the minimum necessary personal confidential data

The minimum of information is shared to enable accurate identification and to check if there is already a care package in place.

CP4 Access to personal confidential data should be on a strict need-to-know basis

Initial sharing is restricted to police officers and the mental health team, but information is not shared with the wider task force unless consent is agreed with the person.

CP5 Everyone with access to personal confidential data should be aware of their responsibilities

Staff are made aware of their responsibilities through training. The partnership and each care agency is led by professionals with codes of practice and personal accountability.

CP6 Comply with the law

An ISA is in place between the partnership agencies that defines the purpose for sharing information, legal gateways used and secure channels of communication with procedures and staff training in place to reflect this arrangement.

CP7 The duty to share information can be as important as the duty to protect patient confidentiality

The focus is accurate identification of frequent callers to allow care agencies to develop appropriate care packages for these vulnerable people.

Good practice

This case studies illustrates good practice from a local initiative between care agencies to help vulnerable people who repeatedly call emergency services:

- frequent 999 and 101 callers are identified for purposes of early intervention, prevention and safeguarding by the Police, and on the basis of public interest by the Police and ambulance service; the assumption is that these individuals are vulnerable and in need of help;
- if the callers are existing mental health patients, their care co-ordinator visits and develops a new package of care for them through a collaborative approach with local care agencies;
- if the callers are not known, a home visit is made by a police officer and a mental health nurse to ask them about their personal situation and to offer the chance of help; and
- privacy notices of both Police and health service organisations state how information is held and shared and an ISA summarises the arrangement.

If you have further questions on this case study, please contact:

Margate Task Force

MargateTaskForce@Thanet.gov.uk

If you have found this resource useful and are planning to start work on improve information sharing between health and Police in your area, please let us know so we can track the impact of this work by emailing info@informationsharing.org.uk

Data sharing between the Police and health services for care purposes

Case Study

Norfolk Police: Mental health nurses in police call centre

CP1 CP2 CP3 CP4 CP5 CP6 CP7

Caldicott Principles covered

The example within this case study is governed by the Data Protection Act (1998) but will be updated from May 2018 to reference any changes made to comply with the introduction of the General Data Protection Regulation (GDPR).

Overview

A pioneering project to reduce the number of Section 136 of the Mental Health Act[34] interventions and detentions through improved information sharing has been running in Norfolk. The pilot is based on the introduction of mental health nurses into the Police Contact and Control Room (CCR) to help respond to calls involving mental health patients to ensure they receive an appropriate response.

View at www.informationsharing.org.uk/healthandpolice

The nurses, from the Norfolk and Suffolk Foundation Trust (NSFT)[35] have immediate access to databases to enable them to make 'on the spot' professional assessments. This could involve the use of alternative options rather than the attendance of a police officer.

This new approach has seen a significant reduction in the number of section 136 interventions carried out by police officers and also of section 136 detentions.

As Norfolk is a large rural area with a scattered population, a decision was made to invest in a shared approach to police call-handling rather than in more local integration (e.g. street triage). A team of four mental health nurses and a drug and alcohol dependency worker led by a senior nurse manager are located in the police CCR. To decide on the most appropriate response to a call, they are able to access a number of databases, including:

- trust patient systems for mental health and drug and alcohol abuse services;
- Norfolk and Suffolk social care applications (for members of the public with dementia and children in care); and
- police call-handling system.

A nurse is present between 8am and 10pm, Monday to Friday with weekend and bank holiday cover. They are able to refer patients to other agencies such as Social Care and Housing and also make follow up visits to patients with the Police.

Why is information sharing necessary?

In recent years there has been a reported increase in calls received by the Police concerning mental health patients. A member of the public, in health crisis benefits from appropriate and informed care and this should start with the call handling team. This means that members of the public can receive a better service from the Police and also, for mental health patient's, diversion from custody and early intervention.

What does this mean for vulnerable people?

A better experience for members of the public contacting the Police for health related emergencies. For patients with long term mental health issues, the right interventions at the right time by the right people (e.g. suicide prevention) with appropriate follow up to other care agencies (e.g. GPs, housing and social care).

[34] Section 136 of the Mental Health Act - www.legislation.gov.uk/ukpga/1983/20/section/136

[35] Norfolk and Suffolk Foundation Trust - www.nsft.nhs.uk

How is information shared?

