Online Meeting Services:
Information Governance Guidance

Author: Richard Trusson
Date: March 2012
Version: 1.0
# Contents

1. Executive Summary ........................................................................................................... 3
2. Background .......................................................................................................................... 4
   2.1 Disclaimer ....................................................................................................................... 4
3. Introduction .......................................................................................................................... 5
   3.1 Scope ............................................................................................................................... 5
   3.2 Terminology .................................................................................................................... 5
   3.3 Clinical Safety ................................................................................................................. 5
4. Scenarios for using online meetings .................................................................................... 6
   4.1 Introduction .................................................................................................................... 6
   4.2 Clinician to Patient Consultation .................................................................................. 6
   4.3 Multi-Disciplinary Team Meeting .................................................................................. 7
5. Information Governance Guidance ..................................................................................... 8
   5.1 Introduction .................................................................................................................... 8
   5.2 Key Considerations ....................................................................................................... 8
   5.3 Service Commissioning ................................................................................................. 8
   5.4 Meeting Preparation ...................................................................................................... 8
   5.5 Privacy Statement ......................................................................................................... 12
   5.6 Recorded Meeting ........................................................................................................ 14
6. Appendix A: Summary of Legal and Policy Obligations and Considerations ................. 17
   6.1 Using and Disclosing Confidential: Patient Information ............................................. 17
   6.2 Legal Considerations ................................................................................................... 17
   6.3 Policy Obligations ......................................................................................................... 19
7. Appendix B: Medical Records Guidance ........................................................................... 20
   7.1 Recommended minimum lengths of retention of GP records (England, Wales, and Northern Ireland) ........................................................................................................ 20
   7.2 Recommended minimum lengths of retention of hospital records (England, Wales, and Northern Ireland) ......................................................................................... 21
8. Appendix C: Good Practice Guidelines .............................................................................. 22

© Crown Copyright 2012
1. Executive Summary

The use of online meeting services within the NHS is increasing and there exists an opportunity to realise significant benefits and shift the channel by which consultations can take place. As more look to use online meeting services two key questions are emerging:

1) What is the best procurement route?
2) Where is the Information Governance guidance for using an online meeting to discuss patient identifiable information?

Advice on procurement is given in the paper published on NHS Networks¹. This outlines how, for no initial outlay and with no contractual tie in, an online meeting service can be commissioned. It also contains details on case studies showing how cash-releasing savings by NHS Derbyshire of £92 per person per meeting and by the North East SHA of £1,785 for just one meeting are being realised.

The purpose of this guide is to outline the key areas of consideration for Information Governance when presenting and sharing patient identifiable information in an online meeting. This is done by considering two scenarios; one is a consultation between a patient and clinician and the other a multi-disciplinary team meeting where patient identifiable data is discussed.

Much of the required local processes and controls will already exist in organisations to govern face to face consultations and meetings. These should form the basis of the procedures used for any online meetings.

The three key Information Governance areas that need to be considered when using online meetings are:

1) Meeting preparation – to ensure the meeting will be run safely – see section 5.4;
2) Issuance of a privacy statement – this will vary if the meeting is being recorded – see section 5.5;
3) Safe storage and data protection if an audio / visual recording of the meeting is made – see section 5.6.

All of these areas are considered in detail within this guide including the steps that need to be considered, and recommended local controls that should be implemented.

No specific clinical safety concerns have been identified when using an online meeting service to discuss clinical matters including diagnosis or treatment plans. Existing local clinical safety processes should continue to be used.

NOTE
Organisations are reminded that this document is for guidance only. It does not alter the legal responsibility of local organisations to protect patient data.

Professional legal advice should be sought if in doubt.

2. Background

The term online meeting service often refers to different solutions depending on the context in which the term is used. In this paper it covers the three types of meeting listed below.

- **Audio only**: this can be accessed from anywhere using a mobile or desk telephone; for example BT MeetMe. This type of service is good for ad hoc meetings to discuss a single topic or regular team meetings.

- **Web conferencing**: audio (Voice Over IP and telephones), webcams and desktop/application sharing: this can be accessed from mobile and desktop devices to enable access to shared information; for example using WebEx or Live Meeting. Audio only content can be accessed via a telephone and often a VOIP device.

