

“Sealed Envelopes” Briefing Paper: “Selective Alerting” Approach

Contents

Management Summary	3
Introduction	3
Patient sealing requirements in outline	3
Clinician sealing requirements in outline	3
Plans	3
1. Introduction	4
1.1. Purpose of document	4
1.2. What is meant by “sealed envelopes”?	4
1.3. “Sealed envelopes” in context	4
1.4. Progress on “sealed envelopes”	4
2. Patient “sealed envelopes”	6
2.1. Why patient sealing is being introduced.....	6
2.2. What patients will be able to do	6
2.3. Access restrictions applicable to sealed, and sealed and locked, information	7
2.4. Patient information that can and can’t be sealed	8
2.5. Duration of the access restrictions.....	9
2.6. Contemporaneous, retrospective and prospective patient sealing	9
2.7. Identifying the users that retain access.....	10
2.8. Workgroup allocation when care transfers.....	10
3. Clinician “sealed envelopes”	11
3.1. Why clinician sealing is being introduced	11
3.2. Access restrictions applicable to clinician sealed information	11
3.3. Clinicians entitled to seal and “unseal” patient information.....	11
3.4. Patient information that can and can’t be sealed by clinicians.....	11
3.5. Duration of the access restrictions.....	12
3.6. Contemporaneous and retrospective clinician sealing.....	12
3.7. Checks against abuse	13
4. Appendix A: More explanation of patient “sealed envelopes”	14
A.1 Justifiable reasons to access sealed patient information without patient consent	14
A.2 Checks against abuse	15
A.3 Informing patient sealing decisions	15
A.4 The sealing process	16
A.5 Justifications for refusing to seal information	16

Management Summary

Introduction

The NHS Care Record Guarantee¹ promises that, in future, patients will be able to request that parts of their record are kept from general view, and that in specific circumstances a clinician will be able to withhold certain types of information from a patient. These features of the NHS Care Record Service are often referred to as patient and clinician “sealed envelopes”. In September 2006, the NHS Care Record Programme Board agreed to a revised approach in order to simplify patient sealing. The underlying thinking behind the approach is that it is a team, rather than a legal organisation or individual, that should be the entity around which sealing is based. Within the NHS Care Record Service, the concept that best represents the team is a Workgroup.

Patient sealing requirements in outline

Patients, and/or their authorised representative(s)², in consultation with their clinician(s), will be able to:

- identify one or more sets of sensitive information which should be sealed from everyone other than the author and people in the same Workgroup as the sealer;
- for each set of sealed information, decide whether people other than the author and those in the same Workgroup as the sealer³ could ever gain access:
 - if “sealed”, the information could be made available to users outside the Workgroup with the patient’s permission, or through override in exceptional circumstances (e.g. public interest); OR
 - if “sealed and locked”, users from outside the Workgroup would be unaware that the sealed information existed;
- change their minds at any time and change or remove one or more of the restrictions.

Exceptionally, a patient’s request to seal can be refused, but this can only be justified in the public interest.

Clinician sealing requirements in outline

The law allows patients to see their health records. In specific circumstances, such as where the record contains confidential information about a third party, information should be withheld from the patient. “Clinician sealing” enables NHS CRS users to identify such information, so that the remaining information can be made available to the patient.

Plans

Detailed “sealing” requirements and design are being developed. Once agreed, they will be incorporated within clinical software applications to be delivered through NHS Connecting for Health. Current estimates are that this functionality will start to become available within applications from 2008/9.

¹ Available at: <http://www.connectingforhealth.nhs.uk/crdb>

² A parent/guardian is entitled (within certain limits) to make access control decisions on behalf of a child that lacks the capacity to do so, and an authorised third party such as a clinician, or proxy decision maker empowered under the Mental Capacity Act, will be able to make decisions on behalf of an adult lacking capacity.

³ For contemporaneous sealing, the sealer will be the author..

1. Introduction

1.1. Purpose of document

The purpose of this paper is to provide an overview of the planned NHS Care Record Service (NHS CRS) requirements for "sealed envelopes".

Note that although the terms "patient" and "NHS" are used in this report, the mechanisms described can also be applied in non-health care settings supported by the NHS CRS (e.g. where health and social care is provided under the single assessment process).

1.2. What is meant by "sealed envelopes"?

The NHS Care Records Service will enable users to limit access to sensitive information within patient records. A patient will be able to request that specific sensitive information within their clinical record is accessible only with their consent. This is sometimes referred to as a patient "sealed envelope". A clinician⁴ will also be able to withhold certain types of information from patients in a clinician "sealed envelope". "Sealed envelope" and "sealing" are metaphors; no information within the patient record is expected to be physically sealed or moved as a result of sealing.

1.3. "Sealed envelopes" in context

"Sealing" is one of several mechanisms for ensuring the confidentiality of patient information within the NHS Care Records Service⁵. Other mechanisms include:

- Patient consent or dissent to NHS CRS information sharing – patient dissent prevents identifiable clinical information being accessible across organisational boundaries;
- "legitimate relationships", which allow only those users with a direct relationship with the patient (such as the patient's care team) to access that patient's NHS CRS clinical records;
- Role Based Access Controls, where a person's job role and other attributes determine the NHS CRS system functions they can use and thus the type of data they can access (preventing, for example, an NHS manager from accessing identifiable clinical data);
- Alerts: alerting a privacy officer⁶ where there is a question about the appropriateness of user access; and
- Audit trails: records made when a patient's record is accessed, which are available to patients on request and to privacy officers for investigative purposes.

