The British
Psychological Society
Promoting excellence in psychology

Electronic records guidance

March 2019

If you have problems reading this document and would like it in a different format, please contact us with your specific requirements.

Tel: 0116 252 9523; E-mail: P4P@bps.org.uk.

Contents

Preface

This document provides guidance for psychologists working in any context where they may use, retain, manage or process electronic records. It is the formal advice of the Society to its members and is intended to provide assistance on the professional, ethical, and legal responsibilities of members contributing to these records.

The Society expects that these guidelines will be used to form a basis for consideration, with the principles being taken into account in the process of decision-making, together with the needs of others, the specific circumstances and local organisational policy. This guidance should be read in conjunction with the Society's *Code of Ethics and Conduct* and *Practice Guidelines* or *Code of Human Research Ethics*, as appropriate. Practitioner psychologists may also refer to the HCPC standards of proficiency and separate guidance regarding confidentiality[1].

This document replaces the Society's 2011 guidance. It is updated to reflect changes in practice, context and technology.

For definitions of the terms used throughout this document please see the Glossary on p.18.

Acknowledgements

This document was prepared by a working party of the British Psychological Society's Professional Practice Board.

The members are:

Graham Fawcett – Chair – Chartered Clinical Psychologist, East London NHS Foundation Trust

Michael Berger – Chartered Psychologist

Pirashanthie Vivekananda-Schmidt – Chartered Occupational Psychologist and Medical Educationalist

Robert Stephens – Clinical Neuropsychologist, Nottingham NHS Trust

Hannah Farndon – Policy Advisor

Sunarika Sahota – Policy Administrator

1. Introduction

Electronic Health Records (EHRs) are widely used by psychologists and other professionals to record, store and process health-related and personal information. Data in the individual EHRs serve multiple purposes:

- recording and communicating service user demographic and clinical characteristics;
- recording assessments, treatments, interventions and outcomes;
- local service management;
- to support commissioning and contracting requirements;
- local and national policy information requirements;
- clinical and other research.

It is important to recognise that EHRs are not just repositories of information but play a dynamic role in clinical practice. Their content can have a profound effect on what clinicians think and do, with major implications for the quality and safety of care. Increasingly the content of the record is available to be accessed, added to and commented upon by multiple staff in different services with appropriate access rights and by service users themselves. Also, with informed consent, and as appropriate and needed, information from the EHR can be shared with others involved in care, including non-NHS agencies, such as social care providers.

With the advancing sophistication and use of personal mobile technology, major software companies are creating electronic applications (apps) that enable the recording and storing of personal health-related information collected from body worn sensors and device apps that have the potential to be included in GP or other health system records. The Microsoft Health Vault[2] is an instance of such, aimed at collecting family member health information for use by healthcare services.

EHRs have proven beneficial to the quality of service delivery: an up-to-date record of interventions and findings that can be readily and immediately available to staff within and across different settings. This delivers safety, time efficiencies and increases the potential for live feedback of results to service users. EHRs can also have downsides, such as disruption of existing practice, greater demands on practitioners to gather and process information, difficulties in locating information, inappropriate information entry and record access within an organisation or through hacking or through the misuse of information and the potential for the wider propagation of poor quality information.

The use of EHRs can pose professional and ethical concerns for users and clinicians. Agencies such as NHS-Digital, The Professional Records Standards Body for Health and Social Care as well as the Department of Health in England and equivalent national health bodies and professional organisations all devote a substantial amount of effort to addressing and resolving these issues. The National Advisory Group on Health Information Technology in England's *Making IT Work* report, also known as the Wachter Report,[3] outlines a digital roadmap for the development of EHRs and system implementation in England, with relevance to the other nations.

Wachter, in his influential book *The Digital Doctor*[4] also outlines the key challenges and potential gains arising from the introduction of EHRs. Keeping a record up to date may isolate the patient from staff if done during a consultation because professionals are looking at a screen, decision making may become more precise but less personal, algorithms may deliver the wrong dose of a treatment or the wrong treatment altogether, and while data may be shared efficiently they can be invalid. Wachter's overall conclusion is optimistic but requires a medium to long term view to be taken, rather than making judgements based on current experiences, with changes involving all users, patients, clinicians, policy makers and commissioners.