Information is shared through direct discussion between police officers, their call-handling colleagues and the mental health nurses. Nurses have access to multiple care plans and records but only share the minimum from these to support decisions by the Police team. Events and decisions are recorded in the Police system. An operational guidance manual has been developed and there is training for Police as part of the initiative.

Information sharing barriers and how they were overcome

- relationships between the mental health trust and Police were poor, inconsistent and personality led; and
- systems and procedures were not connected so that key events for patients and outcomes were not shared (e.g. results of Police intervention on wards following assaults by patients on other patients or on staff).

These issues were addressed through:

- development of a joint bid for location of a team of mental health nurses with the police CCR team;
- mental health nurses in the CCR were enabled to access the trust, social care and police systems to allow sharing with the police. The police CCR team are able to discuss callers and events with the nurses;
- support for an improved understanding of the circumstances of individuals in health crisis though training of the police CCR team and other officers; and
- the initiative was underpinned with appropriate governance, an ISA and policies and procedures were put in place to ensure effective team working in the CCR.

Management of consent

A care plan is agreed with all mental health patients. This discussion includes a decision on what is to be shared with whom and in what circumstances (e.g. with Police, social services, GP) - when nurses share information from this care plan it is limited by this consent. In terms of social care and drug and alcohol teams, again, a care plan developed with consent is the basis for sharing. On occasions a best-interest or public-interest decision is made by the nurse to share information without consent. Whenever an event takes place and this information is shared, the patients mental health care coordinator or GP is briefed. No complaints have been received from patients concerning sharing of information at the date of publishing.

If the caller is not an existing patient with a care plan, this is relayed to the police officers on the spot and appropriate follow up is put in place with consent arrangements for new patients followed.

What are the benefits of information sharing?

Health services

- improvement of service provision for patients in crisis and fewer arrests. Earlier intervention and lower admissions and detentions under the Mental Health Act 1983 (Section 136)[36].

Police

- better experience of Police service by people in crisis;
- improved integration and collaborative working of Police with other care agencies; and
- provision of specialist training in mental health.

Joint benefits

- better case management for patients with long term conditions through access to services for people contacting the Police and, as a result, less use of Police/health service resource.

[36] Section 136 of the Mental Health Act - www.legislation.gov.uk/ukpga/1983/20/section/136

Governance of the work

A county-wide ISA is in place which sets out the information sharing arrangements of the partnership with an agreed procedure manual which underpins the joint CCR team.

Cultural issues affecting information sharing

Overcoming cultural issues is a key aspect of successful information sharing between organisations. The introduction of the mental health nurses in the CCR immediately challenged the traditional relationship and changed the model of delivery. Successful implementation is due to effective relationship building, joint understanding of role and co-design. This new team has developed a culture of collective responsibility.

How the Caldicott Principles are applied in this case study

CP1 Justify the purpose(s)

For the nursing team the purpose is provision of care and, for the Police call handling team, early intervention, prevention and safeguarding of vulnerable individuals.

CP2 Don't use personable identifiable information unless it is absolutely necessary

Identifying information is necessary for this service.

CP3 Use the minimum necessary personal confidential data

The emergency call team apply this principle and nurses search care systems to see if the caller is already known and has a care package.

CP4 Access to personal confidential data should be on a strict need-to-know basis

The nursing team can access the records of the NHS and social care providers with access granted by the relevant organisation. An audit trail is available if there is ever a question of whether access was inappropriate. For the nurses, sharing with Police and other agencies, is, for the most part verbal and limited to what helps in resolution of the crisis, there have been no complaints from callers at the time of publishing.

CP5 Everyone with access to personal confidential data should be aware of their responsibilities

Only the nursing team, as registered health care professionals, can access records of care. Training is delivered by the care provider before access is enabled and the nursing team also provides training to the wider police force on mental health and management of health crises.

CP6 Comply with the law

The partnership has an ISA in which the legal basis for sharing is stated. Staff are trained in operating procedures that are drawn from this agreement.

CP7 The duty to share information can be as important as the duty to protect patient confidentiality

The nursing team enables appropriate sharing with the Police, and other agencies such as housing and social care. Police CCR and response teams share information with nurses as required by the context of the caller and the incident.