1.4. Progress on "sealed envelopes"

The contracts with NHS Connecting for Health contractors specified high-level "sealed envelope" requirements. After these contracts were signed, NHS Connecting for Health, with the close involvement of the NHS Care Record Service Confidentiality Requirements Advisory Group (CRAG), developed detailed sealing requirements. Additionally, a consultative implementation strategy was carried out to assess how sealing might best work within the NHS. Feedback received⁷ from some patient representatives and clinicians was that these original patient sealing requirements were too complex.

As a result, alternative approaches were proposed and assessed in order to simplify the requirements. In September 2006, the NHS Care Record Service Programme Board agreed the way forward on patient sealing. This "selective alerting" approach gained further backing from the Care Record Development Board, and other advisory bodies. It is explained in this

⁴ The term clinician is used in this report to mean a member of staff providing direct clinical care to patients e.g. doctor, nurse, therapist etc. The results of the "sealed envelope" implementation strategy suggest that a somewhat wider group of users could carry out clinician sealing i.e. qualified health professionals with a legitimate relationship.

⁵ The Care Record Guarantee sets out how patient information will be protected, including both patient and clinician "sealed envelopes".

⁶ The term "privacy officer" is used to refer to a member of staff within an NHS CRS user organisation with responsibility to act on behalf of a Caldicott Guardian, maintaining security and patient confidentiality, and dealing with security issues raised through use of the NHS CRS by staff in that organisation.

⁷ Received during a "sealed envelope" risk assessment project, and to a lesser extent, during the implementation strategy.

briefing paper; a balance has been struck between flexibility for patients to express access restrictions, and the need to limit complexity so that computer and people systems can work in practice.

Once elaborated, the detailed sealing requirements and design for the “selective alerting” approach will be published and agreements reached with contractors on implementation timescales. Current estimates are that sealing functionality will start to become available within applications from 2008/9. However, some suppliers already have proprietary controls built into their software and can already provide some patient sealing functionality.

Readers should be aware that the detailed requirements explained in this paper are still being elaborated and are therefore subject to change.

2. Patient “sealed envelopes”

2.1. Why patient sealing is being introduced

Most patients are happy for their health information to be shared within health care teams on a “need to know” basis. However, patient surveys⁸ show that some people would prefer that particularly sensitive information (e.g. the record of a teenage termination of pregnancy) is not shared routinely amongst health care practitioners. Furthermore, the common law⁹ allows patients to place restrictions on disclosure of their confidential health information. Patient sealing and consent/dissent to information sharing will be the primary means for achieving this within the NHS CRS. Where no such access restrictions are expressed, the patient’s consent to information sharing for the direct provision of care and treatment of the patient on a need to know basis will be inferred. This approach will be explained to patients through a national publicity campaign, backed up by information provided in face-to-face contacts between NHS staff and patients.

2.2. What patients will be able to do

Patients, and/or their authorised representative(s)¹⁰, in consultation with their clinician(s), will be able to:

- identify one or more sets of sensitive information which should be sealed from everyone other than the author and people in the same Workgroup as the sealer;
- for each set of sealed information, decide whether people other than the author and those in the same Workgroup¹¹ as the sealer¹² could ever gain access:
 - if “sealed”, the information could be made available to users outside the Workgroup with the patient’s permission, or through override in exceptional circumstances (e.g. public interest); OR
 - if “sealed and locked”, users from outside the Workgroup would be unaware that the sealed information existed;
- change their minds at any time and change or remove one or more of the restrictions.

Where information is recorded in particularly sensitive care settings such as mental health, many patients might be expected to choose to have it sealed and locked¹³. However, some patients may prefer to simply seal sensitive information in case it becomes relevant to future care provided by other teams.

The patient would be able to ask anyone with the appropriate role-based access control privileges¹⁴, and access to the relevant information, to seal the data. If the patient chooses to “unseal” the information, then the user would have to first access the sealed data, and this could either be done by a member of the Workgroup with permission for access, or more unusually, through someone outside the Workgroup but with the patient’s permission (in which case an alert is generated – see section 2.3).

A patient will be able to change his/her mind to:

- seal, or seal and lock, data that were not sealed when recorded;
- unseal – removing the restrictions on a set of data that is sealed or sealed and locked
- unseal some of the data that are sealed, or sealed and locked¹⁵;

⁸ See, for example, the results of the Consumer Association survey at:

http://www.connectingforhealth.nhs.uk/publications/all_images_and_docs/swc.pdf

⁹ This has become clear through recent interpretations by the Department of Health, the General Medical Council and the courts of the common law of confidence - “judge-made” civil law that has been built up over centuries.