- **Video Conferencing**: typically accessed from fixed locations using specialist hardware; for example Polycom hardware.

The use of email to conduct a consultation is not covered in this paper as it is not considered to be an online meeting. The use of email for this purpose is covered in “The Good Practice Guidelines for GP electronic patient records Version 4” published in 2011 by the Royal College of General Practitioners, the BMA and the Department of Health; see section 11.6 Using the Internet for Consulting of that document.

2.1 Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NHS Connecting for Health. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

Any party relying on or using any information contained in this document and/or relying on or using any system implemented based upon information contained in this document should do so only after performing a risk assessment. A correctly completed risk assessment enables an NHS organisation to demonstrate that a methodical process has been undertaken which can adequately describe the rationale behind any decisions made. Risk assessments should include the potential impact to live services of implementing changes.

This means that changes implemented following this guidance are done so at the implementers’ risk. Misuse or inappropriate use of this information can only be the responsibility of the implementer.

---

3. **Introduction**

3.1 **Scope**

This paper specifically considers the Information Governance process and procedures applicable to clinicians and multi-disciplinary teams conducting consultations with patients or discussing patient identifiable data via an online meeting service. It also considers the additional process controls required if meetings are recorded.

This document does not consider the local technical implementation of procedures. Those readers who are interested in infrastructure security and implementation should consult the Good Practise Guides\(^3\); see section 8. The guides are a series of informational documents which provide best practice advice in technology specific areas of Information Security and Governance.

A recorded meeting, where no patient identifiable data is presented and shared, is outside the scope of this document. The reader should review the Regulation of Investigatory Powers Act 2000 and The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 for guidance on managing such a recordings.

3.2 **Terminology**

The term clinician is used to refer to professional care providers. This includes, for example, General Practitioners, Consultants, Nurses and Health and Social Care professionals.

A multi-disciplinary team (MDT) is used to refer to a group of people who need to jointly look after the health and well-being needs of a citizen.

A consultation is taken to mean a meeting of one or more health care professionals and patient to discuss the diagnosis, prognosis or treatment of a particular case.

A meeting, in the context of this document, is taken to mean an MDT meeting, where patient identifiable data is presented, between professionals both within and outside of the NHS; this may also include consultations with the patient.

3.3 **Clinical Safety**

No specific clinical safety concerns have been raised when using online meeting services to discuss an existing diagnosis or a treatment plan. Existing clinical safety processes and guidelines should continue to be used.

Out of hours stroke solutions have explored clinical safety concerns for using online meeting type services to make diagnoses. It is suggested that readers interested in this area, at this time, contact an out of hour’s stroke service to determine what steps were taken.

**NOTE** This guide does not cover clinical safety concerns where an Online Meeting Service is used to **make** a diagnosis.

---

\(^3\) [http://nww.connectingforhealth.nhs.uk/infrasec/gpg](http://nww.connectingforhealth.nhs.uk/infrasec/gpg)
4. Scenarios for using online meetings

4.1 Introduction

Two example scenarios where patient identifiable data is presented, Clinician to Patient and Multi-Disciplinary Team (MDT) meetings, were used to help form the Information Governance guidance and controls outlined in section 5 Information Governance Guidance. When considering the guidance it became clear that not all guidance and controls need to be observed for each meeting. For example, if no audio / visual recording is made of the meeting then section 5.6 Recorded Meeting can be ignored.

Guidelines and processes laid down by the Department of Health, professional bodies and the local organisation regarding record keeping standards still apply to all consultations and meetings.

This guidance is aimed at supporting local leads wishing to start using online meeting services, but who recognise that they will need to ensure suitable Information Governance arrangements are in place, understood and complied with. The local lead could be a clinician or local data owners and IG assessors. Much of this guidance builds on arrangements which should already exist for holding face to face consultations and MDT meetings. It should be read to aid in the creation of local process and procedures for securing online meetings, consultations or MDTs where patient identifiable information is discussed.

For both the scenarios the following are suggested as core tenets;

- Existing professional standards and organisational policies for records and record keeping are followed; as for current face to face meetings.
- Informed patient consent has been obtained – this may require a meeting in person to ascertain patient capacity and any specific safeguarding controls.
- All care professionals, at least, are participating from private areas.
- The security risks of the local IT infrastructure, for example the desktop, are understood and accepted.
- The online meeting service has been assessed as meeting the required level of security and confidentiality.