Good Practice

In this case study nurses from a local health service provider have joined a Police emergency call-handling team. Good practice is illustrated in terms of:

- a joint call team which is better able to identify callers who are in crisis and to provide more appropriate support;
- for the caller this means that the right interventions, at the right time, by the right people with appropriate follow up;
- Police share information for purposes of early intervention, prevention and safeguarding and nurses share on the basis of either consent, where it is recorded in care plans, public interest, or best interest where the caller is considered to lack capacity;
- in addition to the mental health and substance abuse systems, nurses are also able to access social care for members of the public with dementia and children in care;
- since nurses work as part of the emergency call team, training has been provided to the wider Police force and there is greater awareness of how to handle people with illness when they are in crisis; and
- privacy notices of both Police and health service organisations state how information is held and shared and an ISA summarises the arrangement.

If you have further questions on this case study, please contact:

Ellisam@norfolk.pnn.police.uk

If you have found this resource useful and are planning to start work on improve information sharing between health and Police in your area, please let us know so we can track the impact of this work by emailing info@informationsharing.org.uk

Data sharing between the Police and NHS for care purposes

Case Study

Seaview voluntary organisation for rough sleepers: access to services

CP1 CP2 CP3 CP4 CP5 CP6 CP7

Caldicott Principles covered

The example within this case study is governed by the Data Protection Act (1998) but will be updated from May 2018 to reference any changes made to comply with the introduction of the General Data Protection Regulation (GDPR).

Overview

Seaview is a charity based in St Leonards-on-Sea that offers open access for rough sleepers and a range of services addressing isolation including substance misuse, learning and physical disabilities. A mental health street triage team of police officers and nurses visit the centre and there is a close working relationship with the local housing department; this case study illustrates how a charity provides a safe place of trust and how information is shared with formal care agencies to allow the provision of services.

The Seaview approach

Homeless people often have bad experiences of the Police and poor outcomes in terms of service usage. Many are the victims of violence, some are violent and many have problems of addictions and substance abuse and suffer both physical and mental health issues. Seaview has been running since 1985 and has grown year on year seeing an increase in impact, and the number of people it can help. In 2014/15 the charity supported 92 new homeless individuals and helped two thirds of those find secured housing options. In 2015/16, Seaview saw 1392 individuals across all areas of support, 147 of whom were rough sleepers.

View at www.informationsharing.org.uk/healthandpolice

The partnership of Seaview with care agencies is aimed at providing a safe environment where trust of service users develops and they are then able to access services. The Seaview centre provides access to a wide variety of statutory and voluntary sector support services. St Johns Ambulance operate a primary care nurse-practitioner, and podiatrist clinic through the centre. Sussex Police fund a mental health nurse who works with a liaison officer to provide a street triage service in the area.

The team create a safe environment in which the trust of the service users is established and maintained. A service user-centred approach underpinned by consent is normal; however, there are rare occasions when information is shared without consent for safety, public interest or safeguarding reasons. The Seaview team follow the Caldicott Principles in training staff from different agencies in working with this service user group who are often excluded from care environments because of their behaviour. All staff sign a declaration based on these principles.

For service users a layered approach to consent is followed. Sometimes service users come in only for a meal, a shower and a chat. Once it is clear they wish to move forward, a discussion is held of what services are appropriate in which consent is sought and a form is signed. In terms of sharing outside the centre, aside from the street triage team, this is centred on verification of eligibility for housing services.

Seaview have explicit rules for service users and act to maintain a safe environment. Use is made of the police liaison officer and East Sussex County Council safeguarding team to share concerns when they arise. On occasion action is taken to ban an individual from the wellbeing centre in order to protect the welfare of others. In those circumstances the individual can still access health and professional appointments via the side entrance.

Why is information sharing necessary?

Service users have multiple health and social needs and Seaview provides an environment where partner care providers are available. The referral process for the different providers requires information to be shared.

What does this mean for vulnerable people?

Interventions are available to service users at the right time delivered by the appropriate service in a place of trust and safety.

How is the information shared?

Information is shared on a need to know basis wherever possible with full participation of service users. The mental health triage nurse and the police officer attend morning meetings in order to discuss and manage any risk concerns and the potential for any mental health referrals for the street community.

For housing access services, Seaview and other partners participate in a monthly case conference focussed on entrenched rough sleepers. This is chaired and hosted by the council housing department to review complex issues for the current service users and new members. A confidentiality agreement is signed by all attending each meeting with an action plan agreed and owned by the Hastings Borough Council housing team.

Health services are available in the centre currently through St Johns Ambulance Service, soon to be expanded to include the GP services. Service users self-refer and information is shared with health practitioners is shared with direct involvement of the individual concerned. If the 'house rules' are broken the Seaview team will contact the Police through agreed procedures.

