CASE STUDY
Mental Health Care Patient Management System (MHCPMS)

This case study is based on a real system that is in use in a number of hospitals. For reasons of commercial confidentiality, I have changed the name of the system and have not included information about any specific system features.

1. Background

A 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 generate management information that allows health service managers to assess performance against local and government targets.
2. To provide medical staff with timely information to facilitate the treatment of patients.

The health authority has a number of 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.

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. In a minority of cases, they 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.

Users of the system include clinical staff (doctors, nurses, health visitors), receptionists who make appointments and medical records staff. Reports are generated for hospital management by medical records staff. Management have no direct access to the system.

The 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.

The system is NOT a complete medical records system where all information about a patients' medical treatment is maintained. It is solely intended to support mental health care so if a patient is suffering from some other unrelated condition (such as high blood pressure) this would not be formally recorded in the system.

2. Viewpoints and Concerns

This case study was originally developed to illustrate the DISCOS method which support the derivation of dependability and functional requirements for systems which may be implemented using off-the-shelf components. The DISCOS method supports the derivation of requirements from a number of *viewpoints* with the requirements elicitation and analysis driven by a set of *concerns*. Viewpoints reflect the requirements from different classes of system stakeholder. Concerns reflect organisational goals, constraints and external requirements. A paper on the use of DISCOS is included as an appendix to this document. A more detailed slide set with a comprehensive description of DISCOS is available for downloading at:

http://www.software-engin.com/Resources/DISCOS

2.1 Concerns

Concerns are intended to represent high-level organisational goals that are often vague and poorly specified. These are important to the success of the system and so the requirements engineering process must try to understand their implications for the system. However, the nature of concerns is such that some aspects will always be vague (e.g. the notion of 'reasonable' costs) and subject to individual interpretation.

The principal concerns in the MHCPMS are:

1. *Usability*. The system must be used by a range of staff, often working under time pressure and with different levels of experience using computer-based information systems.
2. *Safety*. Patients may cause harm to themselves or others. The provisions of the Mental Health Act must be taken into account.
3. *Privacy*. Patient privacy must be maintained according to the Data Protection Act and local ethical guidelines.

4. *Operational costs*. The operational costs of the system must be 'reasonable'.

Note that concerns reflect organisational goals rather than the goals of the different classes of system stakeholders. Safety and privacy are concerns because of legislation and the negative consequence of failures which affect safety and privacy. Usability is a concern because of the need for efficient working and staff retention. Operational costs are a concern because of budgetary constraints.

Note that properties such as availability and reliability are not organisational concerns although they may be important to system stakeholders. Furthermore, availability and reliability requirements may be derived from the principal organisational concerns.

Functionality, the definition of the services that the system has to provide, is an implicit concern for all system.

2.2 Viewpoints

Viewpoints are a means of structuring the collection and documentation of requirements from classes of system stakeholder. Each viewpoint represents a partial specification of the system so the complete specification is created by integrating the requirements from each viewpoint. Viewpoints may either be interactor viewpoints representing stakeholders who interact directly with the system, indirect viewpoints representing stakeholders that require information from the system or are involved with the system management and domain viewpoints that represent

There are four principal viewpoints that place requirements on this 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. *Receptionists*. Receptionists 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.
3. *Medical records staff*. Medical records staff interact with the system to generate management reports and to link information in the system with more general patient health records.

4. *Health service management*. These are indirect viewpoints as health service managers do not directly interact with the system. However, they do require reports generated from the system and so generate information requirements.

There is no explicit viewpoint representing other computer-based systems that may interact with this system. It is assumed that any requirements of this type will come from one of the principal viewpoints.

3. Concern decomposition

The DISCOS method starts by identifying concerns and decomposing these to sub-concerns and questions. A complete decomposition would be too lengthy to show here but we can look at the early levels of decomposition for all concerns and then examine a limited number of these in more detail.

The four concerns identified are usability, safety, privacy and operational costs. Figure 1 shows the first stage of decomposition of these concerns.

