# Requirements for the Mentcare system

A system to support the clinical management of patients suffering from mental illness

## Preface

Many users of previous editions of this book have asked me if I can suggest where they can find examples of real requirements documents that they can use to support some of the material on this topic that I have covered in the book. I have not been able to do so as system requirements documents are usually commercially confidential and neither the system buyer or the system developer wishes these to be made public.

I have developed this requirements document by reengineering the requirements of a medical records system from my knowledge of that system and requirements documents in general. This example system is based on a real patient information system that was in use in a number of health authorities in the UK. The requirements document for this system is commercially confidential so this is not the actual document that was used in the system procurement and development. For reasons of commercial confidentiality, I have changed the name of the system and have not included information about specific system features that relate to the use of the system in a particular health authority or hospital.

For non-UK readers, you should be aware of the following:

1. The UK has a National Health System where all citizens are entitled to healthcare that is free at the point of delivery. Consequently, all citizens have a unique national health number. While some people do have private health insurance, the system is not insurance based so this document has no mention of costs or billing issues.

2. The UK has a Data Protection Act that sets out the protection that must be implemented on personal information held by organizations. All personal information systems are constrained by this Act.

Real requirements documents inevitably contain omissions, inconsistencies, repetition and requirements conflicts. This document is no different and I made a number of mistakes when originally writing this document. Some of these have been pointed out and, whilst I have corrected some problems, I have deliberately left some of the omissions, conflicts and inconsistencies in the document. The reason for this is that requirements documents are always generated to meet a deadline and, in reality, the time available for review and update is very limited. I want to retain the imperfections of the document as these reflect the reality of requirements for real systems. I leave it as an exercise for the reader to find some of the conflicts etc. in the document.

# 1. Introduction

The Mid-Scotland regional health authority wishes to procure an information system to help manage the care of patients suffering from mental health problems. The overall goals of the system are twofold:

1. To provide better management information about mental healthcare in the region.
2 To provide an improved records system for clinical staff involved in diagnosis and treatment.

The system is NOT intended to be a complete medical records system where all information about a patients' medical treatment is maintained. It is solely intended to support mental health care (e.g. if a patient is suffering from some other unrelated condition, such as high blood pressure, this would not be formally recorded in the system). The system must therefore interoperate with and shared information with other patient record systems that are in use.

This document sets out the high-level requirements for this proposed system, known here as the Mentcare system. In some areas, these requirements are incomplete and more detailed requirements must be derived after consultation with the system stakeholders.

## 1.1 System overview

The mid-Scotland health-authority has a statutory duty to provide mental healthcare services to citizens living in the mid-Scotland area. Most mental health patients do not require dedicated hospital treatment but need to attend specialist clinics regularly where they can meet a doctor who has detailed knowledge of their problems. The health authority has a number of day clinics that patients may attend in different hospitals and in local health centres. Patients need not always attend the same clinic and some clinics may support 'drop in' as well as pre-arranged appointments.

All patients seen at clinics have been referred to the clinic either by their own doctor, by doctors in Accident and Emergency when they have attended for treatment or by hospital doctors, when they have completed a course of hospital treatment. The nature of mental health problems is such that patients are often disorganised so may miss appointments, deliberately or accidentally lose prescriptions and medication, forget instructions and make unreasonable demands on medical staff. The Mentcare system must therefore be able to cope with patient unpredictability and irregular attendance at clinic sessions.

The patient information system to support mental health care (the Mentcare system) is a medical information system that maintains information about patients suffering from mental health problems and the treatments that they have received. The Mentcare system has to provide both management and clinical information:

1. Management information that allows health service managers to assess performance against local and government targets and to monitor the costs of treatment.

2. Clinical information on medical history, diagnoses and treatments.

The system is used to record information about patients (name, address, age, next of kin, etc.), consultations (date, doctor seen, subjective impressions of the patient, etc.), conditions and treatments. Reports are generated at regular intervals for medical staff and health authority managers. Typically, reports for medical staff focus on information about individual patients whereas management reports are anonymized and are concerned with conditions, costs of treatment, etc.

The key features of the system are:

1. *Individual care management* Clinicians can create records for patients, edit the information in the system, view patient history, etc. The system supports data summaries so that doctors who have not previously met a patient can quickly learn about the key problems and treatments that have been prescribed.