4.2 Clinician to Patient Consultation

In this scenario the online consultation is taken to mean between a clinician and a patient. However it could be with an attorney for a patient under the terms of a Welfare Lasting Power of Attorney and/or patient and/or chaperone See the RCPG publication ‘A Patient Guide to GP Services’4.

The consultation is scheduled, initiated and run, by the clinician. Because the patient is participating it is assumed that patient identifiable data will be discussed. Therefore the clinician must take reasonable steps to protect this information before, during and after the meeting. For example the clinician should ensure they are sat somewhere where their conversation could not be overheard or their computer screen observed. The recommendation, and default position, is that audio visual recordings of meetings are not made. However if the meeting is recorded, then the recording must be treated as part of the clinical record (See section 7 Appendix B: Medical Records Guidance.)

A high level model of the components involved in delivering an online consultation is shown in Figure 1.

![Clinician to Patient Consultation Diagram](image)

**Figure 1 Clinician to Patient Consultation**

### 4.3 Multi-Disciplinary Team Meeting

In this scenario a multi-disciplinary team meets to consult about a patient, either with or without the patient themselves being present. Patient identifiable data will be discussed and the meeting may be recorded.

An MDT meeting typically has more factors to be considered from an Information Governance perspective, for example, who is taking part in the meeting and do all attendees have a legitimate relationship or right to be involved with discussions about that patient, see section 5.4 Meeting for more detail.

A high level model of the components involved in delivering an online MDT meeting is shown in Figure 2.

![MDT Meeting Diagram](image)

**Figure 2 MDT Meeting**
5. Information Governance Guidance

5.1 Introduction

Many of the local processes and procedures that govern online meetings will already exist for normal, face to face, consultations or meetings. These will form the default starting point for creating online meeting service specific processes and procedures.

5.2 Key Considerations

Privacy and confidentiality of the service should be key concerns when assessing a service. This covers not only the actual meeting itself but also what happens to any information associated with the meeting, for example storage or sharing of documents, attendee lists, recordings etc. ownership of the information should also be considered. If it passes to the service or is jointly owned what implications are there for data protection? For example can the service be audited to determine what information is held and who has accessed it? As a starting point organisations should look for services that have ISO27001 certification, for example the N3 offering. This certification specifies implementation of security controls customised to the needs of organisations and has been adopted by the NHS. The three key Information Governance considerations in relation to meetings are;

1) Meeting preparation – for example that the meeting will be run safely i.e. that those present have a legitimate reason to be there;
2) Issuance of a privacy statement – this will vary if the meeting is being recorded;
3) Safe storage and data protection if the meeting is recorded.

5.3 Service Commissioning

When an online meeting service is first commissioned it should be assessed as part of the normal local Information Governance process for services. A re-assessment should be completed on a regular basis as required by local process. The assessment should include the local Caldicott Guardian and SIRO to ensure data controller responsibilities are clearly identified.

5.4 Meeting Preparation

The following Information Governance controls are aimed at ensuring that;

a) Informed patient consent has been obtained
b) the correct people are invited
c) the correct people are attending
d) attendee discussions are private