Information sharing barriers and how they were overcome

- the tension between service criteria and goals of the different partner organisations;
- when sharing with local authority services (e.g. housing) that the same information cannot be used for another purpose (i.e. another service);
- the need to balance provision of trust with management of behaviour; and
- as the centre grows, the need for training new staff and volunteers to a common set of procedures for this distinctive approach.

These issues were addressed by:

- developing a strong vision for information sharing across the partnership; discussion continues on terms of reference and development of an ISA;
- establishing, a consent model for access to health and housing services;
- transparent rules are followed for behaviour and there is rapid response to problems with clarity of roles in emergencies between partner organisations; and
- there is a close working relationship of police liaison officers and mental health nurse who provide the street triage service.

Management of consent

Service users give consent for access to health and housing services. For the mental health triage service the police officer shares information for early intervention, prevention and safeguarding and the nurse with consent, where it is recorded in care plans, or on the basis of public interest or best interest where the individual is considered to lack capacity.

What are the benefits of information sharing?

Health services

- improvement of service provision to a difficult to reach group of service users and patients many of whom have complex mental, physical and social needs.

Police

- improved integrated and collaborative working with service users and better early intervention in mental health crisis for individual service users.

Voluntary sector organisations

- earlier access to shared information can result in less stress to service users in repeating distressing information. This also creates more holistic planning and faster referrals with improved outcomes for individuals .

Joint benefits

- provide better access to services for a historically difficult to reach group and to lower demand on individual teams through collaborative working. Outcome measures are yet to be determined but the intention is to establish these as the commissioning process continues to develop allowing services to be more targeted and to maximise impact.

Cultural issues affecting information sharing

Embedding information sharing across partnerships invariably highlights a number of cultural issues between organisations that need to be addressed. In this example the fractured relationship between care agencies and rough sleepers meant that a new approach had to be found. Clear and trusted communication channels and procedures have been developed to allow service users to access support on a consensual basis but for this to be balanced against safeguarding. The Caldicott Principles are used by the Seaview Project to breakdown cultural barriers.

How the Caldicott Principles are applied in this case study

CP1 Justify the purpose(s)

The sharing of information within Seaview is for the purpose of progressing service users from rough sleeping into health care and housing services. For the street triage team, Police share information for purposes of early intervention, prevention and safeguarding and nurses share on the basis of either consent, where it is recorded in care plans, or public interest, or best interest where the caller is considered not to have capacity.

CP2 Don't use personable identifiable information unless it is absolutely necessary

The necessity to share information is governed by the situation of the individual. All staff are trained in the multi-agency approach to sharing based on the Caldicott Principles.

CP3 Use the minimum necessary personal confidential data

The sharing of information for an individual is based on enabling a progression toward a more conventional life which includes access to care services. On that basis, at times, risk information is shared.

CP4 Access to personal confidential data should be on a strict need-to-know basis

Information shared is relative to the situation e.g. need to know basis led by the practitioner's knowledge and service user disclosure. Access to Police and care information systems is limited to officers and registered health care professionals.

CP5 Everyone with access to personal confidential data should be aware of their responsibilities

Confidentiality and data protection is the responsibility of each staff member. All information about individuals, that several agencies may be supporting, is treated as confidential and used only for the purposes for which it was given.

CP6 Comply with the law

Staff are aware that they are sharing highly confidential information and gaining consent is normal practice, however, in some situations where there is significant risk of harm to an individual, confidential information is shared without consent. Service users are made aware of this possibility through 'house rules'.

CP7 The duty to share information can be as important as the duty to protect patient confidentiality

The sharing of information in appropriate ways is an essential way of working for the Seaview team as they seek to support service users back into main stream life. For the professionals involved, an understanding of their duty of care to the individual enables them to decide whether, when and how to share.

Good practices

This case study concerns a voluntary organisation that provides a safe environment for rough sleepers where service users can choose to access services including housing and health. Police work closely with the team to make sure that, whilst the trust of the service user is gained, at the same time, safety is maintained. The following good practice is illustrated:

- establishing a trust environment for vulnerable individuals can be disruptive in care environments;
- a common approach to professional development for all staff through training in confidentiality and the use of consent for sharing in a multi-agency context;
- clear procedures for exceptions to consent-based sharing, e.g. safeguarding of the individuals, their family and children and the wider public;
- for the Police and mental health triage service - the police officer shares information for early intervention, prevention and safeguarding and the nurse with consent, where it is recorded in care plans, or public interest or best interest, where the individual is considered to lack capacity;
- there also continue to be negotiation of the mechanisms for information sharing and of consent for the different partner organisations as the collaborative care model is developed; and
- privacy notices of both Police and health service organisations state how information is held and shared and an ISA summarises the arrangement.