2. *Patient monitoring* The system regularly monitors the records of patients that are involved in treatment and issues warnings if possible problems are detected. Therefore, if a patient has not seen a doctor for some time, a warning may be issued. One of the most important elements of the monitoring system is to keep track of patients who have been sectioned (detained in a secure hospital without their consent) and to ensure that the legally required checks are carried out at the right time.

3. *Managing involuntary detention* In a minority of cases, patients may be a danger to themselves or to other people. They may regularly change address and may be homeless on a long-term or short-term basis. Where patients are dangerous, they may need to be 'sectioned' – confined to a secure hospital for treatment and observation. The system must make provision for managing patients who have been detained and for ensuring that all required legal processes are followed and documented.

4. *Administrative reporting* The system generates monthly management reports showing the number of patients treated at each clinic, the number of patients who have entered and left the care system, number of patients sectioned, the drugs prescribed and their costs, etc.

The overall design of the system has to take into account both safety and privacy concerns.

1. The safety implications stem from the fact that some mental illnesses cause patients to become suicidal or a danger to other people. Wherever possible, the system should warn medical staff about potentially suicidal or dangerous patients. Other safety issues concern checking of drug dosage and appropriate medication. The system must be available when needed otherwise safety may be compromised and it may be impossible to prescribe the correct medication to patients.

2. As in all medical systems, privacy is a critical system requirement. It is essential that patient information is confidential and is never disclosed to anyone apart from

authorized medical staff and the patient themselves. Hospital managers should not have access to individual patient information.

## 1.2 System users

There are 4 types of user that may make use of the Mentcare system:

1. *Clinical staff*. Clinical staff interact directly with the system, looking up and modifying patient information. They are particularly concerned with maintaining a history of consultations and recording the treatment and medication prescribed to patients.
2. *Administrators*. Administrators interact directly with the system and use it in conjunction with a generic appointments system to record information about patient appointments. They need to record when appointments were made, the appointment date and whether or not patients attended appointments. Administrators are also responsible for generating reports for clinic management.
3. *System administrators and records managers* The medical records office is responsible for ensuring the overall integrity and security of the data in the system. They are also responsible for integrating the system with other patient record systems, sharing information when required. System administrators are responsible for ensuring the security and integrity of the system. Medical records managers are responsible for ensuring that the system conforms to legal requirements on personal information systems.
4. *Health service management*. Health service management do not interact with the system directly. Rather, they make use of reports covering consultations, diagnoses and treatments. These creation of these reports is initiated by medical records staff. The reports are generated automatically by the system and do not contain personal patient information. Managers do not have access to the clinical features of the system or to individual patient records.

## 1.3 System usability

The Mentcare system will be used by a range of professional and administrative staff including senior doctors and consultants. For acceptance of the system by these staff, it is essential that close attention is paid to system usability so that users (a) can learn to use the system quickly; (b) can use the system without undue effort during a patient consultation and (c) make as few errors as possible when using the system.

Usability is particularly important in a context where senior professionals, such as hospital consultants, with considerable autonomy in how they work are expected to use the system. They cannot simply be instructed that they must use the system – if they don't like it, they may refuse to use it and create a clinical rationale for this. User reliability is important from an organisational as well as a clinical perspective. Not only may user errors affect the

diagnosis and treatment of patients, incorrect patient information may mean that management reports are inaccurate.

## 1.4 Operational constraints

The following operational constraints shall apply to the Mentcare system:

1. The Mentcare system shall make use of the health authorities drug information system that includes information about the characteristics of drugs and the costs of these drugs. Details of the interface to this system are available in the document Mid-Scot-DrugSys-2011.

2. The Mentcare system shall provide summary information about patients and treatments for the national patient record system. The format of the information required is defined in the document Mid-Scot -NatSysInfo-2010. Interface definition for the National Patient Record System.

3. The Mentcare system shall make use of the Mid-Scotland health authority's single sign-on authentication system. This is a multi-factor authentication system that requires both a login/password and answers to personal questions for each user. Information about this system is available in the document Mid-Scot -AuthSys-2013.

4. The Mentcare system shall run on hardware (Linux servers) that is available in the authority's data centre. Note that the maximum server memory available is currently 32GB. System administrators in the center are responsible for system backup.

   The Mentcare system security shall conform to the standards and provisions for secure medical systems as set out in Mid-Scot-Security-Requirements-2013.