¹⁰ A parent/guardian is entitled (within certain limits) to make access control decisions on behalf of a child that lacks the capacity to do so, and an authorised third party such as a clinician, or proxy decision maker empowered under the Mental Capacity Act, will be able to make decisions on behalf of an adult lacking capacity.

¹¹ If the sealer is associated with more than one workgroup they must select the appropriate one for this purpose (see section 2.7).

¹² For contemporaneous sealing, the sealer is also the author. See section 2.6...

¹³ This could be the default adopted by software supporting those environments.

¹⁴ A RBAC Activity has been created for this purpose, and would be assigned to people with the necessary understanding and skills to advise patients and seal data.

¹⁵ Note that the patient may have to approach different clinicians in order to unseal all of their data since a clinician is only able to unseal the data to which they have access.

- make sealed data become sealed and locked, or vice versa¹⁶.

2.3. Access restrictions applicable to sealed, and sealed and locked, information

When a user attempts to access sealed information that (s)he created, or is a member of a Workgroup with access permission, the NHS CRS software will initially withhold the information, indicate (e.g. through an icon) that information has been withheld, and if the user seeks to view the information, then display a message such as:

- A. "you or one of your colleagues has 'sealed' information for the patient; do <X> to view this information" or
- B. "you or one of your colleagues has 'sealed and locked' for the patient; do <X> to view this information".

So the author, and users from a Workgroup with permission to access the restricted data, and with the appropriate role-based access control privilege to open sealed information, will be able to gain access to sealed, and sealed and locked, information.

When a user attempts to access information that was recorded by another Workgroup and sealed (but not locked) by the patient, then the NHS CRS software will withhold the information and display an icon. If the user proceeds (perhaps by clicking on the icon) then a message will be displayed such as:

- C. "information recorded by another team providing care to the patient has been 'sealed' by the patient. You can access this information on this occasion with the patient's explicit permission. You should seek advice before accessing the 'sealed' information without permission; it can only be justified where the law specifically requires, or where the public interest outweighs the patient's right to confidentiality¹⁷."

To view the information, do <Y>, but be aware that an alert will be sent to a privacy officer within your organisation, and if you are found to have accessed this confidential information inappropriately, disciplinary action will be taken against you for breach of patient confidentiality."

A user who accesses sealed data after being displayed message C gains temporary access to sealed data whilst logged on to the system. If they, or any of their colleagues, subsequently try to access the sealed data, they will again have to justify the access, and another alert will be raised. The temporary permission allows access to any data that has been sealed for the patient¹⁸, but not sealed and locked data. The alert is sent to an authorised person within the user's organisation with a responsibility for protecting confidentiality. This is to deter staff with no justification for access from pretending that they have explicit patient consent or that they have a legal reason for access. It is expected that such alerts should be relatively rare.

When a user attempts to access information that was recorded by another Workgroup and sealed and locked by the patient, the information will be withheld. No message will be displayed. No override is possible. The user will not be aware that information has been withheld. The sealed and locked data would be accessible only by the author, the Workgroup assigned to the information (see section 2.7), or a user servicing a subject access request for the patient (which triggers an alert).

Note that no icon or message will be displayed where the patient has sealed some data (e.g. a mental health episode) and the user is not attempting to access it, but instead is accessing another part of the electronic record (e.g. the patient's screening appointments).

The rules above apply whether the user is attempting to output information to a computer screen, or to a paper report.

¹⁶ The Workgroup assigned from this change would be the sealer's Workgroup.

¹⁷ The access restrictions are not absolute; clinicians will be justified in "breaking the seal" in exceptional circumstances (see Appendix A.1).

¹⁸ assuming that the user has role-based access control permissions for access

The processing rules are slightly different for decision-support software:

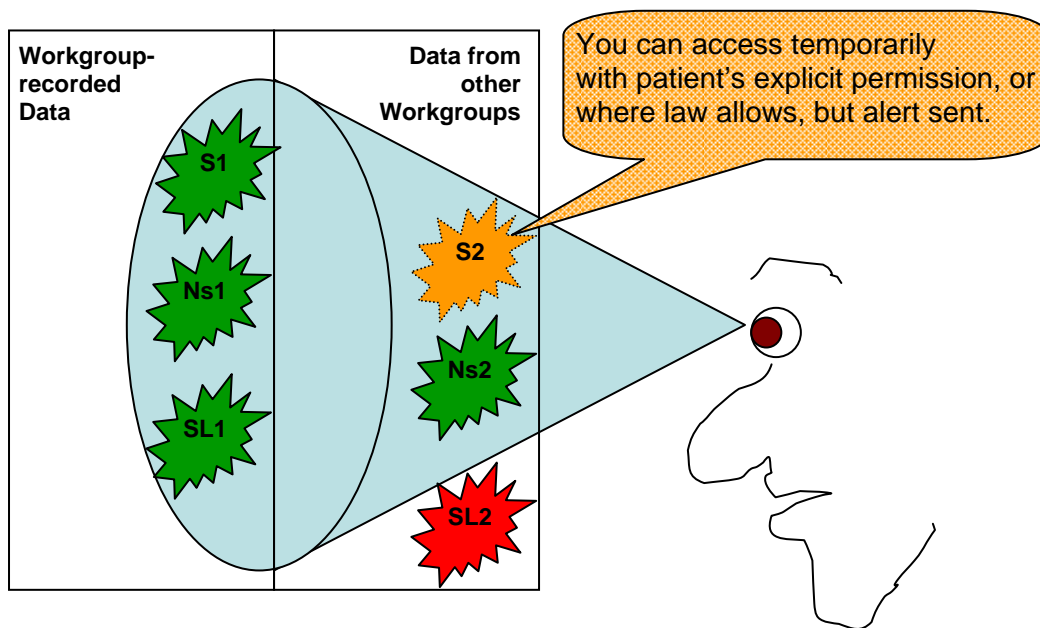
- If the user currently¹⁹ has access to all the 'sealed' and 'sealed and locked' information that is encountered during decision support processing, then the decision support software operates as if no information was sealed.
- Decision support software will ignore sealed and locked information to which the user does not have access,
- If the decision-support software encounters any sealed data to which the user does not have access, a warning will be displayed to the user that no decision-support advice will be given; this is to prevent such software being used to infer what information has been sealed by the patient.

