Security and Confidentiality in Clinical Information Systems

Centre for Health Informatics

Prof John Chelsom

Runs: 3 hours
Tutor: Prof John Chelsom
Mode of attendance: Classroom

Learning Objectives

- This session provides an overview of the issues and technology related to the security and confidentiality of clinical information
- Specific learning objectives are to:

1. Understand issues of information security and confidentiality
2. Identify relevant legislation and guidelines
3. Differentiate between authentication and authorisation
4. Consider technology for information security
5. Consider technology for access control

Security and Confidentiality in Clinical Information Systems

- Issues of Security and Confidentiality
- Identity, Authentication, Authorisation
- Information Security
- Access Control
- Practical Application
- References and Further Reading

Information Sources

- Sources are listed in the references at the end of these slides

Some definitions and descriptions have been taken from quoted resources.

Retrieved October 2010.

Where consensus on definitions or descriptions Is required, these have been taken from Wikipedia.

Retrieved October 2010.

Issues of Security and Confidentiality

NHS Data Security Breaches

NHS board Data Protection Act breach

Thursday, September 30, 2010

Patient details have been put at risk by the Forth Valley NHS Board, the Information Commissioner's Office has said.

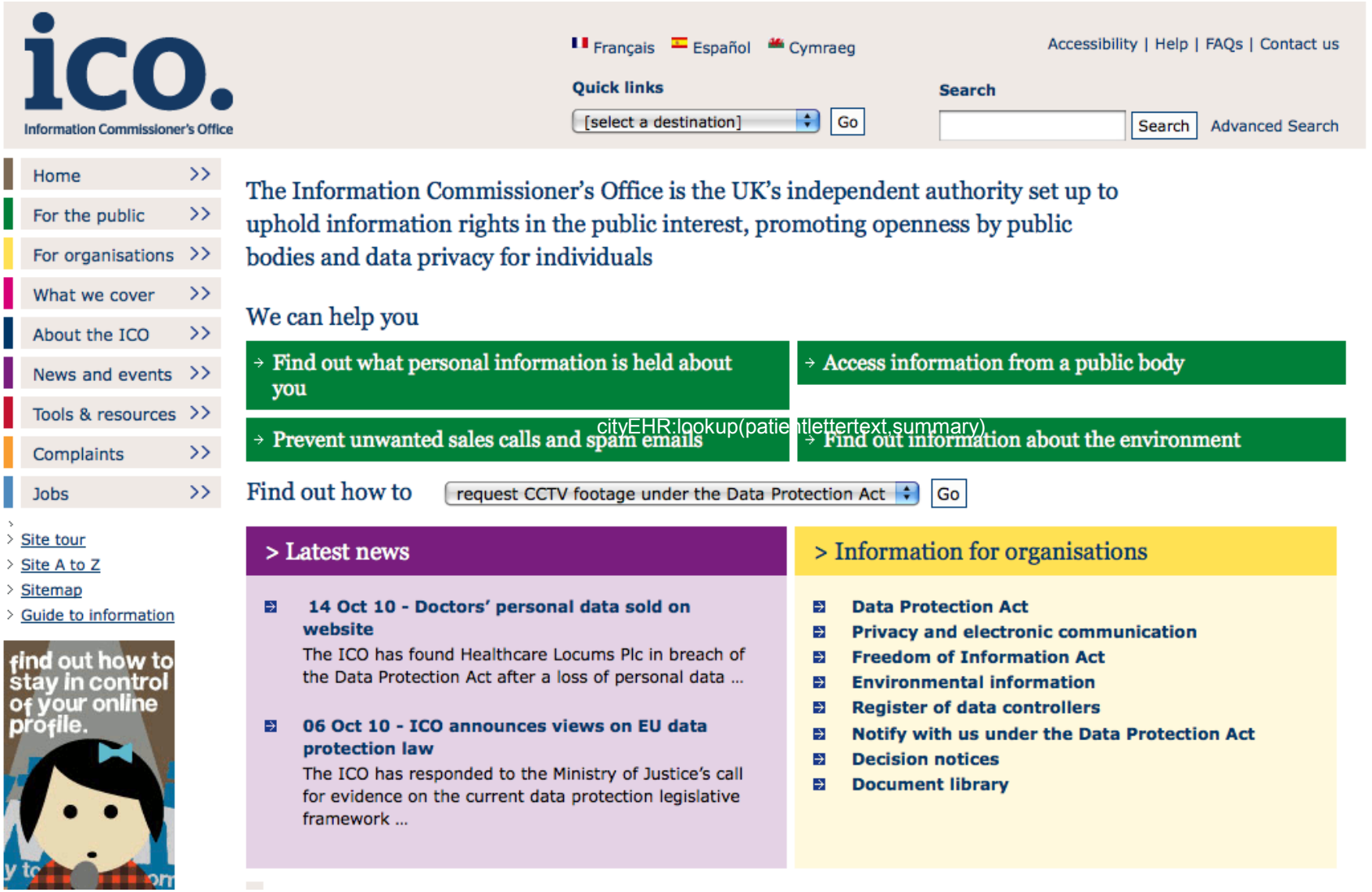
The ICO found the board to be in breach of the Data Protection Act after sensitive personal data relating to patients and board staff was lost.

The ICO said they were informed that an unencrypted memory stick was handed to the press. The personally owned memory stick contained personal information that had been uploaded by a member of staff. This was then lost or stolen.

"This case highlights the importance of health bodies complying with the Data Protection Act when storing and transferring patients' sensitive personal information," said Ken Macdonald, assistant commissioner for Scotland.

http://www.publicservice.co.uk/news_story.asp?id=14296

Information Commissioners



http://www.ico.gov.uk/

But Have We Seen These Headlines?

GP Receptionist Photocopies Health Records

Patient Dies After Surgeon Fails to Access Health Record

Psychiatric Patient Stabs Three in A&E Attack

Relatives Learn of Illness Through Hospital Records

Physiotherapist Reveals Footballer is HIV Positive

What are the Real Problems?