6. There is an existing system for prescribing medication called the PRESCRIPTION system. It is desirable that this system should be used rather than implement new prescribing functionality in the Mentcare system.

# 2. System requirements

The Mentcare system is a patient information system that maintains individual patient records as described in Sections 3.1 and 3.2 (Clinical and Management user requirements). This section sets out general requirements that apply to the system as a whole and which are not derived from any specific stakeholder.

2.1 The system shall be implemented as a client-server system with patient information held on a server maintained by the mid-Scotland health authority.

2.2 Client access to the system shall be provided through a standard web browser. In keeping with the heath authorities policy of using open-source software wherever possible, the Firefox web browser shall be the standard browser that is supported.

2.3 The user interface to the system shall be an interactive forms-based interface.

2.4 The information that shall be maintained in the system is defined in sections 3-6 of this document.

2.5 As far as possible, all user selections shall be made using menus of allowed items.

*This avoids certain types of user input errors where invalid information is input.*

2.6 All user inputs that are not selected from a menu shall be validated according to validation rules to be established when the system user interface is designed. If an input is invalid, the user shall be informed why it has been rejected by the system.

2.7 The Mentcare system shall include a search feature that allows users to discover the records for individual patients. Search may be based on patient name or the patient's national health identifier.

## 2.1 Availability requirements

2.1.1 The Mentcare system shall be continuously available during 'normal' clinic working hours between 0800 and 1830, Monday to Friday.

2.1.2 Periods of scheduled maintenance for the Mentcare system shall normally be arranged during the authority's 'systems at risk' periods i.e. between 2100 and midnight, Monday to Friday and between 0800 and 1200, Sunday.

## 2.2 Response requirements

The response time of the system contributes to both operator satisfaction and operator reliability. If the response time is too long, operators will become frustrated with having to wait for this system; this frustration can lead to errors being made.

2.2.1 The system shall normally respond to all user queries about an individual within 2 seconds.

2.2.2 If a system response is greater than 2 seconds, then the system shall display an indicator to the user that processing is taking place.

*This avoids user frustration if there has been a system failure and they keep waiting for a response that does not arrive.*

## 2.3 Data exchange requirements

2.3.1 The system shall be required to exchange information with the national summary patient record system. The information to be exchanged and the format of that information shall be decided after consultation with the managers of the summary patient record system.

2.3.2 The Mentcare system shall run on the same system platform as an APPOINTMENTS diary system and it shall be possible to transfer appointment data to and from the APPOINTMENTS system to the Mentcare system.

# 3. User requirements

## 3.1 Clinical requirements

Clinical staff use the system directly when patients attend for a consultation. They access and read individual patient records and, for every consultation, update the patient record with details of the consultation and the treatment prescribed. Patient records must be updated at each consultation.

Individual doctors may also access the system in read-only mode outside of consultations. For example, a doctor who is reading a paper about a new drug treatment may use the system to see if she has any patients for whom this may be useful.

The critical clinical requirements for the system are:

3.1.1 The Mentcare system shall allow for the creation, updating, storage and management of patient records. The specific format of patient records shall be determined in collaboration with clinical and medical staff but it shall include at least the following information:

A unique patient identifier, which should normally be their national health number. If patients do not have or know their NH number, then a unique patient ID shall be generated by the system.
Personal patient information (name, address, date of birth, contact details, registered medical practice, family contacts);
A risk assessment for self-harm/violence;
Diagnoses of conditions (patients may suffer from several conditions at the same time);
Treatments (several treatments may be prescribed including CBT);
Prescribed medications (several medications may be prescribed);
Consultations;
Referrals (information about referrals to other clinical departments, social services, etc.)
Information as required by the Mental Health Act (see Section 4).

3.1.2 The system shall use a relational database system from the approved list published by the health authority. The specific choice of database system may be delayed until implementation.

3.1.3 One or more free form text input fields shall be provided to allow comments on the patient by individual clinicians to be recorded.

*Mental health conditions are complex and this complexity cannot necessarily be captured in choices from drop-down menus. It is essential that clinical staff can write narrative comments about a patient.*

3.1.4 To reduce the interaction time required, the system shall provide a 'no change' button which will cause a consultation record to be created and which will simply carry forward the diagnoses and medication from the previous consultation.