As this document went to press the results of the Topol Review on preparing the healthcare workforce to deliver the digital future was published

2. The Record

The 'record', electronic or paper, is data collected in a wide array of formats to store and communicate clinical information. While certain core elements are common (name, reference number etc.), there are formats unique to the context of use and variations introduced by individual systems and the companies who sell them. This section will outline some of the types of data which feature in a record that Psychologists may encounter during their work.

The development of digital technologies is increasingly leading to records containing new and varied data formats and links to service user-specific information. This can include:

- pharmacy, radiology, information from instruments and associated clinical interpretations and reports. These data formats can be added or electronically linked to individual records.
- links to scanned and indexed paper documents including correspondence, images, drawings, psychological test pro-formas, test data and reports.
- scope for including audio and video recordings from body or other cameras and devices.
- information from smartphone or other apps, providing real-time physiological, psychological and other data. These are all components of tele-medicine, developing tele-psychology and AI applications.

These diverse forms of information pose particular challenges, for example capturing, storing, accessing, interpreting and integrating new content where the identity of the service user and the response sources may be difficult to verify. Psychologists are already facing challenges related to internet-delivered therapies, online psychological tests, email, telephone and video conversations, exercise/activity meters etc. Also, the data quality may be questionable, reflecting issues in device calibration or underlying software characteristics and errors.

2.1 A standardised clinical language for EHRs

To deal with the potential for variation in meaning and to facilitate accurate coding of clinical language and information in EHRs, special coding systems have been introduced.

SNOMED CT (Systematised Nomenclature of Medicine – Clinical Terms) is a systematically organised computer processable collection of medical terms providing numerical codes, terms, synonyms and definitions for use in clinical documentation and reporting to ensure standardisation.

Psychologists should recognise that this methodology is increasingly used within EHRs to process free text (i.e. unstructured text) and other clinical information for data analysis of, for example, prevalence, clinical activity and clinical outcomes. The Society recommends that Psychologists become involved in the implementation of such approaches to coding both in their local services and at national level to ensure the chosen system is valid and relevant to psychological practice.

2.2 Apps

Apps and online intervention programs (e-therapy) offer widespread benefit. They enable service users to use their own devices to monitor and report their mood, set reminders for actions to take or complete mood regulation techniques.

Apps and e-therapy approaches vary in their efficacy. Clinicians must evaluate them before recommending them to clients or adopting them into clinical practice. This should include consideration of the developer of the app and how any data from the app will be collected and stored and shared. Psychologists should also consider that not everyone has access to the internet at home and it may also not be appropriate to use these apps in public places.

Some apps and programs will not retain personal identifiable information and so any data captured are likely to be anonymous. Other apps may require a minimal level of identification to allow for repeat use and to display progress, however such identification may, itself, be pseudonymised. From a record keeping perspective, apps may retain person level data that are:

a) anonymous,

b) anonymous on the device but reported to the clinician by the client,

c) anonymous on the device but recoverable through an electronic key for use by the clinician,

d) have sufficient personal identifiable information to allow for the data to be exported to another system and matched with the correct record.

Where personally identifiable data may be recovered, this is subject to the Data Protection Act, 2018 for health and social care information in the same way as any other personally identifiable data processed (i.e. used) by a clinician. For further information, see Section 3 Legal Frameworks.

2.3 Portals

Portals are a way of electronically viewing personally identifiable information stored on a remote record system or database. Portals can be used in different ways depending on their access rights.

- Asynchronous portals allow for one party to write to a database and change it – for example making an appointment with a GP through an appointment booking system.
- Synchronous portals allow for two-way communication such that data may be entered, and the system then responds. Some online electronic CBT programmes have this facility.