[Drafting note: the above behaviour for decision support software is still to be confirmed.]

The information which the user is attempting to access may be held within the patient's Summary Care Record or within their Detailed Care Records; either way the controls would be the same.

The above access rules are illustrated in the diagram below, where:

- the user is attempting to access data recorded both by their own and other workgroups, including:
 - some data that is not sealed (Ns1 and Ns2)
 - some data which have been sealed (S1 and S2)
 - some data which have been sealed and locked (SL1 and SL2); and
- **green** data are accessible;
- **orange** data are accessible only with patient permission, or override; and
- **red** data are not visible or accessible in any way by the user.



2.4. Patient information that can and can't be sealed

A patient will be able to have any part of his or her Summary or Detailed Care Record sealed or sealed and locked, other than:

- a. Patient identifying data and demographics (such as name and address²⁰) and certain other specific data items which should never be "sealable" by a patient²¹;

¹⁹ The user may currently have access either by being a member of a relevant workgroup or by having gained access during their session thus triggering an alert.

²⁰ Other means of protecting sensitive addresses (e.g. for people in refuges) are planned.

²¹ Exemplar items that would not be "sealable" if held are: a violent patient indicator, immigration status, and entitlement to NHS treatment. Legal Status is not excluded because a patient may be classified under some sections of the Mental Health Act that can be sealed.

- b. Any information within the record that the patient is not entitled to see, such as confidential third-party information (see section 3)²²;
- c. Data which is not feasible to seal (see below);
- d. Where the patient lacks mental capacity and the clinician judges that “sealing off” the information is not in the patient’s best interests; and
- e. Information which, in the overriding public interest, should not be sealed, as judged by the clinician reviewing the sealing request (see Appendix A.5).

There are a number of potential NHS CRS constraints of type c) above. It will not be possible to seal:

- individual items that only make sense within a logical grouping of data²³;
- items that are component parts of a standard “unit of sealing”²⁴;
- part of an image (e.g. part of a letter that has been “scanned in”);
- patient information that was recorded in application software before the NHS CRS was introduced with LSP record structures that can’t reasonably²⁵ support sealing.

Within the NHS CRS, some information (e.g. about an out-patient appointment) recorded within a patient’s Detailed Care Records will be automatically copied onto the patient’s Summary Care Record, and may be copied to other parts of the Detailed Care Record. Therefore multiple copies of the information may exist. Some may be derivations rather than direct copies.

All direct copies and derivations of information should be “sealable” as part of one sealing request from the patient, and the patient’s “sealing request” should be applied to all copies of the information. The NHS CRS should be designed so as to ensure that the sealing instructions that apply to information in one copy of the record, are automatically preserved if that information is subsequently copied.

2.5. Duration of the access restrictions

When a patient seals, or seals and locks, the restrictions apply until the patient changes their mind, or dies. Access to a dead person’s records is still subject to normal access controls²⁶, but the patient’s sealing restrictions no longer apply.

[Drafting note: the required actions following a patient’s death are to be confirmed.]

2.6. Contemporaneous, retrospective and prospective patient sealing

It is envisaged that sealing will be either “contemporaneous” or “retrospective”, but not, prospective. With contemporaneous sealing, patients would be asked whether they wish to seal information as it is recorded during the clinical process, in settings where information is likely to be considered to be sensitive. For example, when a patient attends a mental health clinic they can be informed about how their information will be shared, and about their options for limiting information sharing, including sealing. As information is recorded, it can be sealed. This means that particularly sensitive information is sealed immediately, with advice from clinicians that will understand the clinical implications of what is being done.

However, some patients may be sensitive about information that is already within their record, and will want an opportunity to review their record and seal retrospectively. In general, it is expected that retrospective sealing will be done as part of a special consultation with a clinician (e.g. the patient’s general practitioner). The patient and clinician will be able to review the record together and decide what information can and should be sealed. The

²² Note that it is possible in exceptional circumstances for information to be withheld from both the patient’s representatives (e.g. a child’s parent) and NHS CRS users (e.g. the child’s GP). This might be achieved by applying both a patient and clinician seal, or by other system design approaches.