3.1.5 As a general principle, staff should not be required to re-enter patient information that is already recorded in the system. Whenever possible, therefore, provision should be made for prefilling forms with existing system information.

3.1.6 The system shall automatically create a consultation record at the start of each consultation recording the date and time and the clinical staff (up to 6) involved. This should allow clinical staff to record comments on the consultation, referrals and changes of medication made.

3.1.7 The system shall maintain a record of all medication prescribed, date of prescription and the prescriber. Provision shall be made in each prescription for free-form comments to be included by the prescriber.

3.1.8 The system shall maintain a record of all diagnoses made, date of diagnosis and the diagnostician. The conditions diagnosed shall be selected from a list of known conditions and it shall be possible for multiple conditions to be diagnosed. Provision shall be made for free-form comments about the diagnoses to be included by the prescriber.

3.1.9 When a patient has been referred to another clinical, information about all referrals including the date of referral, the referrer and any information provided by the referrer shall be maintained by the system.

3.1.10 It shall be possible to update a patient record during a consultation when the record has been opened or at a later date. Records which have not been updated during a consultation should be flagged to indicate that they are not completely up-to-date.

*This allows for system failure or for individual doctors, for whatever reason, being unable to update the record at the time of a consultation. An example of such a situation is where a patient threatens or commits violence and has to be forcibly restrained.*

3.1.11 It shall be possible, from within the system, to consult the known side-effects for any drug that may be prescribed using the system.

3.1.12 The system shall provide a risk indicator field that allows the risk status of the patient to be recorded. Risk status reflects the clinical assessment of whether the patient is likely to be a danger to themselves or others.

3.1.13 The Mentcare system shall support the printing of medication prescriptions. The medications prescribed shall be chosen from the list of medications approved for use by the health authority. Several medications may be prescribed on a single prescription. It is recommended that the PRESCRIPTION system currently used by the mid-Scotland health authority is used to provide this feature.

3.1.14 The Mentcare system shall support the generation of repeat prescriptions by an administrator. Patients may be identified by their PID or by a name/date of birth combination.

*A repeat prescription is a prescription for drugs that has been previously approved by a doctor; doctors must still sign these prescriptions before they are issued to patients.*

3.1.15 The Mentcare system shall maintain a list of repeat prescriptions issued and the time/date of issue.

3.1.16 It shall be possible to print patient records selectively by highlighting record components that are to be printed.

3.1.17 Clinical staff visiting patients at home shall be able to download patient records in advance to a laptop computer, modify these records then upload the records to the server.

3.1.18 Uploaded records shall be securely deleted from the laptop after the upload is complete.

3.1.19 The Mentcare system shall maintain a log that records the records and the MAC address of the computer to which the records have been downloaded.

## 3.3 Administrator requirements

Clinic and health service administrators use the system for two main functions:

1. To manage patient appointments and to set up meetings of clinical staff for discussion of patients and involuntary detention.
2. To define and generate reports for clinic management on diagnoses, prescribed treatments and numbers of patients seen by clinical staff.

This leads to the following administrative requirements:

3.3.1 The Mentcare system shall integrate with the health service APPOINTMENTS system so that patient appointments are made and managed using the APPOINTMENTS system.

3.3.2 The Mentcare system shall allow the list of clinic appointments for any specific clinic to be downloaded to the Mentcare system. For each clinic, the appointments for that clinic shall be automatically downloaded from the APPOINTMENTS system to the Mentcare system for viewing in the Mentcare system. The previous list of appointments shall be deleted automatically before a new list is downloaded.

3.3.3 The patient record shall include a facility to record if a patient has missed an appointment along with details, if available, of why the appointment was missed.

3.3.4 Patient records shall contain a record of all meetings set up by clinical staff to discuss that patient. Meeting information shall include the date and time of the meeting, the staff involved and a summary of the meeting decisions.

3.3.5 The system shall provide facilities for administrators to set up meetings by proposing a list of staff involved and a list of possible dates/times for the patient meeting. The system shall automatically email staff involved with the meeting proposal. If staff are not available, it is the responsibility of administrators to find an alternative date and time.

3.3.6 A report format definition tool shall be provided for administrators to define the format of the reports required by managers. A list of available reports shall be maintained by the system. Initially, the developers should work with administrators to define a set of common reports.

3.3.7 The Mentcare system shall allow administrators to select a management report to be generated and shall generate that report from the patient information.