---

<table>
<thead>
<tr>
<th>Item</th>
<th>Recommended Control</th>
<th>Guidance</th>
<th>Legislation / Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient Consent</td>
<td>Local procedure</td>
<td>The informed consent of patients should be sought before engaging in an online consultation. The recommendation is that this would normally be done face to face before online meetings take place, for example at the diagnosis consultation with the clinician. For one off meetings this may not be practicable and individual risk assessments should be undertaken. Points to consider when seeking consent are that the patient has the capacity to consent and they understand the risks of sharing data online. In addition the patient may want to give consent for a chaperone, family member or other carer to be involved in the meeting. See patient confidentiality at the end of this table.</td>
<td>Data Protection Act&lt;br&gt;NHS Code of Practice: Confidentiality&lt;br&gt;Care Records Management Principles</td>
</tr>
<tr>
<td>Assure legitimate relationship(s) exist</td>
<td>Local procedure</td>
<td>Highly relevant during MDT meetings. Use defined contact lists, work lists, Care Worker assignment and information in the patient records to verify legitimate relationships.</td>
<td>Data Protection Act&lt;br&gt;Common Law Duty of Confidentiality</td>
</tr>
<tr>
<td>Assure invite list</td>
<td>Use assured contact details</td>
<td>For example if inviting NHS staff only use emails on the secure NHS email system. If inviting patients use the email address or telephone number held on record.</td>
<td>Data Protection Act&lt;br&gt;DH Care Record Management</td>
</tr>
<tr>
<td>Verify meeting details</td>
<td>Local procedure</td>
<td>If multiple meetings are organised you should ensure that the attendee is being invited to the correct one. For example check the date and time and other attendees to verify a match.</td>
<td>Data Protection Act</td>
</tr>
<tr>
<td>Item</td>
<td>Recommended Control</td>
<td>Guidance</td>
<td>Legislation / Policy</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Verify Identity of participant(s)</td>
<td>Use of an assured digital identity where possible</td>
<td>While assured contact details may have been used, the wrong person may have been invited. For example the wrong J Smith was selected from the list of possible people. A local procedure should be used to check at the start of each meeting that the correct participants have joined.</td>
<td>Duty of Confidentiality Care Record Guarantee Care Records Management Principles</td>
</tr>
<tr>
<td></td>
<td>Local procedure to verify identity if un-assured digital identity is used</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verify Patient(s) Identity</td>
<td>Use of an assured digital identity where possible</td>
<td>A local procedure will be required to ensure a consistent and robust approach is taken. It may not be enough to rely on seeing that a person with the expected name has joined the meeting and further identity checks should be carried out in a similar way to those used on many telephone services.</td>
<td>Care Record Guarantee</td>
</tr>
<tr>
<td></td>
<td>Local procedure to verify identity if un-assured digital identity is used</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Who initiates the meeting</td>
<td>Local process or procedure</td>
<td>Patients should be able to request an online meeting. However it is recommended that electronic meetings are not initiated by patients. Care professionals should always initiate the meeting using the details in the patient record. Care must be taken to ensure that once started it is the verified patient in the meeting. As you would for a telephone conversation.</td>
<td>Public Service Guarantee for Data Sharing – guarding access</td>
</tr>
<tr>
<td>What protocol or procedure is used to start the meeting</td>
<td>Local process</td>
<td>There should be an agreed procedure to start a meeting. This includes selecting the chair-person who will be responsible for the meeting and would issue the privacy statement. If the meeting is recorded any additional requirements are articulated and accepted by the attendees, see section 5.6</td>
<td>Data Protection Act Public Service Guarantee for Data Sharing NHS Code of Practice: Confidentiality</td>
</tr>
<tr>
<td>Item</td>
<td>Recommended Control</td>
<td>Guidance</td>
<td>Legislation / Policy</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Where are the participants Physical location | Local procedure to verify end user locations are secure | Guidance should be issued on where online meetings should be held. This would suggest that conversations including Patient Identifiable Data are not held in public locations such as internet cafes.  
In some cases it may be required to check with attendees (as part of the protocol used to start the meeting) that they are in a private location in which they cannot be overheard. Even if using earphones meeting participant contributions may still be audible to others in the vicinity.  
Any devices used to support the online meeting services are expected to meet minimum requirements of devices used to deliver health care. | Public Service Guarantee for Data Sharing – guarding access            |
| What information about the consultation will be logged | Local process | If patient identifiable data is held by the online meeting service the NHS organisation needs to be assured this will be protected by the service.  
For example checking that meeting information is not visible to anyone who should not be able to see it. Usually controlled by only allowing those invited to a meeting to see the invite list. | Data Protection Act  
NHS Code of Practice  
Professional body codes of practice                                       |
| Patient confidentiality                     | Local procedures   | It is important to ensure that those taking part in the meeting are safeguarded for example are not coerced or otherwise unduly influenced in the answers given.  
Unlike in a face to face meeting it may be much more difficult to ensure attendees are not being pressured into providing certain answers.  
This control links back to the privacy control at the start of this table. | Data Protection Act  
NHS Code of Practice: Confidentiality                                     |
5.4.1 Example Local Procedure

Some organisations are starting to address meeting governance in a variety of ways. One example is the Video Conferencing Etiquette Guide created by the Lancashire and South Cumbria Cancer Services Network. While it does not address IG concerns directly it forms the basis for running a safe meeting. Questions can be sent to enquiries@lsccn.nhs.uk and the guide can be found at;


5.5 Privacy Statement

It is important that attendees are aware of why information is being shared or collected during the meeting and with whom, where it will be stored (if it is), and for how long. This is conveyed to the attendees at the start of the meeting or consultation by the verbal privacy notice. If this is not clear and its implications are not understood by all then cancelling the meeting should be considered.