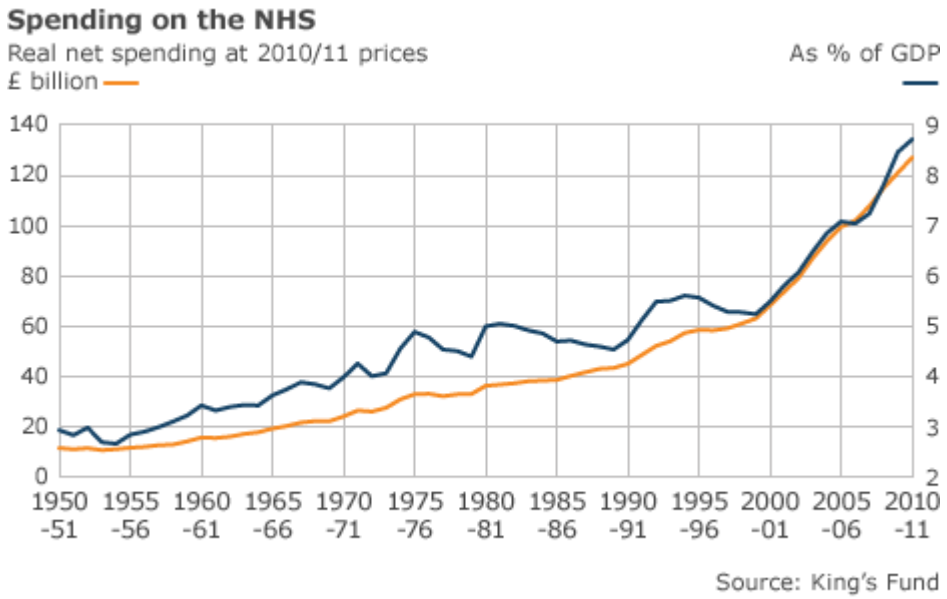
- Keeping information secure is an obvious problem
  - But is relatively easy to solve
- Controlling access to information is a bigger problem
  - Who can see what information
  - When professionals can't see the right information
  - When the rights of individuals conflict
    - Right of confidentiality of a patient
    - Right of protection for a professional

The NHS Plan

A major review of healthcare provision, backed by increased investment.

March, 2000

"The NHS will respect the confidentiality of individual patients and provide open access to information about services, treatment and performance"



What is Information Security?

- Confidentiality. “Information access is confined to those with specified need and authority to read and/or change the information”
- Integrity. “Information accuracy and completeness is safeguarded”
- Availability. “Information is available to authorised users, when required”
- Accountability. “Alteration of information can be traced back to the responsible individual”

To Reduce The Risk Of

- Disruption to the organisation's activities
- Breaches of confidentiality
  Personal privacy
  Organisational confidentiality
- Financial loss
- Failure to meet legal obligations
- Embarrassment to the organisation

Threats to Information Security

- Inaccuracy of records
- Loss/alteration of data
  Accidental
  Intentional
  Theft of equipment
- Disclosure of data to unauthorised parties
  Accidental
  Intentional
- Unavailability of the system or data

Legislation and standards

- 90 Acts of Parliament, Statutory Instruments, Regulations, Orders in Council
- 16 EU Treaty Articles, Directives, Decisions, Proposals
- 7 Other International Agreements and Conventions (Council of Europe, UN, WHO)

Legislation

- Copyright, Designs & Patents Act (1988)
- Access to Health Records Act (1990)
- Computer Misuse Act (1990)
- Data Protection Act (1998)
- Human Rights Act (1998)
- Freedom of Information Act (2000)
- RIP Act (2000)
- Health and Social Care Act (2012)
- Care Act (2014)
- Common Law

Statutory and Organisational Guidance

- Data Protection Act
- Freedom of Information Act
- Others

- Caldicott principles

- NHS Care Records Guarantee

Data Protection Act (1998)

- Everyone processing personal information must be a registered “Data Controller” with the Information Commissioner
- Information must be used only for the purposes it was collected for
- “Data Subjects” have the right to see their records whenever they wish
- “Data Subjects” must give their consent for their information to be shared with other parties

Access to Medical Records

- Previously a separate Act
- Now incorporated in DPA (1998)

How do I access my health records?

- You have a right to access your health records, under the Data Protection Act 1998.
- If you want to read your health records, you can ask in your GP surgery and arrange a time to come in and read them.
- You don't have to give a reason for wanting to see your records. You may be asked to submit your request in writing. It's a good idea to state the dates you want to see, for example from 1995-1998 and to send the letter by recorded delivery and keep a copy. By law, you must receive a response to your letter within 40 days.
- Your GP surgery has your medical records, as well as a summary of any hospital tests or treatment you may have had. Any hospitals where you have had treatment or tests will hold records of this. You can write to the medical records manager at the hospitals medical records department. Your optician and dentist will also hold records about you.
- You may need to show proof of identity before you are allowed access.

How do I access my health records?

- If your records have been updated in the last 40 days (i.e. you have seen your GP or other health professional in the last 40 days) you are entitled to see them at no charge. The charge for a copy of your health records is £10 if they are held on computer. For a copy of older records on paper, and results like X-rays you may have to pay photocopying charges up to a maximum of £50 (in total). Ask the surgery first what they charge before you apply.
- Your family are not allowed to see your health records unless you give them written permission, or they have power of attorney. If you don't have a GP, or you are applying on behalf of someone who has died, you should write to the Medical Records Officer at your local health authority.
- If your GP or other health professional believes that information in the records is likely to cause you or another person serious harm, they may refuse you access to the records.

How do I access my health records?

- If your records have been updated in the last 40 days (i.e. you have seen your GP or other health professional in the last 40 days) you are entitled to see them at no charge. The charge for a copy of your health records is £10 if they are held on computer. For a copy of older records on paper, and results like X-rays you may have to pay photocopying charges up to a maximum of £50 (in total). Ask the surgery first what they charge before you apply.
- Your family are not allowed to see your health records unless you give them written permission, or they have power of attorney. If you don't have a GP, or you are applying on behalf of someone who has died, you should write to the Medical Records Officer at your local health authority.
- If your GP or other health professional believes that information in the records is likely to cause you or another person serious harm, they may refuse you access to the records.