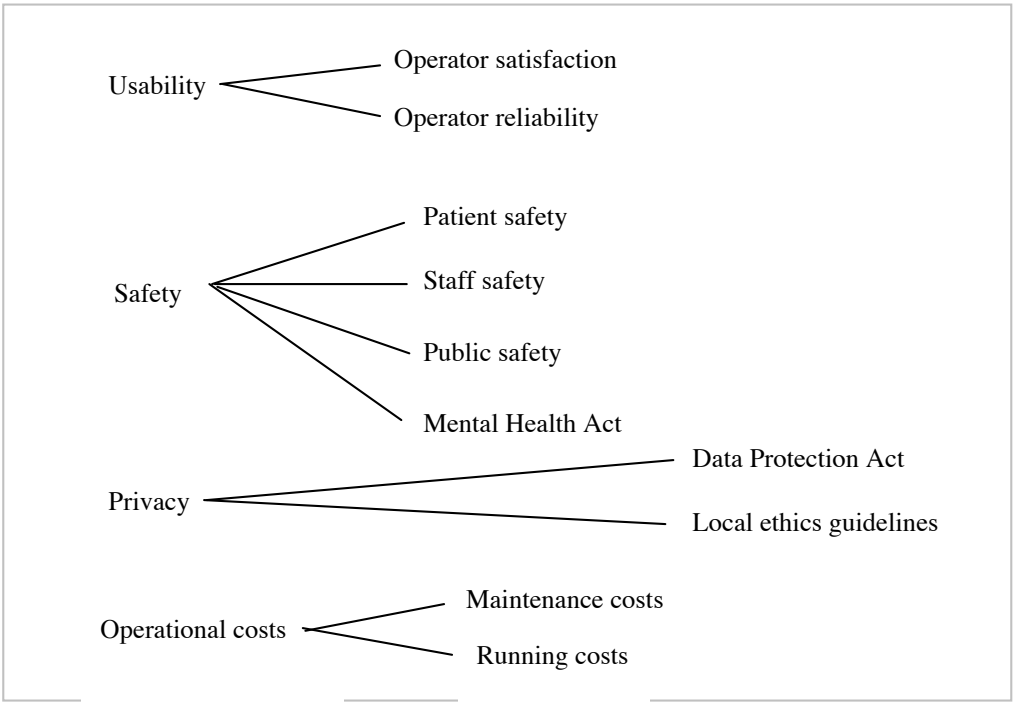

Figure 1: Concerns in the MHCPMS

Now consider each concern in turn:

1. *Usability* is decomposed into operator satisfaction (are the users happy to use the system) and operator reliability (do the operators use the system in the way it was intended without making mistakes). Operator satisfaction 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. Operator reliability is important from an organisational as well as a clinical perspective because the system is used to generate information that affects the funding of the service.
2. *Safety* is decomposed into patient safety, staff safety, safety of the general public and safety issues associated with the mental health act. The reasons for this decomposition should be obvious.
3. *Privacy* is decomposed into privacy issues associated with the mental health act and additional privacy issues over and above these that are defined by local ethics committees.
4. *Operational costs* are decomposed into maintenance costs which include hardware and software update costs and running costs – the costs associated with staff, such as helpdesk staff, who support the everyday running of the system.

At this level of decomposition, concerns are still vague reflections of issues that the organisation considers to be important. To break these down into more detailed concerns, we ask 'what are the issues' questions e.g. 'what are the issues around patient safety that are of concern for the system'. This results in a further level of decomposition as shown in Figure 2.

Patient safety concerns the health and well-being of the patient themselves. Two of these are generic to all medical situations namely incorrect treatment and adverse reactions to treatment. The other two are more specific to mental health situations where the often confused nature of patients can result in accidental self harm and, sometimes, deliberate self-harm to gain attention.