As a minimum the verbal privacy notice used at the start of the online meeting or consultation must:

- Tell the attendees who you are / your organisation is
- What you are going to do with the information;
  - who will be able to access it
  - who it will be shared with and why

In addition it could:

- Outline how to access the data
- How the data will be kept
  - Will it be secure?
    - Will it be kept in England or within the EU?
- How long the data will be kept for

An example privacy statement for a consultation is given below;
During the course of this online meeting information may be shared or collected with other attendees about you and your treatment. Any such information will be held in confidence and its use is covered by the Data Protection Act as well as the NHS Care Record Guarantee, which governs how the NHS can use your data.

Information will only be used by and shared with those who have a legitimate need to access the information to provide health care.

*If the meeting is recorded the following should be added…*

Any recording made of the meeting will be held in England and will be treated under the same rules as the rest of your medical record.

*If the recording is to be transcribed add the following…*

A transcription will be made using the recording. Once the transcription has been added to the medical record all copies of the recording will be permanently deleted.

If you do not want information about you to be held and used in this way please make this clear to the meeting organiser prior to the commencement of the meeting.

**Figure 3 Example Privacy Statement**

Once the privacy statement is verbally issued attendees of the meeting must be given the opportunity to opt out of the meeting and withdraw any permission for use of data already captured.

If the meeting is recorded the content of this statement will vary, as outlined in Figure 3.

For example if the meeting is not recorded then no information other than required by professional guidelines, for example medical outcomes, might be captured. This should be reflected in the privacy statement.

If the meeting is recorded the statement must specifically address what will be done with the recording and agreement must be sought to continue.

The Information Commissioners Office produced clear guidance on when to use and how to write a privacy statement. This information can be found on their website at the following location –


Many online meeting services allow some form of information sharing. This can take one of two forms;

1) Screen or application sharing. In this case the information displayed on one screen is shown to all participants in the meeting.

2) Uploading documents. In this case information is uploaded to the meeting service and stored on their systems. Such content may then be downloaded by the attendees.

Of the two options using screen or application sharing presents fewer Information Governance issues and is the recommended method of sharing data during an online
meeting. The same approach to safeguarding data should be taken as would be in a face to face meeting when displaying information on a computer screen.

Uploading to an online meeting service documents with patient identifiable information introduces additional Information Governance issues because of where and how the data may be stored. Uploading information is not recommended as a general practice during online meetings. If this approach is adopted each meeting service provider must be approached to ascertain where the documents are stored and that access can be controlled in accordance with policies and professional guidelines existing at the time.

5.6 Recorded Meeting

Professional standards for documenting consultations, patient to clinician and MDT, already exist. Regardless if an audio visual recording is made of the meeting these standards must still be followed. If no audio / visual recording of the meeting is being made this section may be ignored.

The recommendation is that audio / visual recording of meetings are not generally made. Making an audio / visual recording of a meeting is expected to be the exception.

Any audio / visual recording made during a meeting that presents patient identifiable information will be classed as part of the medical record. The recording will therefore be subject to the same governance and legal constraints as any other medical record; see Appendix B: Medical Records for more guidance.

Not all traditional clinical record systems will be able to store a recording attached to the record. The recording therefore may have to be stored elsewhere, in line with regulation, with a note in the medical record pointing to the storage location. This may require additional safe guards to be taken and local policies created to control the recording and access to it.

Alternatively, if all agree, the recording may be transcribed. The transcription is then placed in the medical record and the audio, or visual recording, may be deleted if all agree the transcription is accurate and depending on policy, professional guidelines and local process and procedures.