Caldicott Principles

- Justify the purposes for which information is required
- Don’t use patient identifiable information unless it is absolutely necessary
- Use the minimum necessary patient identifiable information
- Access to information should be on a strict need to know basis
- Everyone with access should be aware of their responsibilities
- Understand and comply with the law

The Caldicott Committee (December 1997). "The Caldicott Report". Department of Health.

Read the principles again…

- They don’t say “named patient”…
- They don’t mention a particular medium…

Caldicott mnemonic: FIONA C

F Formal justification of purpose

I Information transferred only when absolutely necessary

O Only the minimum required

N Need to know access controls

A All to understand their responsibilities

C Comply with and understand the law

Caldicott mnemonic: FIONA C

F Formal justification of purpose

I Information transferred only when absolutely necessary

O Only the minimum required

N Need to know access controls

A All to understand their responsibilities

C Comply with and understand the law

Caldicott Update, 2013

Information Governance Review, Fiona Caldicitt 2013

Led to a report from the HSCIC

"A guide to confidentiality in health and social care"

www.hscic.gov.uk/confguideorg

Rule 1

Confidential information about service users or patients should be treated confidentially and respectfully.

Rule 2

Members of a care team should share confidential information when it is needed for the safe and effective care of an individual.

Rule 3

Information that is shared for the benefit of the community should be anonymised.

Rule 4

An individual's right to object to the sharing of confidential information about them should be respected.

Rule 5

Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

HIPPA

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191) [HIPAA] was enacted by the U.S. Congress in 1996.

Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.

Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

The Administration Simplification provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system.

http://en.wikipedia.org/wiki/HIPPA

The HIPPA Privacy Rule

The HIPAA Privacy Rule regulates the use and disclosure of certain information held by "covered entities" (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions.)

It establishes regulations for the use and disclosure of Protected Health Information (PHI). PHI is any information held by a covered entity which concerns health status, provision of health care, or payment for health care that can be linked to an individual.

This is interpreted rather broadly and includes any part of an individual's medical record or payment history.

http://en.wikipedia.org/wiki/HIPPA

The HIPPA Privacy Rule

The HIPAA Privacy Rule regulates the use and disclosure of certain information held by "covered entities" (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions.)

It establishes regulations for the use and disclosure of Protected Health Information (PHI). PHI is any information held by a covered entity which concerns health status, provision of health care, or payment for health care that can be linked to an individual.

This is interpreted rather broadly and includes any part of an individual's medical record or payment history.

http://en.wikipedia.org/wiki/HIPPA

The HIPPA Security Rule

The Security Rule complements the Privacy Rule. While the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (EPHI).

It lays out three types of security safeguards required for compliance: administrative, physical, and technical. For each of these types, the Rule identifies various security standards, and for each standard, it names both required and addressable implementation specifications.

Required specifications must be adopted and administered as dictated by the Rule. Addressable specifications are more flexible. Individual covered entities can evaluate their own situation and determine the best way to implement addressable specifications.

http://en.wikipedia.org/wiki/HIPPA

Administrative Safeguards

Physical Safeguards

Technical Safeguards

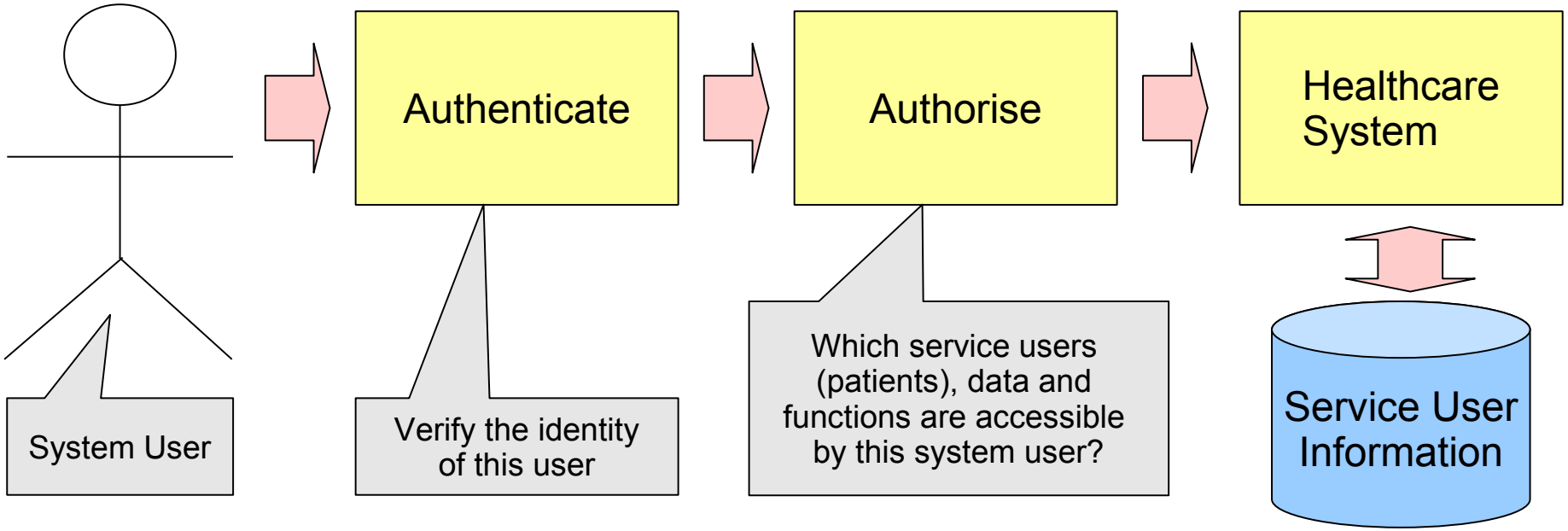
Practical Guidance

- Always focus on protecting the data, not just the infrastructure, and not simply adherence to regulation
- Identify common technologies for achieving best-practice information protection
- Use standard language and definitions to convey the need for NHS regulatory compliance
- Investigate rule sets used by other organisations in the handling of large volumes of confidential information
- Clean up the data "toxic waste dump" by deleting low-value / high risk data, if permissible, and actively reconcile conflicting regulations
- Develop a penalty matrix
- Regard the security rules and regulations as an ongoing process, not just a huge panic to get things in order a week before the compliance auditor comes in
- Remember that liability for data breaches cannot be outsourced