- A 'view only' portal allows for personally identifiable data in one electronic system to be viewed in another. For example, Health Information Exchange in London allows for blood test results held in one hospital to be viewed by a community clinic, and for care plans in the community to be viewed by a clinician in a hospital.
- 'Write portals' allow clients to enter or amend data in their own record, for example to note a change of address or phone number. Opening data sources in this way, subject to appropriate governance, is broadly welcomed by service users, particularly those with complex conditions, who will, among other things, then have less need to recount their story repeatedly. This facility can also have drawbacks that need to be planned for and systematically managed, for instance when a user challenges the correctness of record content. Such integrated records are most helpfully considered to be a single record subject to Information Governance, Data Protection and Clinical Safety considerations.

2.4 Social media

Social media, whilst widespread, has until recently contained little personal identifiable information that would constitute a health record. Recent advances however indicate that the way social media is used by an individual may predict, amongst other events, suicide attempts[5]. To that end and with the service user's permission, there is the potential for social media to be monitored for risky mood states and clinicians alerted as required.

2.5 Psychometric testing apps

Apps for psychometric test users have long been available. They can automatically convert raw test data to standardised scores and generate an initial interpretation in the form of a report. This can be very helpful as it reduces the risk of human error when making repeat calculations and cross-referencing normative tables (although not immune to any errors introduced by those who programmed the systems). These apps can sometimes produce much more detailed analyses than are practicable for clinicians to do manually. Of course, it is critical that the data entered into the apps are accurate.

As with all test results, overall clinical interpretation is essential, taking into account the psychometric robustness of particular tests, the service users' clinical history and performance factors during testing. For these reasons, it is advised that automatically generated reports are used as a helpful starting point, rather than a finished and complete interpretation.

All the technologies mentioned in this section are evolving very quickly. Psychologists should aim to keep abreast of developments and be aware of the potential consequences. Sophisticated apps that can access personal data shared on social media could potentially be used in ways not approved by the individual concerned.

3. Legal frameworks

The legislation that is relevant to decisions around storing, sharing and facilitating access to electronic health records and the use of record data includes:

- the UK Data Protection Act, 2018 that embodies the EU General Data Protection Regulation (GDPR),

- the Freedom of Information Act,
- the Mental Capacity Act (including devolved nation equivalents). Further information is available in Appendix 1.

Psychologists need to be aware of their responsibilities under the General Data Protection Regulation 2018 (GDPR). All personally identifiable data held about a service user in an electronic record, email or document, is subject to these regulations, even if pseudonymised. This includes clinical notes held on an electronic record system, emails relating to a service user, supervision notes (even if on paper), process notes, photos and social networking exchanges.

Service users have the legal right to access their EHRs. Practitioners need to carefully consider whether there could be exceptions to disclosure, for instance, if the information may cause harm to the service user, or the information held can reveal information about another person who has not consented to the disclosure.

If there is statutory duty to share information, e.g. a court order, it is important to ensure that only what is requested is shared – with suitable caveats – and irrelevant information (i.e. information not relating directly to the request) is removed prior to sharing. Additional considerations need to be exercised about sensitive information such as sexual or reproductive history. As the service user is the owner of their health record, so a service user with competence (as determined by the practitioner) is ultimately responsible for any consequences regarding requests for sharing their own health record with any third-party practitioners.

4. Information Governance

Psychologists should make, keep and disclose information in records only in accordance with national policy and legislation, and the policies and procedures of the organisation(s) they are employed by or working in collaboration with.

Systems that are explicitly designed and manufactured to provide electronic information for health or social care purposes are subject to two **Clinical Safety standards**. SCCI0129 sets out clinical risk management requirements for manufacturers of health IT systems and SCCI0160 requires a health organisation to establish a framework within which the clinical risks associated with the deployment and implementation of a new or modified health IT system are properly managed under section 150 of the Health and Social Care Act 2012. This applies equally to those in private practice as well as in the public sector.

The NHS and other healthcare organisations are responsible for ensuring that all EHRs comply with the manufacturer's requirements and conducting their own internal Clinical Safety evaluation. Independent practitioners are strongly advised to be mindful of safety issues when using any system or process to record service user information, e.g. an Excel spreadsheet. Independent Practitioners must satisfy themselves that the clinical risks of deployment of the EHR have been reduced to as low as possible – for example considering how service user care is conducted if the power fails.