<table>
<thead>
<tr>
<th>Item</th>
<th>Recommended Control</th>
<th>Guidance</th>
<th>Legislation / Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have patients been informed of the use to which their data may be used after it is recorded? (and given consent?)</td>
<td>IG Toolkit and local process.</td>
<td>You should provide a local process that may be in two parts – one to ‘enrol’ the patient into the online meeting service. This may need a regular review / renew. The second part would be the privacy statement issued at the start of each meeting. This covers capture of the data (the recording) what will be done with the recording and who will have access.</td>
<td>Health and Social Care Act 2001 Public Service Guarantee for Data Sharing NSH Code of Practice: Confidentiality</td>
</tr>
<tr>
<td>Item</td>
<td>Recommended Control</td>
<td>Guidance</td>
<td>Legislation / Policy</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Where is the recording held?</td>
<td>Local process and service features</td>
<td>Different countries have different legal protections for personal data. It is currently accepted practice that all patient identifiable data should be held in England. Where data is held outside the bounds of England, it is the responsibility of the organisation to ensure that appropriate controls and legislation exist in the hosting country which is comparable with the protections in place within the Data Protection Act. Even if the recording is to be transcribed it must still be protected during the transcription process.</td>
<td>Department of Health Policy Data Protection Act</td>
</tr>
<tr>
<td>Who will have access to the recording?</td>
<td>Local process</td>
<td>Because the recording is a medical record access must be controlled and restricted as with any other medical record. Only those with a legitimate need should have access.</td>
<td>Department of Health Policy Data Protection Act</td>
</tr>
<tr>
<td>How will access be controlled and audited?</td>
<td>Local process</td>
<td>At any time it must be possible to give a list of who has accessed the recording, why and when they did so.</td>
<td>Data Protection Act Care Record Guarantee</td>
</tr>
<tr>
<td>Item</td>
<td>Recommended Control</td>
<td>Guidance</td>
<td>Legislation / Policy</td>
</tr>
<tr>
<td>------</td>
<td>---------------------</td>
<td>----------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Transcribing the recording.</td>
<td>Local Policy and DH Guidance</td>
<td>It is recommended that transcription is managed on an exception basis; that is either all meeting are transcribed or none are. This process should be agreed before the meeting takes place. It should also be confirmed in the policy statement read out at the start of the meeting. If the recording is transcribed and subsequently deleted rigorous controls need to be put in place to control this process. There must be a procedure to; capture the agreement, verify that the transcription is true and accurate, audit who created it and when. It must be possible to verify that all copies of the recording have been permanently destroyed if applicable.</td>
<td>Data Protection Act</td>
</tr>
<tr>
<td>Any recordings must meet the DH Records Management code.</td>
<td>Local Process (Medical Records)</td>
<td>Under the DH Records Management: NHS Code of Practice Electronic Patient Records may not be deleted. This imposes on-going requirements for maintaining the recording and providing storage space. If the audio / visual recording is not added to the medical record, for example it is transcribed, this retention requirement may not apply. Local data guardians should be consulted.</td>
<td>Department of Health (2006) Records management: NHS code of practice</td>
</tr>
</tbody>
</table>
6. Appendix A: Summary of Legal and Policy Obligations and Considerations

NOTE

This is a summary of the stated acts and should be considered as guidance only.

Before proceeding with any service commissioning an NHS or other health care organisation must satisfy itself that all legal requirements are met. It is the organisation's responsibility to consider any regulatory requirements which may apply. Professional legal advice should be sought if in doubt.

6.1 Using and Disclosing Confidential: Patient Information

The disclosure and use of confidential patient information needs to be both lawful and ethical. Whilst law and ethics in this area are largely in step, the law provides a minimum standard that does not always reflect the appropriate ethical standards that the government and the professional regulatory bodies require. For example, the Department of Health and the General Medical Council are in agreement that, whilst there are no clear legal obligations of confidentiality that apply to the deceased, there is an ethical basis for requiring that confidentiality obligations must continue to apply. Further, where the law is unclear, a standard may be set, as a matter of policy, which clearly satisfies the legal requirement and may exceed some interpretations of the law.

6.2 Legal Considerations

There are a range of statutory provisions that limit or prohibit the use and disclosure of information in specific circumstances and, similarly, a range of statutory provisions that require information to be used or disclosed. Up to date details can be found on the Department of Health web-site at,


Generally, however, there are four main areas of law which constrain the use and disclosure of confidential personal health information.