http://www.bjhcim.co.uk/features/2007/703005.htm

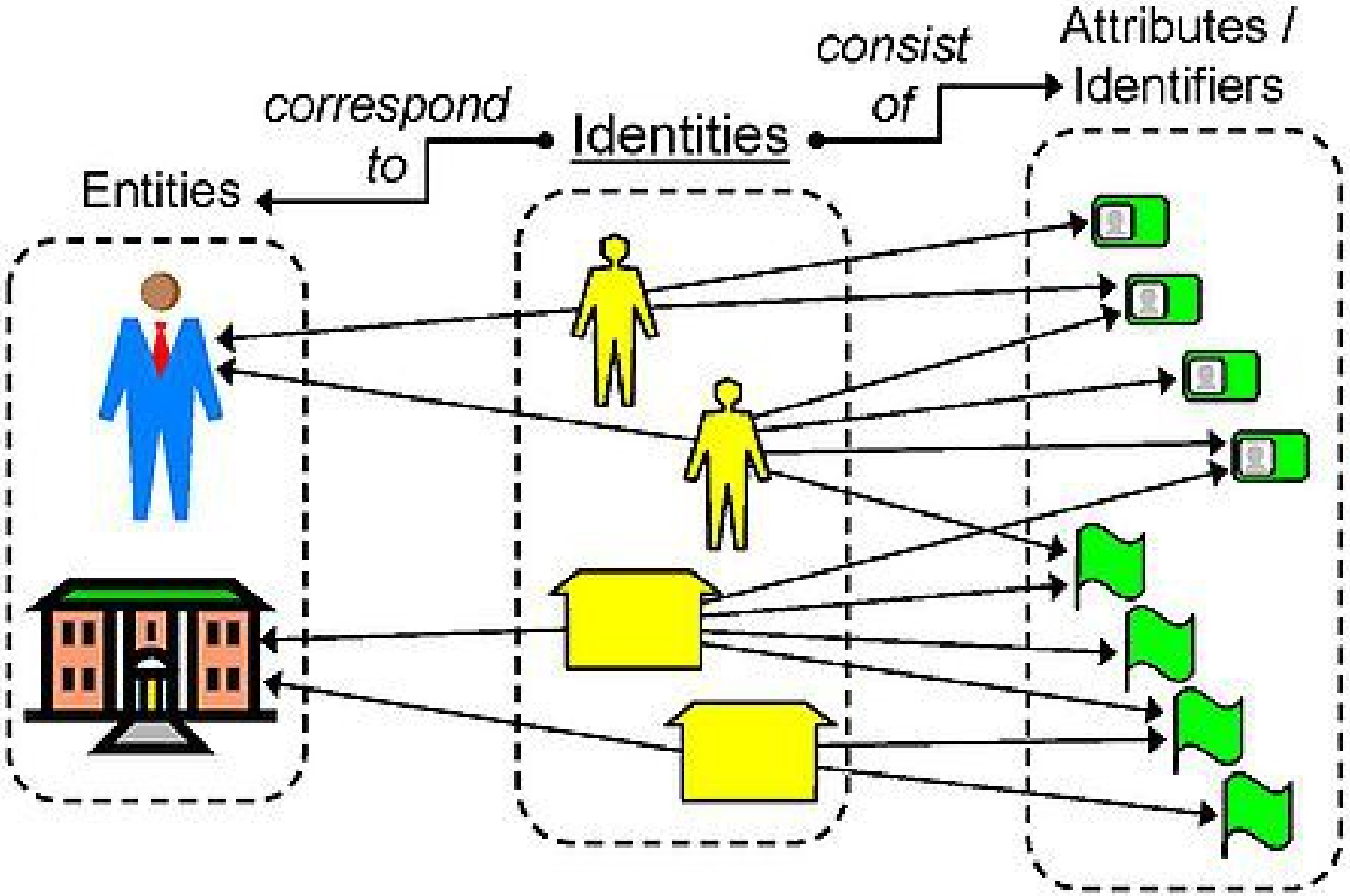
Identity, Authentication, Authorisation

Authentication and Authorisation



- System user must be *authenticated* and then
- *authorised* to access service user information

Identity



http://en.wikipedia.org/wiki/File:Identity-concept.jpg

Authentication

Authentication is the act of establishing or confirming something (or someone) as authentic, that is, that claims made by or about the subject are true. This might involve confirming the identity of a person...

http://en.wikipedia.org/wiki/Authentication

Four factors typically used to provide authentication

- Something you know, such as a password or a personal identification number (PIN). This assumes that only the owner of the account knows the password or PIN needed to access the account.
- Something you have, such as a smart card or security token. This assumes that only the owner of the account has the necessary smart card or token needed to unlock the account.
- Something you are, such as fingerprint, voice, retina, or iris characteristics.
- Where you are, for example inside or outside a company firewall, or proximity of login location to a personal GPS device.

Authorisation

Authorisation is the function of specifying access rights to resources, which is related to information security and computer security in general and to access control in particular. More formally, "to authorise" is to define access policy.

http://en.wikipedia.org/wiki/Authorisation

Access control in computer systems and networks relies on access policies.

The access control process can be divided into two phases

1. Policy definition phase
2. Policy enforcement phase.

Authorization is the function of the policy definition phase which precedes the policy enforcement phase where access requests are granted or rejected based on the previously defined authorizations.