Psychologists have a responsibility to ensure that their use of health IT systems is clinically safe, and that they comply with any mitigations identified by the manufacturer or by their organisation to reduce any risks associated with use of the system, to as low as reasonably practical.

Many of the governance requirements relating to paper records apply to EHRs, for instance, the potential impact of the information on all who may have access, including the service user, other professionals, managers, authorised carers, etc. Where possible, distinctions should be made between fact, observation and opinion. Judgmental comments should be avoided.

Irrespective of format, records made, kept or accessed by psychologists should be:

- systematic;
- appropriately detailed;
- in clear language/format;
- accurate;
- up to date; and
- relevant to professional work and to the purpose for which they were collected.

It is good practice for service users to be given feedback on the content of their records. Sharing records with service users supports a collaborative approach and enables full and effective involvement. Service user access to records is restricted to information about themselves alone and does not include access to third party reports. Restrictions also apply when disclosure would place the clients or others at risk of serious harm. In tripartite arrangements involving an employer, access to information should be governed by explicit agreements about what information can be shared with the commissioning organisation.

The individual applied psychologist practitioner makes their own judgement, in consultation with local information governance managers, whether it is in the interests of their client not to proceed in accordance with the official positions and protocols. As with any other clinical professional decision made by practitioners, they may be called upon to account for their action. This will include ensuring informed consent if possible, about the consequences of the decision.

Appendix 2 provides a checklist for clarifying if and how to store clinical material outside of an EHR.

4.1 Storage and sharing

It is the working assumption of many of those designing and managing EHR systems that all information will be entered in the EHR, including digitised or scanned copies of paper documents and that the originals can then be destroyed. This is referred to as a 'paperless' model. Some organisations may permit the storage of some paper records ('paper light'). Given the access limitations of paper records, the amount of space required for storage and the cost of storing and maintaining paper records (to meet the requirements for such retention), some services may also choose to digitise their record archives. If digitisation is in the form of a scanned copy of the record, it is important to ensure that some form of indexation is introduced so they can be searched. Other forms of digitisation, such as using

optical character recognition (OCR) leading to an editable copy of the record, facilitate detailed searches and more efficient retrieval although errors can arise more readily in such processes and such documents need to be checked for errors.

Cloud based storage is now widespread and is used by most EHR systems. Such storage is generally more secure than on site local equipment (e.g. on one computer hard drive), more resilient and accessible from a range of devices. Psychologists and services should be aware that cloud systems require broadband or 4G internet connections for access, which are more prone to failure than the EHR system and which require special arrangements to mitigate potential interruptions. Reputable EHR companies will assure robust continuity provision of record access in the event of a failure of their systems.

Thanks to cloud storage and fast processing systems, access to vast amounts of clinical information is relatively easy. However, with this much data it can be difficult for clinicians to find timely relevant information and to interpret and integrate it into their daily practice to benefit their clients and service users. The range and quantity of information that could be generated can lead to 'information overload' with the challenge for clinicians becoming how to access clinically relevant information rather than having all the information to hand. Psychologists are well placed to assist with the co-production of such systems.

Because cloud based information is networked, there is risk of unauthorised access both within service settings and through hacking or overcoming security arrangements designed to protect confidential clinical information. One of the potential problems with this is that once a practitioner can log into a system, they could potentially have access to the records of other service users, even if access is audited or is restricted to team-based practitioners. The 'right to know and need to know' principle governing record access should apply. Consideration needs to be given to ensuring all software is up to date to reduce the risk of viruses or hacking.

It is the duty of health and social care organisations to store direct care information (clinical and social care, and public health activity relating to individuals[6]) securely and to share it according to clear guidance as expressed in the revised Caldicott Guidelines relating to information governance. The newer guidance makes clear the right of service users to access their own records. The NHS Constitution[7] enshrines certain rights to the individual including the right to be informed how their personal information is used and to exercise control over the sharing of that information beyond their immediate care needs, except in certain legally specified circumstances. It is the responsibility of organisations to induct practitioners into the proper use and sharing of record content: at the same time, it is incumbent on practitioners to ensure they are aware of existing and developing guidance and requirements.