6.2.1 Common Law of Confidentiality

This is not codified in an Act of Parliament but built up from case law where practice has been established by individual judgements. The key principle is that information confided should not be used or disclosed further, except as originally understood by the confider, or with their subsequent permission.

Whilst judgements have established that confidentiality can be breached ‘in the public interest’, these have centred on case-by-case consideration of exceptional circumstances. Confidentiality can also be overridden or set aside by legislation or by court permission.

6.2.2 Data Protection Act 1998 (DPA98)

This Act provides a framework that governs the processing of information that identifies living individuals – personal data in Data Protection terms. Processing includes holding, obtaining, recording, using and disclosing of information and the Act applies to all forms of media, including paper and images. It applies to confidential patient information but is far wider in its scope, e.g. it also covers personnel records.
Personal data is defined under the DPA98 as ‘data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or likely to be in the possession of, the data controller – and includes any expression of opinion about the individual and any indications of the intentions of the data controller or any other person in respect of the individual’.

The DPA98 imposes constraints on the processing of personal information in relation to living individuals. It identifies eight data protection principles that set out standards for information handling.

In the context of confidentiality, the most significant principles are:

- the 1st, which requires processing to be fair and lawful and imposes other restrictions, and;
- the 2nd, which requires personal data to be processed for one or more specified and lawful purposes;
- the 7th, which requires personal data to be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

There are a range of DPA98 requirements that are outside the scope of confidentiality and more information can be found at the Information Commissioner’s site [www.informationcommissioner.gov.uk](http://www.informationcommissioner.gov.uk)

### 6.2.3 Human Rights Act 1998 (HRA98)

Article 8 of the HRA98 establishes a right to ‘respect for private and family life’. This underscores the duty to protect the privacy of individuals and preserve the confidentiality of their health records. Current understanding is that compliance with the Data Protection Act 1998 and the common law of confidentiality should satisfy Human Rights requirements.

Legislation generally must also be compatible with HRA98, so any proposal for setting aside obligations of confidentiality through legislation must:

- a) pursue a legitimate aim;
- b) be considered necessary in a democratic society; and
- c) be proportionate to the need.

There is also a more general requirement that actions that interfere with the right to respect for private and family life (e.g. disclosing confidential information) must also be justified as being necessary to support legitimate aims and be proportionate to the need.

### 6.2.4 Administrative Law

Administrative law governs the actions of public authorities. According to well-established rules a public authority must possess the power to carry out what it intends to do. If not, its action is “ultra vires”, i.e. beyond its lawful powers. It is also necessary that the power be exercised for the purpose for which it was created or be “reasonably incidental” to the defined purpose. It is important that all NHS bodies be aware of the extent and limitations of their powers and act “intra vires”.

The approach often adopted by Government to address situations where a disclosure of information is prevented by lack of function (the ultra vires rule), is to create, through legislation, new statutory gateways that provide public sector bodies with the appropriate information disclosure function. However, unless such legislation explicitly requires that confidential patient information be disclosed, or provides for common law confidentiality obligations to be set aside, then these obligations must
be satisfied prior to information disclosure and use taking place, e.g. by obtaining explicit patient consent.

6.3 Policy Obligations

There are a number of policies issued by the DH and the NHS that contain guidance on protecting personal data. While these are based on the legal considerations outlined above they offer guidance specifically for a health care setting.

6.3.1 NHS Confidentiality Code of Practice

The Department of Health has produced a legal guidance document. This document lists the relevant legal and professional obligations that can apply across the whole NHS. While this is a daunting list much of the obligations are built on Administrative Law and the Common Law Duty of Confidentiality; see above. The DH document can be found at the following location:


6.3.2 Data Sharing

The following document can be used as guidance on the relevant legal issues involved with Data Sharing:

http://www.dca.gov.uk/foi/sharing/index.htm

6.3.3 NHS Care Record Guarantee

The NHS Care Record Guarantee for England sets out the rules that govern how patient information is used in the NHS and what control the patient can have over this. It is based on professional guidelines, best practice and the law and applies to both paper and electronic records. Whilst not a legal document, the Guarantee could be used as the basis for a complaint. The NHS Care Record Guarantee includes information on:

- people’s access to their own records,
- how access to an individual's healthcare record will be monitored and policed and what controls are in place to prevent unauthorised access,
- options people have to further limit access,
- access in an emergency,
- what happens when someone is unable to make decisions for themselves.