Access Control

In computer security, access control includes authentication, authorization and audit. It also includes measures such as physical devices, including biometric scans and metal locks, hidden paths, digital signatures, encryption, social barriers, and monitoring by humans and automated systems.

http://en.wikipedia.org/wiki/Access_control

- In general, three type of access are possible
- Read (R): The subject can
  - Read/view the information
  - Obtain a list of what information is present
- Write (W): The subject can perform CRUD actions
  - Create
  - Read
  - Update
  - Delete
- Execute (X): If the file is a program, the subject can cause the program to be run.

Single Sign On (SSO)

Single sign-on (SSO) is a property of access control of multiple, related, but independent software systems. With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them. Single sign-off is the reverse property whereby a single action of signing out terminates access to multiple software systems.

As different applications and resources support different authentication mechanisms, single sign-on has to internally translate to and store different credentials compared to what is used for initial authentication.

http://en.wikipedia.org/wiki/Single_sign-on

- For example
  - Log on to use clinic system by swiping a Smart Card
  - Then click through to order lab tests, prescribe medication, view diagnostic images
  - For each system, need log on *plus* access to the current patient record

Identifying Patients

- Clinical information systems generally use a single identifier to uniquely identify each patient so that data can be assigned to the record for identified patient
- Some systems will use a published (external) identifier such as the Hospital Number, Körner Number or NHS Number
- Since these identifiers are often imperfect, or may be unknown for any specific patient, many system use their own internal identifier

- EHR systems often hold data that has been aggregated from many different clinical systems, each with their own identifier.

- A Master Patient Index (MPI) manages the set of identifiers for a patient set (with distinct members). It can be used to 'broker' the identifier required to process data from different systems
- Rather than rely on the accuracy of a single identifier, system often require a match on more than one identifier attribute
  - e.g. NHS Number, plus surname, birth date and gender

Anonymising Patient Data

- Patient data used in studies or trials can often be anonymised or pseudo-anonymised

- "Anonymisation Standard for Publishing Health and Social Care Data Specification"
  - NHS Information Standards Board, 2013
  - http://www.isb.nhs.uk/library/standard/128

This process standard provides an agreed and standardised approach, grounded in the law, enabling organisations to:

Distinguish between identifying and non-identifying information

Deploy a standard approach and a set of standard tools to anonymise information to ensure that, as far as it is reasonably practicable to do so, information published does not identify individuals.

Anonymisation Process

- Remove or replace (pseudo-anonymisation) patient identifiers
  - Patient identity number(s)
  - Name
  - Address

- Handle other identifying parameters
  - Dates (including Date of Birth)
  - Postcode
  - Gender
  - Ethnicity
  - Employer
  - Occupation or staff group

Information Security

Encryption

In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

The result of the process is encrypted information (in cryptography, referred to as ciphertext).

In many contexts, the word encryption also implicitly refers to the reverse process, decryption (e.g. "software for encryption" can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted).