EHRs have transformed the landscape of record keeping from a private arrangement between a service user and a Health Professional to a potential contribution to databases used for a variety of purposes including information sharing with other agencies, research and 'big data' applications[8]. A great advantage of EHRs is that information may be shared quickly amongst appropriate professional staff and other agencies. Indeed, numerous national safeguarding inquiries have referred to the unfortunate consequences of failure to share information between professionals and/or agencies. This benefit is also the biggest challenge to the clinical process because services users, families, carers and staff

may have concerns about confidentiality, security and the ease of sharing information that might be inaccurate.

Whilst the BPS commends the general principle of information sharing in the interests of safe clinical care, it recognises that there will be situations, particularly in mental health services, HIV/AIDS services[9], general hospital work, and in services for sexually transmitted diseases, in which the psychologist and/or service user may not wish to share some or all information electronically, or at all.

When making decisions on such matters, psychologists should consider:

- the wishes, needs and interests of the individual service user;
- service policy, input from the organisation's clinical information or equivalent officer (CIO or Chief CIO);
- the risks of sharing or not sharing information;
- the risks of storing and not storing information;
- seeking the advice of their organisation or Trust's Caldicott Guardians.

Psychologists should satisfy themselves that there are appropriate secure arrangements such that access to records is formally audited, monitored and safely controlled.

Encryption standards are detailed on the NHS Digital website[10] which maintains up to date guidance. These cover the standards of encryption for data at rest (i.e. located on a device such as a PC, laptop or data stick) and data in transit (e.g. email). In essence, all patient identifiable data at rest should be encrypted and all patient identifiable information in transit should be encrypted end to end. Passwords should be secure, changed regularly and not written down.

The Information Commissioner Office website contains practical guidance, updated regularly, on how to deal with data breaches. Should a breach occur the circumstances need to be investigated and procedures modified accordingly, those affected informed directly and consideration given to reporting the breach to the ICO.

Some organisations may provide therapy or assessment services to a member of their own staff. Managing such records requires special consideration because it is unsafe clinically to seal or password protect records (see section 4.3 below), especially if a multidisciplinary team is involved in care. Staff records should therefore be monitored regularly for unauthorised access and steps taken under disciplinary procedures should such access occur. EHRs have the facility to flag or provide an alert in the event of unauthorised access, for instance where a service user is not referred to the staff member.

4.2 Specialist material

Some psychological activities involve the use of information which requires specialist interpretation skills, such as the results of psychological tests. Whereas this information used to be secured against general access and possible misinterpretation, there is now a shift in practice towards making such information available. The use of a virtual 'sealed envelope' is no longer considered to be clinically safe practice (see section 4.3 below). Indeed, some raw test data may be clinically important to share to reduce risks, and this shifts the responsibility of proper use and interpretation of test data to whomever uses it: it

is the user's responsibility to work within the bounds of their expertise and competence to interpret the data.

Access to the actual test forms themselves raise additional legal issues. Test materials are often purchased by an individual applied psychologist, and in so doing they enter into a legal contract with the publisher, which usually involves copyright and intellectual property law. The Society encourages psychologists to pay attention to those conditions and use professional judgement when determining how to manage materials such as test forms. Currently, many test publishers require written permission before a test form can be reproduced or scanned; that electronic access is limited to persons qualified to use the test; and that the test material is otherwise kept out of the public domain. This might be achievable for example, if a psychologist in private practice manages their own electronic storage system, but for many who work in a large organisation, it would not.

A consequence of the present situation is that many clinicians will have completed paper test forms that cannot be entered into a service user's EHR. If the psychologist has a strong clinical reason to retain the original paper form, then provision for this needs to be arranged with their employing organisation. However, in many situations, the legally preferable and most practical solution will be to treat test forms in the same manner as process notes (section 4.3), whereby the raw data and other relevant information such a notes made on the form are transcribed into the EHR (in an interpretative report or table of data), and the original form is destroyed.