²³ For example, it would not be feasible to seal an appointment time, without also “sealing off” the appointment date.

²⁴ It is expected that there will be standard units of clinical data that can be sealed, which are likely to be similar to the standard clinical messages exchanged within the NHS CRS e.g. “clinical statements”.

²⁵ It is not yet clear how much (if any) historic patient data that pre-dates NHS CRS won’t be “sealable”; the aim will be to make as much information as possible “sealable”. However, suppliers will be able to make a case to NHS CfH where it is extremely difficult (and therefore disproportionately costly) to seal certain types of information, and a solution will be agreed on a case-by-case basis. Note that all entries in the Summary Care Record will be “sealable”.

²⁶ These include role-based access controls, and legitimate relationships (see section 2). The dead patient’s record would be accessible on a “need to know” basis to NHS CRS users, and so unless specifically authorised, it would not be disclosed to relatives and friends of the dead person.

patient should make their sealing request to the team that originally recorded the data, thereby providing the appropriate workgroup with continuing access to the sealed, or sealed and locked, data. If the patient is no longer receiving care from that team, they can ask another team with access to the relevant data to do the sealing. The sealer's Workgroup will be the one that is assigned access to the data. The original author also retains access.

It will not be possible for patients to seal prospectively. A patient's sealing request can apply to data that have been recorded, or are being recorded, but a patient cannot expect their request to be interpreted and applied to potential future information which is not yet known; there are problems with reliably interpreting a patient's wishes with regard to future information.

In all of the above scenarios, it is the patient that requests that information is sealed. A potential exception to this was investigated: whether information within a health record that revealed a patient's previous gender should be automatically sealed in order to meet the requirements of the Gender Recognition Act 2004. However, after further investigation, it is now clear that such patients can protect such information if they wish e.g. through sealing and/or patient dissent.

For further explanation of the sealing process, see Appendix A.4.

2.7. Identifying the users that retain access

The author of any data always retains access.

When a patient seals or seals and locks data, the sealer's Workgroup must be associated with the sealed data. In many instances, the system will be able to automatically assign the user's Workgroup. However, if the user is part of more than one team, they may have multiple Workgroups associated with the User Role Profile²⁷ they selected when they logged on to the system. If so, when sealing, the user will be prompted to select the right Workgroup to retain access to the sealed, or sealed and locked, data.

2.8. Workgroup allocation when care transfers

If a patient transfers from one general practice to another, the new general practice essentially inherits the duty of care from the previous practice, and so will gain any rights of the previous practice to access sealed data within the patient's record. However, the new practice does not inherit access rights to sealed and locked data, and this is something that patients need to understand when first sealing and locking.

If a patient is referred, and the referrer wishes to include information that the patient has sealed within the referral, then they must gain explicit patient consent, and the information included should be marked as "sealed". The application receiving the referral identifies the Workgroups with permission to access the sealed data. However, referrers should not include any sealed and locked information within referrals.

Workgroups should very rarely close, although they will change in membership and may become part of new organisations (e.g. when new legislation creates new NHS legal entities). However, allowance should be made for such an exception. Therefore, it is planned that special rights will be granted by a national authority to a small number of "super-users" who will be able to reassign sealed, or more likely sealed and locked, data to a new Workgroup.

²⁷ A User Role Profile identifies the user, the organisation to which the user is accountable, and the job role the user performs. Users that carry out more than one job role can have more than one User Role Profile, but must select the User Role Profile for which they are acting before accessing patient data.

3. Clinician “sealed envelopes”

3.1. Why clinician sealing is being introduced

The law allows patients to see their health records. Most patients are entitled to a full copy of their paper and electronic records, but in a small minority of cases, specific information should be withheld from the patient and/or their representatives (e.g. relatives, carers). The aim of clinician sealing is to enable NHS CRS users to identify information within a patient’s NHS CRS records that should not be disclosed, so that the remaining information can be made available to the patient.

3.2. Access restrictions applicable to clinician sealed information

When a NHS CRS user attempts to display or print patient information that has been sealed by a clinician, the sealed data will be withheld initially. A marker (e.g. a clinician “sealed envelope” icon) will be displayed. The user can then opt to display the data which were initially withheld. The information is withheld initially in case the screen is in view of the patient or patient representative. Clinician sealing prevents patients from seeing inappropriate data, and is not a means of one clinician preventing patient information being accessed by other clinicians.

Reports printed from the NHS CRS to satisfy a patient’s subject access request generally²⁸ will omit data that have been sealed by a clinician, but information sealed by clinicians is not withheld from printed reports for clinicians²⁹. Currently, the law does not require patients to be informed that information within their records has been withheld from them, but regulations may be about to change³⁰.

Clinician–sealed data will also be withheld from the patient if he or she gains direct electronic access to their Summary Care Record through *Healthspace*.