Again, the nature of patients suffering from mental health conditions means that they may constitute a danger to others. They may attack them in some way. Although the threat is the same for medical staff, relatives and the general public, the risks and the situations where attacks might take place are different. Consequently, these are identified as separate concerns.

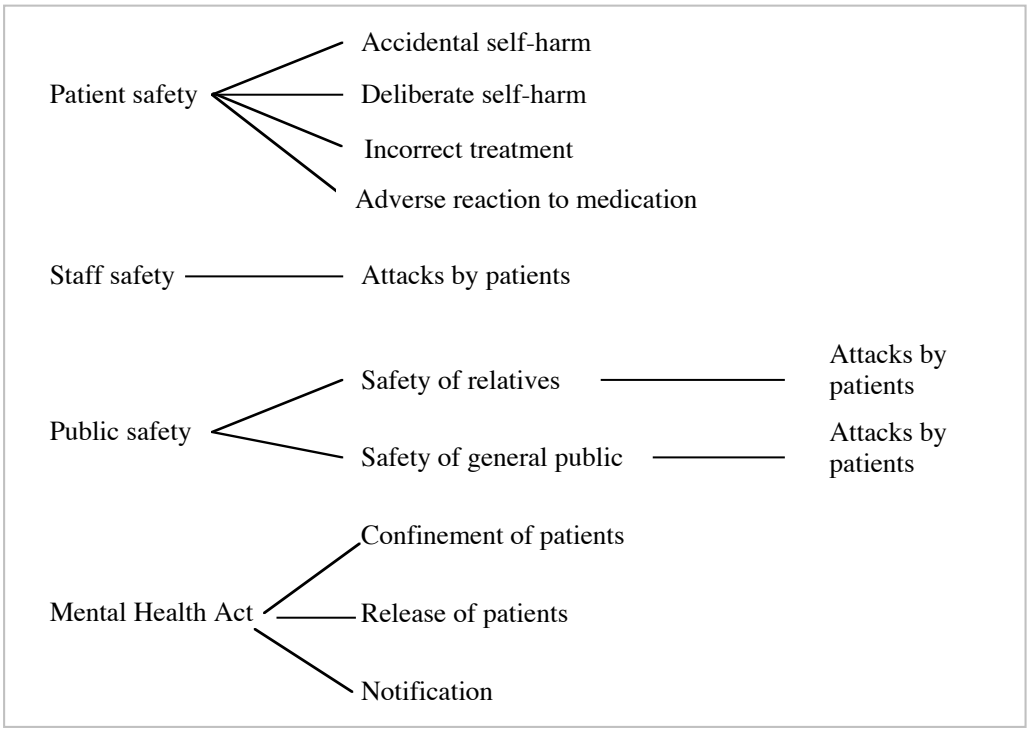

Figure 2: Decomposition of the safety concern

Finally, the Mental Health Act is concerned with both the safety of the public and the rights of patients. Legal formalities have to be followed when patients are confined and released, confinement can only be for a limited time without further examination and various people have to be notified when a patient is confined and released.

The same process is followed for all of the other concerns. I will not go into these in detail here but will do some decomposition of the privacy concern because this illustrates a potential conflict with safety requirements.

The major influences on privacy are the historical ethical safeguards on individual patient records and the more recent safeguards imposed by data protection legislation. I'll simply consider data protection issues here which set out limitations on information systems such as:

1. Require systems to allow individual access to their personal records.
2. Require all 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.

3. Require systems to allow people to challenge and correct information in the system that the data holder cannot demonstrate to be correct.
4. Require that systems 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.

Therefore, the Data Protection Act concern might be decomposed into sub-concerns such as Data Access, Data Relevance, Data Integrity and Data Lifetime.

4. Dependability requirements

Dependability requirements are generated from concerns by associating questions with each of these concerns. The answers to these questions (which may come from stakeholders, documentation, etc.) are the basis for the dependability requirements. Questions may also be generated that apply to the requirements generated from each viewpoint. These questions check that the requirements are consistent with the organisational concerns.