4.3 Process notes and 'Sealed' sections in the Record

Some psychologists and psychology services have a tradition of retaining notes that are not stored in the primary clinical record (commonly the paper case notes), although they may well be stored elsewhere, such as in separate, secure psychology files. Such material is referred to as process notes and might include, for example, a service user's own often highly sensitive personal comments, written observations, drawings and charts as well as clinician hypotheses and formulations.

Keeping process notes, if the information they contain is not immediately made part of the clinical record, should be contingent on the practitioner having considered the risks of such information being inaccessible to others involved in the care of that individual. The Society advises that it is not appropriate to have a separate 'process' file maintained on a long-term basis and that any such material should be kept for specific, justifiable reasons, such as for use in supervision, and for a finite period. The notes should then either be scanned into the electronic file with the relevant information incorporated into a psychology report or destroyed if no longer relevant. This is partly because of clinical risk consequences and partly because of potential legal issues.

Not every piece of writing about the service user will necessarily be stored: the decision to do so, or not, is up to the individual clinician, having regard to the relevant specific circumstances and the attendant risks. Whatever other conditions might apply, such notes and records should be regarded as part of the clinical record and, if retained, kept securely and not removed from the service premises without appropriate secure arrangements.

If there is a facility for the service user to request the 'sealing' of sections of their electronic process notes, then similar conditions apply. The client must be informed of the potential

risks of closing off access, and the psychologist must agree that sealing is appropriate, having considered the risks of so doing and having taken advice from Information Governance leads and their Caldicott Guardian as appropriate. The psychologist must consider the clinical safety risks arising from the presence of a sealed record and ensure these are mitigated (see BPS Document: *Practice Guidelines* for further information).

Psychologists may wish to consider only keeping formal notes and taking care to ensure that speculative or provisional material is clearly identified.

4.4 Diagnosis

EHRs contain or have fields expecting information about psychiatric or other medical diagnosis, this being a vital part of many healthcare records. Some psychologists may use these diagnosis fields whilst others may prefer not to. Provision is now made in all Electronic Health Records for formulations as a standard record feature and is available for use by psychologists.

4.5 Special populations

In managing EHRs appropriately, the practitioner psychologist should be aware that, in some circumstances, standard processes of consent and confidentiality may not apply with certain service user and client groups, for example service users who may lack capacity. Additional guidance regarding consent and confidentiality is available in BPS Document: *Practice Guidelines*.

5. Validation of notes

EHRs do not have a consistent way of allowing 'counter signing' of notes. Usually the function of validating or confirming an EHR note is to prevent future editing of the note. The responsibility for the accuracy of the note lies with the individual making the note. The Society recommends that Trainee or Assistant psychologists with a first degree in psychology are not required to have all their entries into paper or electronic records validated by a fully qualified practitioner, e.g. a note to say an appointment has been changed. At the same time, it is the Supervisors' responsibility to ensure that Trainees and Assistants have their notes audited regularly and in line with their experience and competence. Supervisors must ensure that those they supervise are adhering to good practices in reporting clinical and related activities and that trainees and assistants draw their supervisors' attention to complex or problematic notes. Where countersignature is official policy, the issue should be raised with the Trust Caldicott Guardian. Further information is available in Appendix 1.

6. Training and psychology service implications

Psychology training programmes should ensure that all trainees are familiar with the use of these digital technologies and can understand the use of EHRs through their formal teaching and placement supervision.

Training should cover the nature and accuracy of record content and the fundamental role of records as an integral part of providing psychological services, as well as wider health and social care. Accurate recording of clinical concerns, assessments, formulations, interventions and outcomes should be integral to psychology training and practice. Trainees should learn that information needs to be psychometrically robust and sufficient for the multiple purposes it will be used for, such as supporting psychology practices and the evaluation and commissioning of psychology services. There is also a need for trainees to develop an understanding of the strengths and limitations of structured records and free text, the use of standard terminologies and the items characterising psychology practices and outcomes.

Psychology departments and services should ensure that staff have proper training and experience. This includes issues of confidentiality, cross-agency sharing, client access rights and accuracy of content. There are clear protocols covering key areas such as those highlighted in these guidelines. Where protocols are being developed by psychology services, it is important for the service to engage with the Caldicott Guardian, where available, from the outset to ensure that the approach taken by the psychology service aligns with local information governance processes.