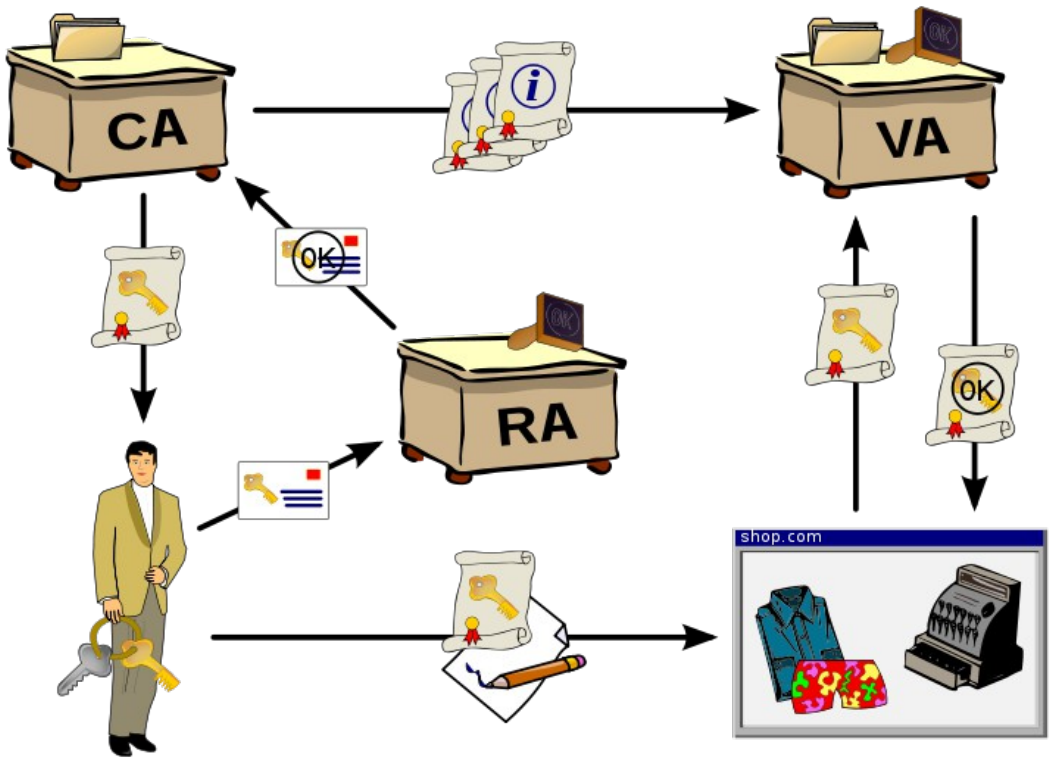
http://en.wikipedia.org/wiki/Encryption

Public Key Infrastructure

Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates

http://en.wikipedia.org/wiki/Public_key_infrastructure

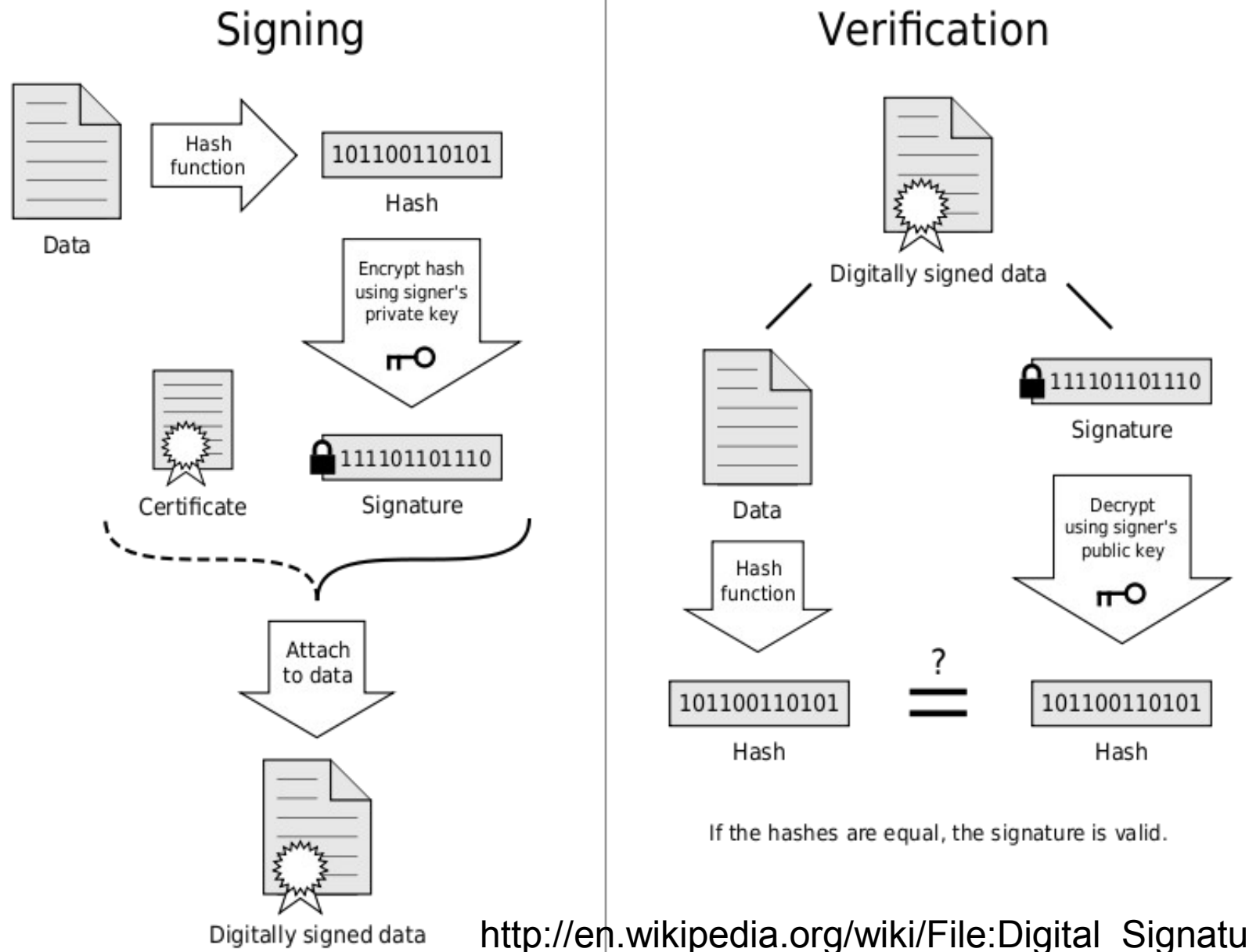
Principles of PKI



A user applies for a certificate with his public key at a registration authority (RA). The latter confirms the user's identity to the certification authority (CA) which in turn issues the certificate. The user can then digitally sign a contract using his new certificate. His identity is then checked by the contracting party with a validation authority (VA) which again receives information about issued certificates by the certification authority.

http://en.wikipedia.org/wiki/Public_key_infrastructure

Digital Signatures



http://en.wikipedia.org/wiki/File:Digital_Signature_diagram.svg

Access Control

Role-Based Access Control

Within an organization, roles are created for various job functions. The permissions to perform certain operations are assigned to specific roles.

Members of staff (or other system users) are assigned particular roles, and through those role assignments acquire the permissions to perform particular system functions.

Since users are not assigned permissions directly, but only acquire them through their role (or roles), management of individual user rights becomes a matter of simply assigning appropriate roles to the user; this simplifies common operations, such as adding a user, or changing a user's department.

http://en.wikipedia.org/wiki/Role_based_access_control

Legitimate Relationships

Full Role-based Access Control was too difficult to implement on a large scale for the NHS Care Records Service

A legitimate relationship (LR) is an electronic record stored on the Spine. It details the care relationship between a patient and a healthcare professional (or group of healthcare professionals).

It is used to restrict access so only the healthcare professionals involved in the patient's care can access clinical information.

In order to determine if a legitimate relationship exists, the healthcare professional must first uniquely identify the patient. This is done by tracing the patient's demographic record on the Personal Demographics Service.

Therefore the healthcare professional requires access to the patient's demographics record prior to determining if a Legitimate Relationship exists.

http://www.connectingforhealth.nhs.uk/systemsandservices/demographics/pds/ig/access/LR

Currently see: systems.hscic.gov.uk/demographics/pds/ig/access/access_pds.pdf

Sealed Envelopes

Sealed Envelopes were to be implemented as part of the Access Control Framework of the NHS Care Records Service.

The NHS Care Records Service will enable users to limit access to sensitive information within patient records.