Let us consider the Patient Safety concern and its associated sub-concerns of deliberate and accidental self-harm, incorrect treatment and adverse reactions to treatment. We can associate general questions with each of these subconcerns:

What information from the system might reduce the risks to patient safety under these headings?

Who requires this information and when do they require it?

By asking these questions, we can establish a set of safety requirements. Examples of these requirements are:

1. The records of patients who have a history of deliberate self-harm shall be highlighted in some way to bring them to the attention of clinical system users.
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.
3. The system shall provide fields that allow details of incidents or threats of *deliberate* self-harm to be maintained.
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. 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.
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.
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.
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.
9. The system shall provide information to medical staff which reduces the probability of over-prescription of medication. (Note: that this is quite a vague requirement – there is an associated question *How can over-prescription of medication be avoided* which is put to the system stakeholders when the system facilities to support prescription are defined).
10. To reduce the probability of over-prescription of medication, the system shall highlight the date of the patient's previous consultation when a patient attends a drop-in consultation session. (Note: some patients attend several sessions to try to get extra medication which they can then sell on).
11. 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).

The process of generating safety requirements for the other safety concerns continues until all concerns have been addressed. Because of the spiral nature of the derivation process (see paper on the DISCOS method), this process will overlap with the process of discovering viewpoint requirements.

Now let us consider some of the dependability requirements that are generated from the privacy concern. Initially, the derivation of requirements from each concern should be undertaken independently. As discussed above, privacy

requirements are generated from access, relevance, integrity and lifetime concerns.

While the privacy concern generates some requirements for the automated MHCPMS system, the nature of the data protection legislation is such that many of the requirements fall on the broader socio-technical system. That is, they are requirements on the ways in which the automated system may be used rather than simply requirements on the automated system itself.

Privacy requirements in medical systems are made more complex by the fact that medical researchers often 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 LA postcode area were treated with drug X'.

Although the data protection legislation could be interpreted so that receptionists can access patient medical records, in this case, a local decision has been made to disallow such access. Therefore, receptionists are only permitted access to some parts of a patient record.

I won't go into the details of generating privacy requirements – some examples of these requirements are:

1. The system shall ensure that access to personal information on patient records is only permitted by accredited staff.
2. The MHCPMS system shall support differential access to patient information depending on the role of the information user. Initial roles supported are a clinical role, a receptionist role and a medical records role.
3. Access to the functionality of the MHCPMS system shall be controlled according to the role of the information user.
4. The system shall only allow the transmission of personal patient information to accredited staff and to the patient themselves.
5. The system shall provide a facility for patients to request personal information and to request changes to that information.
6. A change procedure to accept or reject changes to personal information shall be established by the medical records office.

7. 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.
8. 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 MHCPMS system and stored in an archive system.

5. Viewpoint requirements

Concerns are used to drive the derivation of dependability requirements and requirements associated with organisational goals. System stakeholder requirements must also be discovered. By organising these around viewpoints, we reduce the likelihood of failing to consult key stakeholders and we make it easier to detect overlaps and conflicts between requirements.

The derivation of viewpoint requirements is also driven by concerns. During the process of deriving requirements, each stakeholder should be asked the questions associated with the identified concerns. These not only generate dependability and organisational requirements, but also help stakeholders and requirements engineers to assess the relationships between specific viewpoint requirements and dependability requirements.

5.1 Clinical staff viewpoint

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. Individual doctors (but not normally nurses or other staff) may also access the system 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.

Examples of requirements derived from this viewpoint are:

1. The patient record in the MPCPMS shall include fields to record the diagnosis of the patient's condition and the treatment prescribed. If these are unchanged from a previous consultation, then only a confirmation shall be required. (Staff should not be required to re-enter information already in the system).
2. 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. Free form text input fields shall be provided to allow comments on the patient by individual clinicians to be recorded.
4. It shall be possible, from within the system, to consult the known side-effects for any drug that may be prescribed using the system.
5. 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.
6. The MHCPMS system shall support the printing of medication prescriptions.
7. It shall be possible to print patient records selectively by highlighting record components that are to be printed.
8. Nurses visiting patients at home should be able to download patient records in advance to a laptop computer, modify these records then upload the records to the server.