Principles and practices relating to EHRs and healthcare informatics should be part of continuing professional development. There is a rapidly emerging discipline of Healthcare Informatics, with specialised training being established in the NHS. Psychologists should participate in such training so that the contributions of psychology to this discipline, and the contributions of this discipline to psychology practice, can be properly exploited.

7. Use of EHRs for research

Data held in EHR systems are recognised as a major source of information relevant in many domains of healthcare. Databases derived from these records on a very large scale – 'big data' – are being made available for research in the belief that such information will lead to fundamental insights into many health conditions, their origins and treatment. Psychological data on such a scale can produce similar benefits. These data sets, and those on a more modest scale, are subject to the same research standards as any other data set, requiring ethical approval, informed consent, confidentiality and approval of the relevant research bodies. Similarly, EHR data may be made available for audit purposes and is subject to the relevant audit standards.

References

1 *Health and Care Professions Council (2017) confidentiality – guidance for registrants.* Available at: http://www.hcpc-uk.co.uk/publications/brochures/index.asp?id=164 (accessed 20/12/2017)

2 (https://international.healthvault.com/gb/en)

3 Wachter, R.M. (2016). *Making IT work: Harnessing the power of health information technology to improve care in England.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/550866/Wachter_Review_Accessible.pdf (accessed 02/07/18)

4 Wachter, Robert (2015). *The digital doctor: Hope, hype, and harm at the dawn of medicine's computer age.* New York: McGraw-Hill Education.

5 Wang, X., A, Li & Zhu, T. (2015). Digital detection of suicide risk on social media. *International Journal of Emergency Mental health and Human Resilience, 17*, 281.

6 Department of Health (2013). *Information: To share or not to share. Government Response to the Caldicott review.* Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251750/9731-2901141-TSO-Caldicott-Government_Response_ACCESSIBLE.PDF (accessed 12/01/2018)

7 National Health Service (2015). *The NHS Constitution.* Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/480482/NHS_Constitution_WEB.pdf (accessed 12/01/2018)

8 Ross, M., Wei, W. & Ohno-Machado, L. (2014). 'Big Data' and the Electronic Health Record. *Yearb Med Inform, 9*(1), 97–104.

9 National Health Service (2014). *HIV Patient Information and NHS confidentiality in England, A policy Report.* Available at: http://www.bhiva.org/documents/Publications/Jan-2014-HIV-Patient-Confidentiality-NHS.pdf (accessed 12/01/2018)

10 *NHS. Encryption: Good practice guidance.* Available at https://digital.nhs.uk/services/data-and-cyber-security-protecting-information-and-data-in-health-and-care/cyber-and-data-security-policy-and-good-practice-in-health-and-care/encryption-guidance-for-health-and-care-organisations

Glossary

Algorithms – are the instructions (usually computer programmes or software) for undertaking specific tasks.

Anonymised – data/records are where the normal personal identifiers have been replaced by artificially-created identifiers. The identity of the individual cannot be recovered.

Artificial Intelligence (AI) – involves the simulation of human intellectual skills and processes commonly by computer systems and can involve machine learning, reasoning, rule use and self-correction.

Big Data – extremely large data sets that may be analysed to reveal patterns, trends, and associations; this could be about treatment responses or human behaviour and interactions.

Cloud Storage/Systems – storage and/or processing of information off-site on remote computer systems. These may simply hold data and provide them as needed or they may also process such data and transmit the outcomes to the practitioner.

Digitised Records – Scanned-in copies of the clinical notes or documents such as letters, reports, drawings, completed psychological or other test forms relating to a service user. Digitised records are commonly stored as images whose contents, unlike those of the EHR, may therefore be more difficult to search and process. Some documents may be derived from optical character recognition (OCR), where a computer 'reads' a document and creates an editable form.

Electronic Health Record (EHRs) – a record relating to an individual service user commonly detailing a unique identifier such as NHS number, other demographic information and information about the clinical features, activities and outcomes relating to that individual. The record may be held on a local system in a private practice or a variety of government systems including those of the NHS and Social Care. Services may implement systems aimed at paperless records or may allow some associated records to be retained on paper.