3.3. Clinicians entitled to seal and “unseal” patient information

Clinician sealing and “unsealing” will be carried out by NHS CRS users with appropriate role-based access control privileges and a legitimate relationship to the patient. Consultation has been undertaken as part of the “sealed envelope” implementation strategy to establish which types of clinicians (e.g. doctors, nurses, physiotherapists?)³¹ should be entitled to carry out clinician sealing. Any qualified health professional with a legitimate relationship with the patient can subsequently remove or otherwise change the access restrictions specified by the sealing clinician.

3.4. Patient information that can and can’t be sealed by clinicians

There are several types of information which justify clinician sealing, and one or more of these types may be sealed off in a patient’s record:

- Confidential third-party information;
- Information that is likely to cause serious harm to the patient or another person;

²⁸ Although not data withheld temporarily before a clinician has a chance to speak to the patient, or information that the patient doesn’t want to know (see section 3.4).

²⁹ e.g. clinical details of a patient to be seen by a clinician doing a ward round

³⁰ The Health Records and Data Protection Review Group (HRDG) has recommended to the Secretary of State that patients should be informed that information has been withheld in the exceptional circumstance that information is withheld in response to a subject access request but not the specific reason why. The full HRDG report has not yet been published but is expected to be subject to public consultation. For more information about the HRDG and its work, see:

http://www.dh.gov.uk/PolicyAndGuidance/InformationPolicy/PatientConfidentialityAndCaldicottGuardians/AccessHealthRecordsArticle/fs/en?CONTENT_ID=4100545&chk=u9pOYE

³¹ This issue will be raised with professional and regulatory bodies in the light of the description of “appropriate health professional” in SI 413, The Data Protection (Subject Access Modification) (Health) Order 2000 (see <http://www.legislation.hms.gov.uk/si/si2000/20000413.htm>). Doctors often will be the appropriate health professional, but which other types of health professional should be entitled to make these judgements? The Act defines “health professional” to include many different professions including, for example, music therapists (see <http://www.hms.gov.uk/acts/acts1998/80029--j.htm#69>), but the professional bodies may wish to limit the scope of “appropriate health professionals” who can seal and “unseal” data.

- Where a child, or an adult lacking the capacity to take decisions for him or herself, has asked that the information should not be disclosed to a responsible person who would otherwise be entitled to see it (e.g. parent)³².
- Information that should be held back temporarily until a clinician has had a chance to explain its significance to the patient (e.g. a potentially alarming test result); and
- Information withheld because a patient explicitly asked not to know about it.

The first three bullets are exceptions recognised by the Data Protection Act 1998. The remaining bullets can be justified through the clinician's duty of care to the patient; these are considered sufficient reasons to withhold information (e.g. if the patient attempts to access their Summary Care Record through Healthspace) but not where the patient submits a subject access request under the Data Protection Act.

The NHS CRS will allow most³³ parts of a patient's record to be sealed by a clinician; it is a matter of judgment as to whether clinician sealing can be justified in each case. Whenever a clinician seals, one or more of the justifiable reasons above for sealing must be selected, and a free-text reason may be recorded.

3.5. Duration of the access restrictions

For most types of information being sealed, the clinician can choose to specify a date when the access restriction will end automatically. Otherwise, the information will remain sealed until it has been "unsealed" by a clinician (see section 3.3).

The exception to the above is where information is being withheld temporarily until the clinician has had a chance to explain its significance to the patient. In such cases, the NHS CRS will warn clinicians that the information will be withheld for a national standard³⁴ number of days and then be automatically "unsealed". It will be possible for a clinician to subsequently "unseal" it before the sealing period ends.

Unlike patient sealing, the restrictions will not expire automatically when a patient dies, because there may still be a need to prevent the patient's friends, relatives or carers³⁵ from seeing the restricted information.

3.6. Contemporaneous and retrospective clinician sealing

It is envisaged that sealing will be either "contemporaneous" or "retrospective". With contemporaneous sealing, information that should be withheld is identified at the time of data entry, and sealed immediately.

A clinician identifying inappropriate third party or harmful data already within a patient record may decide at any time to seal it off, so there is also a requirement for retrospective sealing. There are also specific circumstances where a patient is likely to see their own record, and each of these could trigger a retrospective review of a patient record:

- a subject access request made by, or on behalf of, a patient; and
- an appointment being made with a patient who wishes to retrospectively seal information within their health record, because such consultations will almost inevitably involve the patient looking at their own record.

Retrospective clinician sealing is potentially resource intensive³⁶, and will add delays to the above processes. Therefore, the ideal would be for contemporaneous clinician sealing to become the norm so that there is rarely a need for these retrospective reviews.

³² This category is included to meet the requirements of the Data Protection Act 1998 regulation: Data Protection (Subject Access Modification) (Health) Order 2000 (SI No.413), Article 5 (see <http://www.opsi.gov.uk/si/si2000/20000413.htm>).

³³ The same practical sealing constraints identified in section 2.4 also apply here.

³⁴ The initial national standard period proposed by CRAG is 4 weeks. This will be a period for the NHS CRS as a whole, and subject to change if policy changes.

³⁵ However, such people may have a legal right of access under the Access to Health Records Act 1990.

³⁶ Note that this is already a legal requirement when processing subject access requests, although research has shown that many NHS organisations do not screen records routinely.