3.3.8 The Mentcare system shall allow administrators to save the management report on a local storage system. (

*They may then email it to hospital managers or print the report*

## 3.4 Management requirements

Health service managers do not use the system directly but require regular reports on the treatment process for mental health patients. These reports do not contain individual patient details but might record information such as the numbers of patients who attended each clinic each month, a summary of the drugs prescribed each month, a summary of the times that patients have had to wait for appointments, etc.

The reports are generated for managers by administrators – they must not contain information about identifiable, individual patients.

3.4.1 The system shall maintain lists of patient conditions and treatments and clinicians shall select the patient condition and treatment from menus generated from these lists.

*The rationale for this is consistency of terminology for management reporting. If free form input is allowed then different users of the system may refer to the same thing in different ways (e.g. a drug may be available under several different brand names.*

3.4.2 The Mentcare system shall generate weekly reports for each clinic showing the number of patients attending each clinic on each day that it runs, the clinicians involved and the total number of patients who have attended for mental health treatment. The report should also summarise the number of patients suffering from each condition, the total amounts of each drug prescribed as medication and the costs of these drugs to the health authority.

## 4. The Mental Health Act

The Mentcare system is affected by two pieces of legislation (in the UK, Acts of Parliament). These are the Data Protection Act that governs the confidentiality of personal information and the Mental Health Act that governs the compulsory detention of patients deemed to be a danger to themselves or others.

Mental health is unique in this respect as it is the only medical speciality that can recommend the detention of patients against their will. This is subject to strict legislative safeguards. One of the aims of the Mentcare system is to ensure that staff always act in accordance with the law and that their decisions are recorded for judicial review if necessary.

The Mental Health (Care and Treatment) (Scotland) Act 2003 applies to people who have a mental illness, learning disability or related condition. This Act allows, under certain conditions, for patients to be detained for their own safety and the safety of others without their consent and it allows for the compulsory treatment of certain mental health problems. The Act sets out safeguards for the patients and there are strict time limits for compulsory detention. Patients must be assessed before the end of these time periods and cannot be further detained unless this assessment has been completed.

The assessment process itself, which requires the involvement of two medical specialists, is not directly supported by the Mentcare system, However, the results of assessment are maintained in the system and the system is used to facilitate communications with relatives and carers of detained patients and to issue reminders to clinicians of the need for reassessment.

It is assumed that there shall be a Mental Health Act administrator role (MHA administrator), who is responsible for arranging and managing all MHA assessments.

4.1 Patient records shall maintain information about sectioning assessments carried out under the Mental Health Act. This shall include:

The names of the clinical staff involved in the assessment;

The date of the assessment;

Whether or not compulsory detention and treatment was recommended;

The place of detention and the date detention started;

The recommended treatment for the patient;

The date of agreed release from detention;

4.2 In accordance with the timetable set out in the Mental Health Act (Scotland), a reminder email shall be issued to the MHA administrator, 30 days before the required detention review date. This shall provide information about the previous detention review.

4.2.1 If no review has been set up within 7 days of the required detention review date, the system shall generate a daily email to the MHA administrator reminding him/her of the requirement for review.

4.2.2 If no review has been held by the required review date, the system shall generate a letter for the patient concerned informing them that involuntary detention cannot be continued.

4.2.3 The working day before the required review date, a letter shall be generated and sent to for the manager of the facility where a patient is being detained informing them that, unless they receive phone confirmation of a review, the patient should be released on the required review date.

4.3 When a detention review had been arranged, the system shall generate a letter to the patient being reviewed and their carers that sets out their rights under the Mental Health Act.

4.4 When a detention review has been completed, the system shall generate a letter to patients and their carers with information about the conclusions of the review and, if detention is recommended, the required review dates for that detention.

4.5 When a detention review has been completed, the system shall generate a letter for the manager of the facility where the patient will be detained providing information about that patient. (It is assumed that, as part of the review process, a decision of the place of detention and confirmation of availability has been made).

4.5 If a patient being reviewed has a history of self-harm or violence, the system shall generate a warning to the MHA administrator who has the responsibility of informing staff involved in the review of this.

# 5. Safety requirements

The treatment of patients suffering from mental health problems is unique in that the nature of these problems may mean that some of these patients may self-harm as a result of their illness. A very small minority of patients may be violent and pose a threat to themselves, clinic and hospital staff and other patients. These factors mean that, in addition to the usual safety concerns that apply to medical information systems, information systems for mental health care must maintain information about patients that allows staff to come to a judgement about whether or not a patient is likely to self-harm or be violent.