Electronic Health Record (Software) Systems – computer systems designed to capture, store and process individual service user health-related data. Examples include RiO, PARIS, SystmOne, EMIS. While some systems may be generic, they tend to be context specific, e.g. RiO for mental health. These can capture data from a variety of devices including desktops, laptops, tablets and mobile phones, as well as wearable or remote sensing devices.

Primary Care Record (PCRs) – details of the service user's care held by their General Practitioner. These details may be either held electronically or on paper or both.

Primary Care Psychological Care Records (e.g. IAPT) – EHR systems such as IAPTUS (Improving Access to Psychological Therapies System) or PCMIS (Patient Case Management Information System), designed specifically for talking therapies.

Process Notes – a detailed, sometimes speculative, clinician's record of clinical sessions.

Pseudonymised data/records are where the normal personal identifiers have been replaced by artificially-created identifiers. These conceal the identity of the individual but

enable the identity to be decoded through separately and securely stored identifiers.

Service user – For the purposes of clarity, this document uses the term 'service user' to refer to the person who is the subject of the record.

Summary Care Record (SCRs) – contains selected data from the Primary Care Record intended for secure remote access in special circumstances, for instance to provide emergency care clinicians in a hospital for instance with information about service user clinical needs.

Appendix 1 – Useful links

Adults with Incapacity (Scotland) Act 2000
https://www.legislation.gov.uk/asp/2000/4/contents

BPS Practice Guidelines
https://www.bps.org.uk/news-and-policy/practice-guidelines

Caldiott Guardians
https://www.ukcgc.uk/

Code of Ethics and Conduct
https://www.bps.org.uk/news-and-policy/bps-code-ethics-and-conduct

Freedom of Information Act
https://www.legislation.gov.uk/ukpga/2000/36/contents

General Data Protection Regulation
https://gdpr-info.eu/

Health & Care Professions Council (HCPC)
http://www.hcpc-uk.co.uk/

Electronic Health Records. Post Note Number 519.
http://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-0519

Mental Capacity Act (2005):
https://www.legislation.gov.uk/ukpga/2005/9/contents

Information Commissioners Office
https://ico.org.uk/

GDPR
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Professional Records Standards Body
https://theprsb.org/

Appendix 2 – Managing confidentiality within Electronic Health Records

Throughout there is a presumption that the default clinical record will be electronic except in specific, governed, transparent situations. Within the electronic record it is recognised that certain services may be sealed off from mainstream services – for example sexual health. Where exceptions have to be made, the following questions should help clarify local arrangements; they should be worked through with local management with the advice of others in Information Governance and if necessary the Caldicott Guardian.

1. Does the local service have an overarching policy about this reflecting the nature of the service and clinical risk issue (as might be the case in a forensic setting)?
2. If there is no such policy, consider what material may be stored outside of open access, with a summary contained in the main record? Examples for consideration include:
   - Detailed process notes from psychological therapy.
   - Trainee process notes.
   - Psychometric test material.
   - Sensitive material, for example details of childhood abuse.
   - Where client requests this, for example where their alleged abuser is also a member of staff.
3. Who does the psychologist check with locally about this if this requires clarification, recognising that the individual practitioner should not make unilateral decisions within a wider organisation and must always consult with their Information Governance lead and Caldicott Guardian?
4. Consider the options for storing such material outside of the main record, for example:
   - Password protected.
   - 'Sealed envelopes'.
   - Paper record.
5. If paper records are kept, consider where they are stored, who has the access details in case the clinician is not available, and what are the retention policies?
6. If electronic documents are password protected, who has a record of the password and is able to access the document if the clinician is not available?

The British Psychological Society
St Andrews House, 48 Princess Road East, Leicester LE1 7DR, UK
Tel: 0116 254 9568 Fax 0116 247 0787 E-mail: mail@bps.org.uk Website: www.bps.org.uk

Incorporated by Royal Charter Registered Charity No 229642

REP125/03.19