3.7. Checks against abuse

A privacy officer (such as a Caldicott Guardian) will be able to review cases where clinicians working for the organisation have sealed patient data. Access restrictions applied by a particular clinician can be reviewed, and unusual patterns of sealing may be investigated and followed up with the clinician(s) concerned. National guidance will be produced to explain to Caldicott Guardians and privacy officers what is expected from them in order to monitor and prevent abuse.

4. Appendix A: More explanation of patient "sealed envelopes"

A.1 Justifiable reasons to access sealed patient information without patient consent

A user will be unaware of, and unable to access, patient's sealed and locked data unless they are the author, a member of a Workgroup with access, or are servicing a patient's subject access request. There are no facilities to "break the seal" and gain access to sealed and locked data.

However, the rules for sealed data are different. There will be circumstances in which the clinician is unable to ask the patient, or the patient refuses to provide them with permission to access sealed data. Generally, clinicians will be able to work with just the information that is available. However, there may be times when a clinician feels he or she can justify "breaking the seal" and see the restricted data without the patient's consent. If the clinician has the necessary system privileges³⁷, he or she will be able to select a justifying reason (see below), and gain access to the information that has been withheld.

If the patient has sealed data and refuses to give permission for that data to be accessed, a clinician is only entitled to gain access for one of the following reasons³⁸:

- Public interest³⁹;
- Access is required by statute; or
- A court order demands access.

[Drafting note: further legal advice is currently being sought on the above list in light of the Mental Capacity Act 2005 (which is to be introduced in 2008). It is possible that the above list of reasons will change.]

If the patient has sealed data and it is not practical to ask permission to view that data then access must also be justified through one of the above three reasons. The justifying reason must be selected before access is given, and a free text reason may also be recorded.

Best interests of the patient is not sufficient on its own to justify access, even if the patient is unconscious, but it can be taken into account in a judgement to access information and breach confidence in the public interest. A public interest defence will be applicable very rarely⁴⁰. It relies on the clinician being able to justify the breach of patient confidence in the interests of the public, such as a genuine risk that specific individuals, or the public in general, will be harmed if the clinician is unable to see the withheld information within the patient's record. This is a judgement which involves weighing up the public good against the rights of the patient to confidentiality. Whenever practical, such judgements should be reached after conferring with clinical colleagues, and in the light of national guidance⁴¹. When such a decision is taken in the public interest then the reasons for the decision should always be documented within the NHS CRS and normally explained to the patient.

Where a patient consents to a medical report being provided (e.g. to an insurer), a full report will usually be provided, including, if relevant, any sealed, or sealed and locked, information to which the doctor has access. If sealed, or sealed and locked, information is to be included in the report, the patient should be made aware that it has been done. However, The Medical Reports Act does not prevent the doctor withholding information that may be relevant as long as it is made clear that information has been withheld. However, although the patient has a right to ask for inaccurate or misleading information to be amended, the doctor ultimately decides what is relevant to a report, and has no obligation to send an incomplete report...

³⁷ They must be granted the rights through their User Role Profile which they declare when they log on, and must also have a "legitimate relationship" with the patient. A legitimate relationship will exist between a patient and an individual or team providing a direct service to the patient.

³⁸ The list of justifications has been agreed the Department of Health and its lawyers.

³⁹ Where the public interest is judged in the case to override the competing duty of confidence.

⁴⁰ This is particularly true in this case, because the user will not know what information has been withheld. This makes it difficult to assess the value of the information to the public good. Nevertheless, the public interest may prove to be justifiable in exceptional cases, and so must be enabled through the NHS CRS.

⁴¹ to be produced.

Note that data that have been sealed will be accessible without patient consent as long as no *identifiable* patient information is revealed. For example, a management report showing just the annual total number of terminations of pregnancy taking place in a trust would take account of any that have been sealed.

A.2 Checks against abuse

There will be checks against abuses. When accessing sealed data without consent, the clinician must record one of the reasons identified above, and may also record a free-text reason for access. The NHS CRS will trigger and send an alert message with the information about the access to a privacy officer representing the organisation to which the NHS CRS user is accountable (typically, the clinician's employer). Alerts should be investigated, and disciplinary and possibly legal proceedings will follow if there has been an unjustifiable breach of patient confidentiality. Users will be warned of these consequences prior to "breaking the seal".

Sealed, and sealed and locked, data can only be unsealed – in other words, have the seal removed - by someone with permission to access that data i.e.:

- a member of a Workgroup with access permission; or
- in the case of "sealed" data, someone with temporary patient permission for access (the recording of which will have triggered an alert).

Therefore, it will not be possible for a user without permission to access sealed, or sealed and locked, data to unseal it in order to by-pass the controls.

Another means of deterring a user from abusing their access privileges by falsifying a patient's consent would be to routinely inform the patient every time their "sealing instructions" change. However, currently there are no standard NHS CRS mechanisms for automatically sending such communications to patients. When "sealed envelopes" are introduced, it is proposed that patients will be informed of sealing changes by an electronic message if the patient is a registered user of Healthspace. The Healthspace communication to the patient, and the alert to the privacy officer when users add themselves to the access permissions list, are checks against NHS CRS users and other people claiming falsely to be the patient.