If you have further questions on this case study, please contact:

Annie Whelan

Project Manager, Seaview Project

A.Whelan@seaviewproject.org.uk

If you have found this resource useful and are planning to start work on improve information sharing between health and Police in your area, please let us know so we can track the impact of this work by emailing info@informationsharing.org.uk

Data sharing between the Police and NHS for care purposes

Case Study

Access to Summary Care Record and NHS mail in custody suite

CP1 CP2 CP3 CP4 CP5 CP6 CP7

Caldicott principles covered

The example within this case study is governed by the Data Protection Act (1998) but will be updated from May 2018 to reference any changes made to comply with the introduction of the General Data Protection Regulation (GDPR).

Overview

New patient information systems have gone into use in 25 custody suites in the East of England. The NHS Summary Care Record (SCR)[37] allows the health care professional (HCP) to access patient demographic data and a summary of key healthcare information from the record held by GPs. HCPs are also able to use NHS mail for secure email communication with other health care teams and where appropriate with the Police. This case study provides detail of the benefits that result from this investment and references the next phase when an NHS-spine enabled GP system (PCS1)[38] will provide an increasingly integrated healthcare information system along the full criminal justice pathway of England and Wales by 2020.

View at www.informationsharing.org.uk/healthandpolice

In the year ending March 2015, there were 950,000 arrests carried out by Police forces in England, with a total of 3,133 persons detained for longer than 24 hours.

Many detainees have significant health problems which often include drug and alcohol dependency and some suffer from mental health problems. On average over 45% of these people were examined by a HCP whilst temporarily detained by the Police. In 2014-15 official figure showed there were 17 deaths in, or immediately following police custody, which was the highest figure for five years with eight of the people identified as having mental health concerns and 16 known to have issues with alcohol and /or drugs.

Access to the NHS network is required for these integrated systems as it links hospitals, mental health care providers, medical centres, community support services, and all GPs. NHS England East England region, and the six Police forces of Bedfordshire, Cambridgeshire, Essex, Hertfordshire, Norfolk and Suffolk have collaborated on the delivery of the NHS network which links into police custody suites (PCS) within their region.

SCR is a national system that holds information about a patient's medication, adverse reactions to medication, allergies and has more detail on medical history if the patient has agreed this with their GP. About 55 million people in England have an SCR record and the number is growing.

Roll-out of the GP system for custody has been implemented in a number of regions across England since autumn 2016. It has templates developed to support health and welfare provision in police custody. HCPs will be able to view and update a shared record for each detainee in any police region. With the detainee's consent and if the patient's GP Surgery uses the same software, HCPs can access the full, existing GP record. Again with consent, the HCP can securely email a summary of the care provided in custody, or details about new conditions or recommended follow-up to the detainees usual GP and any other appropriate NHS care provider.

[37] Summary Care Records - https://digital.nhs.uk/summary-care-records
[38] NHS-Spine enabled GP system - https://digital.nhs.uk/spine

Places of detention - scale of estate

Residential estate (c.148 sites)

- prisons (population approx. 85,000);
- young offender institutions;
- secure training centres;
- secure children's homes; and
- immigration removal centres (population approx. 3,600);

Non-Residential Estate

- police custody (approx. 216 suites, throughput 1.25m);
- courts (approx. 238 sites, throughput 2,693,000*);
- sexual assault referral centres ** (approx. 30 sites, throughput 13,000); and
- liaison and diversion.

*England and Wales

**Within the scope of Health & Justice direct commissioning although not classed as a 'place of detention'

Why is information sharing necessary?

A shared healthcare record and its availability throughout the criminal justice pathway will enable better healthcare provision and improved outcomes for detainees. Healthcare is based upon a team approach and the use of shared, electronic patient systems are one of the foundations of quality. Many detainees in custody have complex health problems; these new systems support improved co-ordination of health interventions within and across healthcare and criminal justice agencies to prevent self-harm, suicide, and harm to others.

What does this mean for vulnerable people?

Detainees with particular health problems (e.g. mental health) should gain appropriate care including diverting them away from an inappropriate custodial response. For all detainees this includes improvement through:

- assessment of fitness for interview or further interview and documentation and interpretation of injuries;
- court judges and magistrates will have improved understanding of an individual's welfare needs when making judgements;
- appropriate involvement in paediatric forensic medical examination; and
- more timely health information relevant to provision of reports, statements and court attendance.