There are therefore 5 principal threats that must be addressed by the Mentcare system:

•. Accidental self-harm though overdose of medication or other types of treatment.

•. Deliberate self-harm / suicide.

•. Attacks by patients on staff, other patients, their relatives and carers and the general public.

•. Prescription of inappropriate treatment that causes harm to the patient.

•. Adverse patient reactions to prescribed medication or other treatment.

The first three of these threats are specific to mental healthcare systems; threats 4 and 5 are generic threats that apply across all types of treatment. Whilst specific risk ratings for these threats are inevitably provisional, estimates are as follows:

•. *Accidental self-harm*. High risk. The risk here is higher than for some other classes of patient because of the possibly confused state of some patients.

•. *Deliberate self-harm*. High risk. The nature of patient conditions leads to this.

•. *Attacks on other people*. Medium risk. These are uncommon but serious when they do occur.

•. *Prescription of inappropriate treatment*. Medium risk. The risk here is higher than for some other classes of patient because of the possibly confused state of some patients.

•. *Adverse reactions to medication*. Low risk. The reactions to the most commonly prescribed medications are well understood.

These risks lead to the following safety requirements:

5.1 The records of patients who have a history of deliberate self-harm shall be highlighted to bring them to the attention of clinical system users.

5.2 The system shall be able to generate warning letters to clinic staff and patient relatives about a patient indicating the possibility of deliberate self-harm.

5.3 The system shall provide fields that allow details of incidents or threats of *deliberate* self-harm to be maintained.

5.4 Information about incidents of *accidental* self-harm shall only be maintained when these are directly related to the treatment prescribed (e.g. over or underdosing of medication).

5.5 When treatment details are entered in the system, the system shall display details of previous treatment. *This will make it easier for clinical staff to check that treatment prescription errors have not been made*.

5.6 The system shall allow information about adverse reactions to treatment to be maintained. If a patient is known to be allergic to any particular medication, then prescription of that medication shall result in a warning message being issued.

5.7 Prescribers may overrule warning messages from the system. In such situations, the system shall maintain a record of the warning issued and the identity of the prescriber who overruled the warning.

5.8 The system shall generate a daily list of patients who were expected to attend a consultation but who failed to attend. This list shall be automatically e-mailed to the consultants responsible for the care of these patients.

5.9 To reduce the probability of over-prescription of medication, the system shall take the following actions:

5.9.1. Highlight the date of the patient's previous medication prescription and where it was issued. *(Note: some patients attend several sessions to try to get extra medication which they can then sell on)*.

5.9.2 By default, limit the medication prescription to a two week period for medication on the restricted list (Mid-Scot-Restricted-meds-2014)

5.9.3 For specific medication, defined as Pharmacy Only in Mid-Scot-Restricted-meds-2014, require that the patient attend a pharmacy for a daily dose that this medication. (*Note, an example of such a drug is Methadone, for heroin addiction)*.

5.10 The system shall generate a daily list of patients where the patient has attended a consultation and where the records have not been updated. This list shall be emailed to the clinic where the patient has attended the consultation. Each record on this list shall be highlighted in the system until an update has been made. *(Note: this is intended to help detect records which, through human or system failure, have not been updated after a consultation)*.

# 6. Security and privacy requirements

## 6.1 The Data Protection Act

The Mentcare system must conform to the legal safeguards set out in the 1998 UK Data Protection Act. In summary, this means that the system must:

- Maintain information securely and ensure that it is only accessed by authorised users.
- Allow individuals access to their personal records.
- Ensure data that is maintained on an individual to be relevant for the purpose for which it is maintained. Therefore, it is unlikely that the Act would permit details of patient purchases from the hospital shop (for example) to be maintained in their medical record.
- Provide means for people to challenge and correct information in the system that the data holder cannot demonstrate to be correct.
- Only maintain information while it is required for its purpose. For medical systems, you might argue that this is the patient's lifetime or even longer if historical medical analysis is to be supported.

In addition to the Data Protection Act, the provisions for the management of patient information set out in AAAA-Clinical Information Management-2012 shall apply to the Mentcare system.