Privacy officers will also be able to analyse audit trails of changes to patient sealing instructions in order to identify unusual / suspicious patterns of sealing events. Patients will be able to request access to audit trails.

A.3 Informing patient sealing decisions

Whilst a patient has a legal right to place restrictions on access to his or her confidential information, a clinician has a duty of care to the patient to make clear the potential consequences of their decisions. Patients should be made aware of how their confidential information is protected and shared, and the extent of their rights to restrict access to that information. A national publicity campaign aims to provide this information, but inevitably this alone will not mean that every patient is sufficiently informed to make decisions about restricting access to their data. Individual clinicians must also be prepared to provide information, and/or to direct patients towards sources of information.

Patients need to recognise that they are not able to seal certain information (see section 2.4), and that the law requires or empowers the NHS to disclose information in certain circumstances (see Appendix A.1) even if sealed. Patients must also be advised of the potential implications that may result from specific decisions to restrict access. They should understand that clinicians using NHS CRS will be alerted that relevant patient information has been sealed, but this may not mean that the clinician will always ask about the information that has been sealed. Patients must be made aware that sealing decisions place some responsibility on them to inform clinicians whenever they think that information withheld from their electronic records may be relevant. Every patient considering whether to seal sensitive health information needs to be made aware of how their choices could affect their future health (or perhaps the health of others). Sealing, and even more so sealing and locking, introduces the risk that:

- inappropriate treatment options are offered to the patient; or
- appropriate treatment options are not offered to the patient.

A clinician may wish to seek the advice of colleagues to ensure that a patient is properly informed and advised of the potential implications of their sealing request.

If a patient with mental capacity understands that their request to seal information may be harmful to their health, and despite this still wishes to go ahead, then under common law, the patient's decision should be respected. Clinicians will be able to, and will be advised to, record their concerns about such decisions. However, a request may be refused where it could impact adversely on the health and welfare of others (see Appendix A.5).

Free-text notes may be recorded, and sealed, within the NHS CRS of the patient's decision-making process and the implications identified by clinicians.

A.4 The sealing process

Patient sealing can be broken down into a number of logical steps, shown in the table below. How, and by whom, these steps are carried out will differ depending on whether the sealing is contemporaneous or retrospective. A "sealed envelope" implementation strategy has been carried out to investigate how sealing could work in practice.

	Step	Description	By
1	Request	Patient requests that certain information is sealed, or sealed and locked. With retrospective sealing, this step is likely to involve the patient reviewing their record, and if so it may need to be preceded by clinician sealing (see section 3) to prevent the patient viewing inappropriate data.	Patient
2a	Validate request is implementable	NHS checks that there is no law ⁴² preventing these data being sealed, and that the request can be applied in NHS CRS (i.e. it is not data of a type that has been marked as "unsealable", and no system constraints prevent it).	NHS CRS user (Clinician or non-clinician)
2b	Validate public interest acceptability	Checks that the request does not pose a danger to others (e.g. risk to public health, epilepsy for a patient intent on driving, history of abuse endangering children). This is a judgment: the public interest may be a justifiable defence for refusing a patient's request, but there is no law requiring refusal in such situations.	Clinician
3	Advise	The patient is advised of potential consequences of the request on their future care, health and well-being, and the implications of the choice between sealing, and sealing and locking. If the request poses a potential threat to the patient's health, this is not a reason to refuse the request; under common law, a patient is entitled to make decisions that could adversely affect their health.	Clinician
4	Agree	If the action to take, and the precise set of data to be sealed, has not already been unambiguously identified through steps one to three, this needs to be agreed.	Patient and NHS CRS user (clinician or non-clinician)
5	Seal / seal and lock	The agreed data are sealed/sealed and locked on the NHS CRS using an NHS CRS system function.	NHS CRS user (clinician or non-clinician)

A.5 Justifications for refusing to seal information

In exceptional circumstances, refusing a request to seal, or seal and lock, may be justifiable in the public interest, normally because there are identifiable serious risks to third parties. Any refusals should be recorded, and be viewable whenever the patient retrospectively seals information. National guidance will be issued on this subject.

⁴² Note that currently no such law has been identified. It would be possible, for example, to seal, or seal and lock, a termination of pregnancy even though there is an Abortion Act requirement to report the details of patients undergoing a termination to the Secretary of State. The Abortion Act reporting function would output the sealed data because the access is required by law. However, in the case of sealed and locked data, the report could only be generated by a user in a Workgroup with access to the data.

Suppose Tom, a patient with a history of abusing children, realises that notes on this abuse are kept within his GP records. He goes to his GP and asks for such records to be sealed and locked. The GP should weigh up Tom's claim to keep private his past records (which might affect how staff treat him), against the potential danger to the public (e.g. a child at risk from abuse) if this information is concealed. Previous common law judgments suggest that the GP is likely to be justified in refusing Tom's request in the public interest.

It might also be justified in the public interest a patient's request to seal or seal and lock data which concerns information about, for example:

- patient violence that indicates that the patient is a threat to staff and other patients; and
- a diagnosis that indicates that the patient poses a serious risk to the health of others.