How is the information shared?

HCP look up the SCR record for detainees on initial assessment. The new system, PCS1, will allow the creation of a shared police custody healthcare record that can then be accessed by other HCPs during that period of detention when providing health or welfare care to the patient, or at disposal when planning follow-on care. The patient record will also be available to other HCPs working in police custody during any future period of detention. The PCS1 record is not available to healthcare providers outside the police healthcare environment but an intention to extend access to within the health and justice sector is planned and with patient support HCPs are able to email external partner health service care providers. Sharing of patient information with the police custody team is through briefing by an HCP or recording directly onto the police custody record.

Information sharing barriers and how they were overcome

- absence of NHS network and of modern NHS spine-enabled patient information systems in custody suites and other places of detention; and
- lack of ISA between organisations.

These issues were addressed through:

- provision of access to NHS network in custody suites;
- NHS network information governance (IG) statement of compliance and an annual IG toolkit mean the NHS 'rules of the road' are applied in custody suites;
- HCPs sign an acceptable use policy when they are given an NHS smartcard, an access role and are trained to use the new patient information systems; and
- procedures are explained and HCP and police custody staff are trained in how to share information.

Management of consent

The detainee as patient decides if they wish to receive healthcare and the HCP discusses with whom their healthcare information can be shared. Again, HCPs discuss consent with victims for forensic services. Where there is no capacity, information is shared on the basis of best interest.

For use of the SCR, the HCP asks the patient if this can be viewed. There is an override available for patients without capacity, or, in the absence of consent, where it is judged to clearly be in the best interests of the patient. An SCR audit function is available to check access. Random spot checks are conducted regularly including police forces confirmation that patient records checked align with people held in custody. For specialist custody assessments the custody team asks advice of the HCPs, there is no direct access to the healthcare record.

For GP records, the HCP asks the patient if this can be viewed. The patient's GP surgery will also agree access. In the absence of both forms of consent the HCP is not able to view the record. In addition, if the detainee agrees, the HCP can email a note of care and recommendations to other health service care providers.

What are the benefits of information sharing?

Health services

- improvement of information sharing by HCPs for a difficult to reach group of patients many of whom have complex mental, physical and social needs;
- improved patient care delivery pathways through the justice environment and beyond; and
- reduced resource impact on other healthcare environments, particularly hospitals, is also anticipated.

Police

- improved integration and collaborative working on behalf of detainees; this includes more appropriate interventions in mental and other health crisis for individual service users and also a better experience of specialist custody assessment and forensic services;
- better, more informed medical provision reduces the risk of medical accidents and deaths in custody; and
- reduction in rate of reoffending through targeted support services appropriate to the individual's needs.

Joint benefits

- access to GP system, SCR and NHS mail ensures continuity of care and also makes it easier for HCPs to conduct accurate medical risk assessment for detainees. This should ensure the health needs of detainees are addressed more appropriately and custody staff can more safely detain a person with a known medical condition;
- the healthcare record will be available throughout detention from arrest to release; and
- for victims undergoing forensic examinations, the HCP can provide a higher level of support through access to a continuous healthcare record. This should result in improved efficiency and make better use of medical, Police, and justice system resources. In turn this should reduce the impact of offenders on acute health services and contribute to reducing reoffending rates by enabling the effective referral of those who need specialised care to local community schemes including liaison and diversion.

Governance of the work

To allow access to the NHS applications all organisations agree to an IG statement of compliance and all HCP sign a user agreement that allows them use of an NHS smartcard as a strong authentication token.

Cultural issues affecting information sharing

Cultural issues which were tackled in this example include improved relationships between health service organisations, with a shift from keeping health information in silos. This highlights the importance of strong leadership to embed such practice of access in custody suites. It shows what a difference challenging existing cultural barriers to information sharing can make to the services offered to individual patients, and the improved service that can be offered by both health services and the Police.

How the Caldicott Principles are applied in this case study

CP1 Justify the purpose(s)

For the healthcare professional team the purpose is provision of care and, for Police, early intervention, prevention and safeguarding of vulnerable individuals whilst they are in custody.

CP2 Don't use personable identifiable information unless it is absolutely necessary

NHS systems require accurate identification of a detainee. Once the individual record is in use there are system controls which limit access (re authentication of users with an NHS smartcard, role-based access control and legitimate relations functions within the system).