In the event of any system requirement here being in conflict with the Data Protection Act, the conflict must be resolved so that the legal provisions as set out in Data Protection Act are maintained.

## 6.1 Security requirements

Access to the functionality of the Mentcare system shall be controlled according to the role of the information user. For example, an administrator role may access details such as patient name and address but not details of their medical conditions. A security administrator is responsible for setting up the access permissions for the system.

6.1.1 The Mentcare system shall include a role-based access control system that allows access to information to be specified in terms of the role of the system user.

6.1.2 The Mentcare system shall support differential access to patient information depending on the role of the information user. Initial roles supported should be a clinical role, an administrator role and a medical records role. Provision shall be made in the system for adding new roles such as a 'researcher' role or a 'patient' role.

6.1.3 The system shall provide a facility to set up and edit security permissions for each role.

6.1.4 Access permissions shall be set up in accordance with a the Mentcare security policy (to be defined)

6.1.5 All changes to security permissions shall be logged with details of who made the change, the date and time of the change and the changes made.

6.1.6 The Mentcare system shall be maintained on a central server and records shall be accessed and updated in place by staff using the system.

6.1.7 The Mentcare data server shall be maintained as a separate computer in a physically secure location.

6.1.8 The Mentcare data server shall be backed up onto tape or disk each evening at or around 8pm. Backup policy shall conform to the standards set out in AAAA-Clinical Information Management-2012.

6.1.9 A log of all transactions during a clinic session shall be maintained on local computers running the system. The Mentcare system shall allow these to be replayed against a copy of the database to recreate amended records if required.

*This allows records to be restored in the event of system failure in an clinic.*

6.1.10 All PCs used to run the Mentcare system shall have a static IP address and access and update requests shall only be accepted from PCs whose address is registered with the server.

6.1.11 To reduce the probability of SQL poisoning attacks, the system shall validate all inputs that may be part of database queries. Any input that includes valid SQL shall be rejected.

6.1.12 The length of all free-form user text inputs shall be limited and the system shall reject any inputs whose length is greater than the allowed limit.

*This reduces the probability of attacks based on buffer overflow.*

6.1.13 The system shall not allow copies of patient records or transactions to be stored on portable storage devices such as USB flash drives.

## 6.2 Privacy requirements

Privacy requirements are designed to ensure that clinical ethical standards are maintained and that the authority follows the provisions set out in the Data Protection Act.

6.2.1 The system shall ensure that access to personal information on patient records is only permitted by authorised clinical and management staff.

6.2.2 The system shall only allow the transmission of personal patient information to accredited staff and to the patient themselves.

6.2.3 The system shall provide a facility for patients to request personal information and to request changes to that information.

6.2.4 A change procedure to accept or reject changes to personal information shall be established by the medical records office.

6.2.5 The system shall record that information has been deleted or changed according to a patient change request. The patient record shall not be linked to any change requests made for that record.

6.2.6 When notified of the death of a patient, the patient record shall be locked as read-only. Within 3 months of the notification of death, the patient record shall be removed from the Mentcare system and stored in an archive system.

Privacy requirements are made more complex by the fact that medical researchers may require access to treatment details and patient characteristics. The Data Protection Act does not permit researchers access to individual patient records because they have no need to know of the medical problems and treatment of an individual. However, anonymized access is allowed where researchers may access bulk information in the system to answer questions such as 'How many women over 50 in the EH postcode area were treated with drug X'.

It is understood that maintaining anonymity is difficult if (a) there are a small number of people in any data set and (b) cross-referencing with other data sets is permitted. As a consequence, there are restrictions on what can be included in an anonymised report.

6.2.7 The system shall include a report generation feature that allows for the creation of anonymised reports about patient conditions, treatments prescribed and treatment outcomes.

6.2.8 The creation of anonymised lists shall be restricted to a named set of individuals who must be approved in advance by the health authority.

6.2.9 Patient names, dates of birth, places of birth and addresses may not be included in anonymised lists.

6.2.10 Geographical information may be included in anonymised list using the regional postcode designator only.

*The regional postcode designator is the first 3 or 4 postcode characters that indicate a general area but which does not allow identification of individual street addresses.*

6.2.11 Anonymised lists with more than 20 entries may be printed on an approved printer but not exported in any electronic format.

6.2.12 Anonymised lists with fewer than 20 entries may be viewed on screen but may not be printed.