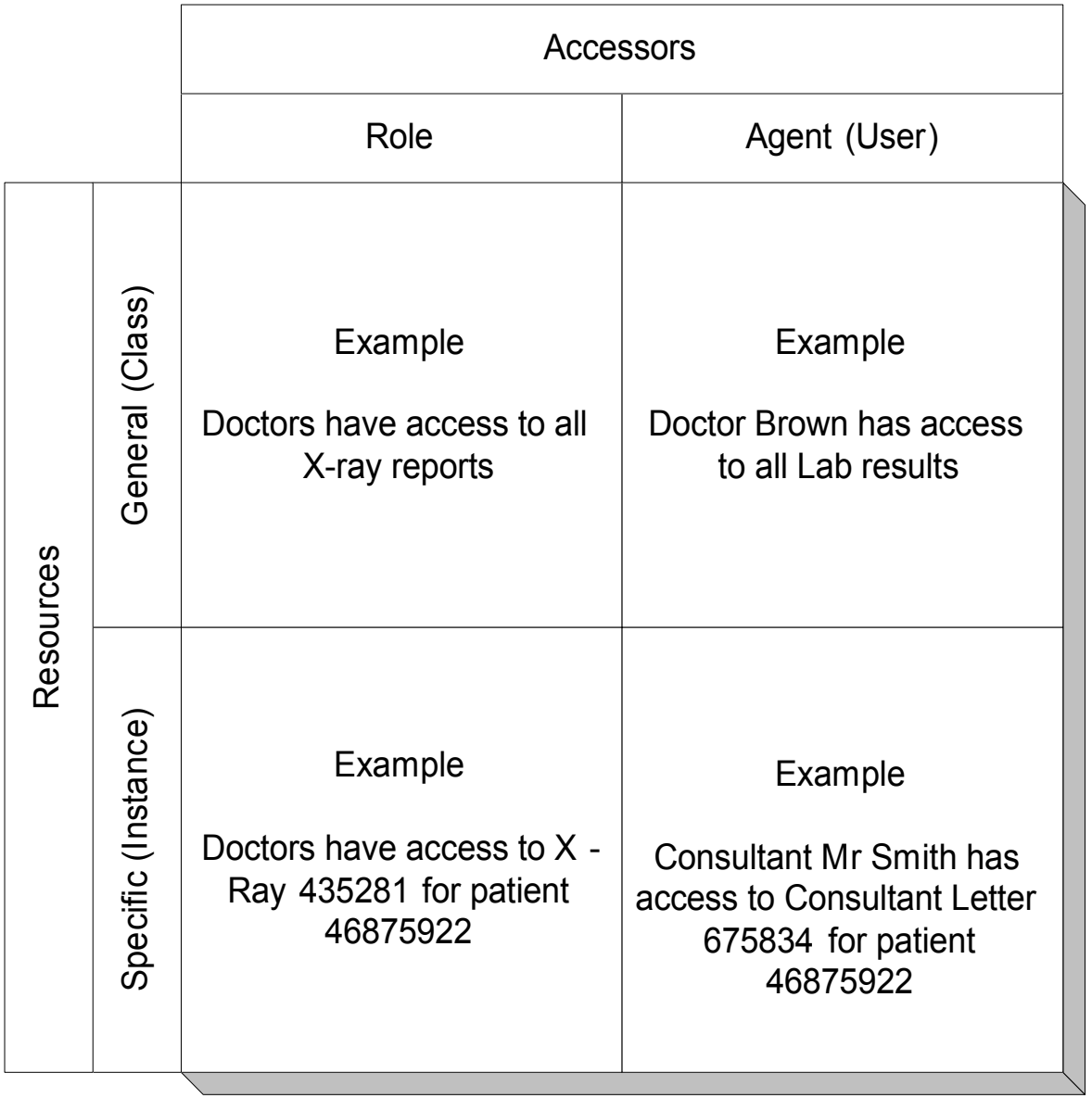
A patient will be able to request that specific sensitive information within their clinical record is accessible only with their consent. This is sometimes referred to as a patient "sealed envelope".

A clinician 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.

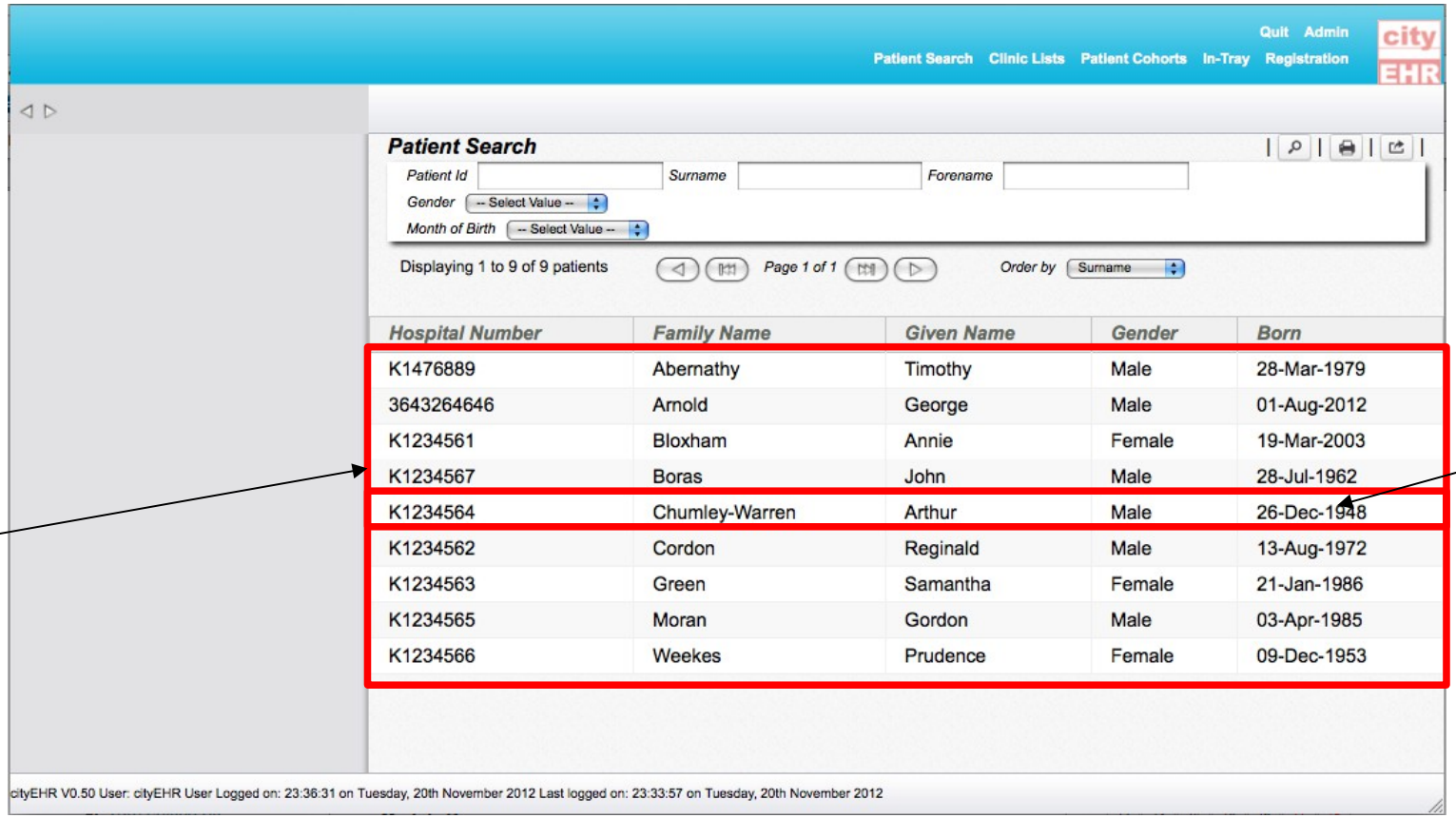
http://www.connectingforhealth.nhs.uk/systemsandservices/demographics/pds/ig/access/LR
Currently see: systems.hscic.gov.uk/demographics/pds/ig/access/access_pds.pdf