The guarantee was first published in 2005 and is regularly reviewed by the National Information Governance Board to ensure it remains clear and continues to reflect the law, professional guidelines and best Information Governance practice.

http://www.nigb.nhs.uk/guarantee

6.3.4 Privacy Statement Guidance

The Information Commissioners Office produced clear guidance on when to use and how to write a privacy statement. This information can be found on their web site at the following location:

7. Appendix B: Medical Records Guidance

The Department of Health is the authoritative source for medical records guidance. Their GP Good Practice Guide v4 published in 2011 was, at the time of writing, the latest available guidance on retention policy.

See section 4.9 Retention of GP electronic patient records and associated audit trails when a patient is no longer registered with a practice, in that document for more information.


The summary given below in sections 7.1 and 7.2 was taken from the BMA - http://www.bma.org.uk/ethics/health_records/retentionrecords.jsp

When reviewing this summary it is important to recognise that while these are guidelines laid down by the Department of Health the Data Protection Act 1998 prohibits retention of personal data for longer than is necessary. Where records are to be retained explicit reasons must be given and recorded.

7.1 Recommended minimum lengths of retention of GP records (England, Wales, and Northern Ireland)

The tables below quote the advice given in Department of Health (2006) Records management: NHS code of practice. Similar advice is provided in the schedules relevant to each of the devolved nations; however, doctors should refer directly to the relevant schedule for more detailed advice specific to each nation.

<table>
<thead>
<tr>
<th>Type</th>
<th>Retention period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maternity records</td>
<td>25 years after the birth of the last child</td>
</tr>
<tr>
<td>GP records</td>
<td>GP Records retain for 10 years after death or after the patient has permanently left the country unless the patient remains in the European Union. In the case of a child if the illness or death could have potential relevance to adult conditions or have genetic implications for the family of the deceased, the advice of clinicians should be sought as to whether to retain the records for a longer period. Electronic patient records (EPRs) must not be destroyed, or deleted, for the foreseeable future.</td>
</tr>
<tr>
<td>Records relating to persons receiving treatment for a mental disorder within the meaning of mental health legislation</td>
<td>20 years after the date of the last contact; or 10 years after the patient's death if sooner</td>
</tr>
<tr>
<td>Records relating to those serving in HM Armed Forces</td>
<td>Not to be destroyed</td>
</tr>
<tr>
<td>Records relating to those serving a prison sentence</td>
<td>Not to be destroyed</td>
</tr>
</tbody>
</table>
### 7.2 Recommended minimum lengths of retention of hospital records (England, Wales, and Northern Ireland)

<table>
<thead>
<tr>
<th>Type</th>
<th>Retention period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maternity records (including all obstetric and midwifery records, including those of episodes of maternity care that end in stillbirth or where the child later dies)</td>
<td>25 years after the birth of the last child</td>
</tr>
<tr>
<td>Children and young people</td>
<td>Retain until the patient’s 25th birthday or 26th if young person was 17 at conclusion of treatment, or 8 years after death.</td>
</tr>
<tr>
<td>Mentally disordered persons within the meaning of any Mental Health Act</td>
<td>20 years after the date of last contact between the patient/client/service user and any health/care professional employed by the mental health provider, or 8 years after the death of the patient/client/service user if sooner</td>
</tr>
<tr>
<td>All other hospital records (other than non-specified secondary care records)</td>
<td>8 years after the conclusion of treatment or death</td>
</tr>
</tbody>
</table>


8. Appendix C: Good Practice Guidelines

The Good Practice Guidelines (GPG) are a series of informational documents which provide best practice advice in technology specific areas of Information Security and Governance. The guidelines can be found online at

http://nww.connectingforhealth.nhs.uk/infrasec/gpg

For more information please contact cfh.infosecteam@nhs.net.

There are a number of Good Practice Guides that are particularly relevant to online meeting services. Three suggestions are given below.

- **Approved Cryptographic Algorithms**: useful for checking that data at rest is encrypted using recommended methods.
- **Securing Web Infrastructure and supporting services**: as most online meeting services are web based this will provide information on what to look for in a secure system.
- **Email, Calendar and Messaging Services**: online meeting services can make use of email and calendaring to organise and schedule meetings.