5.2 Receptionist viewpoint

Receptionists use the system to record when appointments are made, who the patient should see during these appointments and to record if patients keep or miss appointments. They also use the system to generate repeat prescriptions for patients when these are requested.

Examples of requirements from this viewpoint are:

1. The MHCPMS system shall run on the same system platform as the APPOINTMENTS diary system and it shall be possible to simply transfer appointment data from the APPOINTMENTS system to the MCPCMS system.
2. The MHCPMS system shall include a search component that allows a receptionist to discover the record for individual patients.
3. The MHCPMS system shall support the generation of repeat prescriptions given a patient identifier.

5.3 Medical records staff viewpoint

The medical records office is responsible for ensuring the overall integrity and security of the data in the system, with updating the system in response to externally requested changes (normally from a patient) and with generating regular management reports. They are also responsible for integrating the system with other patient record systems. However, no such integration is planned in the near future.

Many of the requirements generated by the medical records staff are security related. Examples of requirements from the medical records staff viewpoint are:

1. The MHCPMS 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.
2. The MHCPMS system shall be maintained on a central server and records shall be accessed and updated in place by staff using the system.
3. The MHCPMS data server shall be maintained as a separate computer in a physically secure location.
4. The MHCPMS data server shall be backed up onto tape or disk each evening at 1800 and copies of backups shall not be stored in the same location as the data server.
5. A record of all transactions during a clinic session shall be maintained on local computers running the system. The MHCPMS system shall allow these to be replayed against a copy of the database.
6. All PCs used to run the MHCPMS 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.

5.4 Health service management viewpoint

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.

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).

2. The MHCPMS system shall generate weekly reports for each clinic showing the number of patients attending the clinic on each day that it runs 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 and the total amounts of each drug prescribed as medication.

6. Requirements conflicts

During the requirements elicitation process, potential conflicts between requirements should be identified and an explicit conflict analysis and negotiation meeting should be scheduled to resolve these conflicts.

From the requirements that have been proposed here, a number of conflicts can be identified. Consider the following safety and privacy requirements:

SAFETY
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.

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

The first requirement is designed for the benefit of the patient and is intended to warn carers that this patient has a history of self harm and that they should therefore watch him or her with a view to preventing or detecting this at an early stage. The second requirement is also supposedly for the benefit of the patient and is intended that patient privacy is maintained. There may be circumstances where a patient does not wish his/her relatives to know that they are attending a mental health clinic.

It is not clear how this conflict can be resolved. It is probably the case that the legal requirements imposed by the Data Protection Act must take precedence so the safety requirement should therefore be amended or rejected.

Another potential conflict may be revealed when the safety and operational costs concerns are compared. Consider the following requirements:

SAFETY
A detailed risk assessment shall be carried out and recorded in the system each time a change in the patient's condition is diagnosed or medication is changed.

OPERATIONAL COSTS
The deployment of the MHCPMS shall not require any additional staff to be employed

These requirements might conflict if a significant time is required for risk assessments. To resolve such a conflict, it might be possible to classify patients as low, medium and high risks and to only re-do risk assessments when a patient's classification changes.

As a final example of conflict, consider the conflict between the functionality required by clinical staff and the security requirement from the medical records viewpoint.

FUNCTIONAL REQUIREMENT

Nurses visiting patients at home should be able to download patient records in advance to a laptop computer, modify these records then upload the records to the server.

SECURITY

All PCs used to run the MHCPMS 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.

It is not practical to assign static IP addresses to mobile systems such as laptops.

Resolution of these conflicts requires discussion with the stakeholders involved to arrive at a compromise situation where requirements that allow system development to proceed can be established. For example, it may be that access from laptops is allowed only on the condition that the laptop disk is encrypte