CP3 Use the minimum necessary personal confidential data

Direct use of the NHS patient health record applications by HCP is usually on the basis of consent and is limited by role and relations. HCP share the minimum amount of information required with the custody team to enable assessments and other custody tasks requiring healthcare information to be completed.

CP4 Access to personal confidential data should be on a strict need-to-know basis

Information is only shared by the HCPs with the custody staff on the basis that they need the information to be able to fulfil their legal duty of care to the individual whilst in their detention. Sometimes sharing is on the basis of consent, or where there is a risk to others, or a strong public interest (i.e. serious crime).

CP5 Everyone with access to personal confidential data should be aware of their responsibilities

Confidentiality and data protection is the responsibility of each individual professional. All information about individuals must be treated as confidential and is used only for the purposes for which it was given. Training is provided to HCP in terms of their responsibilities and also in use of the health care applications.

CP6 Comply with the law

Staff are aware that they share highly confidential information and gaining consent is normal practice. Use of the NHS network requires organisations to follow the 'rules of the road' (IG statement of compliance) and HCPs sign an acceptable use policy when they are given an NHS smartcard. HCPs who access healthcare records are trained in use of the systems.

CP7 The duty to share information can be as important as the duty to protect patient confidentiality

Proper management of the healthcare needs of detainees, as well as effective prevention of self-harm, suicide risk, or harm to others, requires information to be shared within and across healthcare and criminal justice agencies.

Good practice

Modern health information systems are being provided across the criminal justice estate. This case study illustrates early use of these systems in custody suites. Good practice is seen in terms of:

- provision of integrated patient information systems that enable access to a continuous healthcare record before, during detention and on release for members of the public who often have multiple, complex health problems;
- HCP are able to share a more complete set of patient information with the custody team for assessments and other purposes; and
- privacy notices of both Police and health service organisations state how information is held and shared and an ISA summarises the arrangement.

If you have further questions on this case study, please contact:

Chris.Breeze@nelcsu.nhs.uk

If you have found this resource useful and are planning to start work on improve information sharing between health and Police in your area, please let us know so we can track the impact of this work by emailing info@informationsharing.org.uk

Things to consider when sharing information

Two checklists are recommended as step-by-step guides to sharing information:

- as part of a joint team and / or routine business process - see page 37; and
- one-off disclosure on behalf of an individual - see page 39.

Process	Product	Culture
Partnership discussions	• business case for joint innovation	• vision • strategic leadership • informed decisions • service design
Partnership collaboration	• Privacy Impact Assessment	• common purpose • managing risk • working in partnership • stakeholder consultation • professional development
Engagement with service users	• consulting and informing service users • privacy notice update	• communication (do we need to explain?) • community engagement • targeting services
Legal compliance and arrangement for information sharing	• Information Sharing Agreement	• governance for information sharing • legal basis for sharing of information • what is shared, how and what limitations are placed on the informaion
Partnership operational management	• Standard Operating Procedure for joint team • staff training • handling exceptions • governance arrangements • Subject Access Requests, Freedom of Information etc	• trust • partnership working

Diagram one: Process and products for a new joint process of information sharing

Where partnerships develop an approach to routine sharing of information the assumption is that an initial assessment is completed, a PIA,[39] and an ISA[40] is prepared (see diagram one). Service users are informed through consultation, communication and a privacy notice, (in addition, joint procedures are prepared and standard operating procedures (SOP)[41] are implemented, with active, joint governance arrangements and staff training). These arrangements take different forms for each of the case studies.

NB: If a PIA is not undertaken the partnership should document the reasons for not doing one.

[39] Privacy Impact Assessment - https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

[40] Information sharing agreement - https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

[41] Standard operating procedure - www.ncl.ac.uk/ohss/safety/risk/sop.htm

Questions to consider when sharing information in a multi-agency/partnership environment

These questions are recommended to inform discussions. IG officers and project officers should always be jointly consulted.

Implementation phase

- when answering questions 1-10 and 14 consideration must be given to whether all are reflected in the ISA; and
- when answering questions 11, 12, 15-19 and 22 considerations must be given to whether all are reflected in the SOP.

Question		Complete
1.	Has a PIA[42] been undertaken?	
2.	Do both organisations have secure and confidential arrangements in place (e.g. technical and organisational controls)?	
3.	In terms of sharing information, are secure channels used?	
4.	For each organisation what is the legal basis for collecting and sharing information? (see Legal basis for information sharing section, page 9)	
5.	Is a SAR[43] service required?	
6.	Is there agreement on the purpose that the data will be used for?	
7.	Is there agreement on what personal, sensitive and confidential information to share (proportionality, necessity and granularity) with whom?	
8.	Is a statutory obligation for sharing information agreed? (e.g. Road Traffic Act)	
9.	Is there a lawful basis for disclosing personal information with another party (data controller)? (e.g. DPA & Common Law[44])	
10.	What arrangements will be made to restrict access to confidential personal information on a role / position basis?	
11.	Is it clear how long records should be retained?	
12.	How and who will authorise any amendments to records?	

[42] Privacy Impact Assessment - https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

[43] Subject access requests - https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/

[44] Data Protection Act 1998 - www.legislation.gov.uk/ukpga/1998/29/contents

Informing patients and service users

Question		Complete
13.	Do the privacy notices[45] of both organisations tell service users and patients how their records are stored and shared? (Is the Police / NHS information sharing explained? Who will their personal information be shared with? The choices they have and how to exercise them?)	
14.	Is there agreement on the consent mechanism normally used and also public interest and best interest (lack of capacity) mechanism?	

Operational concerns

Question		Complete
15.	Are there agreed arrangements for SAR's[46]?	
16.	Are there arrangements for managing and resolving data quality and accuracy or patient / service user concerns on record accuracy?	
17.	Are there arrangements for handling patient / service user objections to the processing of personal information about them?	
18.	Are incident management and reporting arrangements in place?	
19.	Are shared arrangements in place for requests for access to personal information by third parties?	

Support for staff

Question		Complete
20.	What guidance and training is available for staff?	
21.	Are the 'grey areas' and 'red lines' for information clear for staff?	
22.	Is there a process for escalating uncertainties and issues for staff?	

[45] Privacy notices - https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

[46] Subject access requests - https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/

Questions to consider when sharing information on an individual basis (one-off disclosure)

These questions are a guide for practitioners and project case managers to consider when sharing information:

Question	Complete
Is the information you are planning to share necessary for the purpose for which you are sharing it?	
Is it shared only with the people who need to have it?	
Have you identified exactly which individuals need to access the information you are planning to share, and how they will only have access to the information they need to see?	
Is it accurate and up-to-date? (What is the shelf life of this information?)	
Is it shared in a timely fashion? (Do partners understand this timeline?)	
Is it shared securely?	
If you decided to share information do you have a record of what you shared, with whom and for what purpose?	
If you are asked to qualify your decision and reason for it, have you recorded your actions in regard to information sharing? (Where are these recorded?) *NB: Necessary, proportionate, relevant, adequate, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is as accurate and up-to-date, is shared in a timely fashion, and is shared securely.*	

Question	Complete
Why is it necessary to share personal and/or sensitive information about a person?	
What have you done to ensure that the people who you will be sharing information with are aware of their responsibilities and obligations to respect the privacy of the person/s about which you will be sharing information? *NB: Seek advice from, and discuss with other practitioners if you are in doubt about sharing the information concerned, without disclosing the identity of the individual where possible.*	
Do you know who in your organisation is ultimately responsible for ensuring it complies with its legal requirements, and has the organisation/s you will be sharing information with, identified their equivalent person with overall responsibility? *NB: Remember that the DPA 1998[47] and human right law[48] are not barriers to justify information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.*	

[48] Data Protection Act 1998 - www.legislation.gov.uk/ukpga/1998/29/contents

[49] Human Right Law - www.equalityhumanrights.com/en/human-rights/human-rights-act

Question	Complete
Have you gained consent from the person to share their information; is it reasonable to expect the information would be shared for the purpose it was requested for? *NB: Be open and honest with the individual (and/or their family where appropriate from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement.*	
If you haven't got the person's consent, do the facts of the case mean there is a good reason to share their information, such as where safety may be at risk?	
Have you considered the safety and well-being of the individual and others who may be affected by their actions, when deciding if you should share information? *NB: Share with informed consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, there is good reason to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be certain of the basis upon which you are doing so. Where you have consent, be mindful that an individual might not expect information to be shared.*	

Notes

Notes

We have a range of tools and case studies that we update regularly on our website. Sign up for updates on the site or connect with us to keep updated.

Follow us **@InfoShareCoE**

Join the conversation **#InformationSharing**

Connect with us **LinkedIn**

informationsharing.org.uk

R0264