Tees Access Control Model



- Extended version of the Tees model developed through ERDIP and NHSIA
- Anything that can be accessed is a "Resource"
- Anything that can access a Resource is an "Accessor"
- Both resources and accessors have an associated "Type"
- A "User" is an Accessor Type and called an "Agent" in the "Tees" model
- Can be used to implement the concept of a 'sealed envelope'

Access to Patients



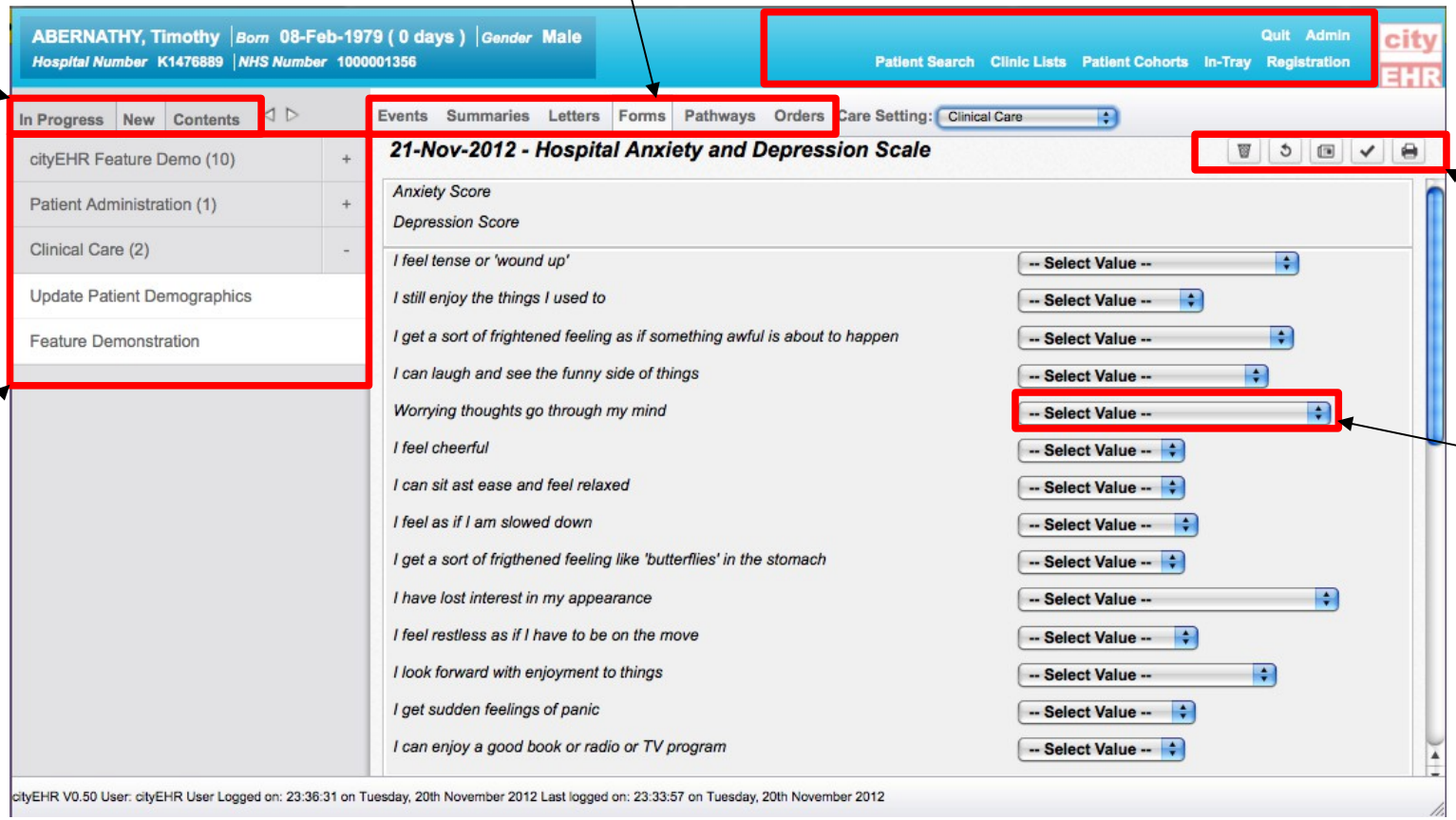
View Patients

Access Patient Record

System user must have a legitimate relationship with the patient

- See that the patient is on the system
- Update the patient record

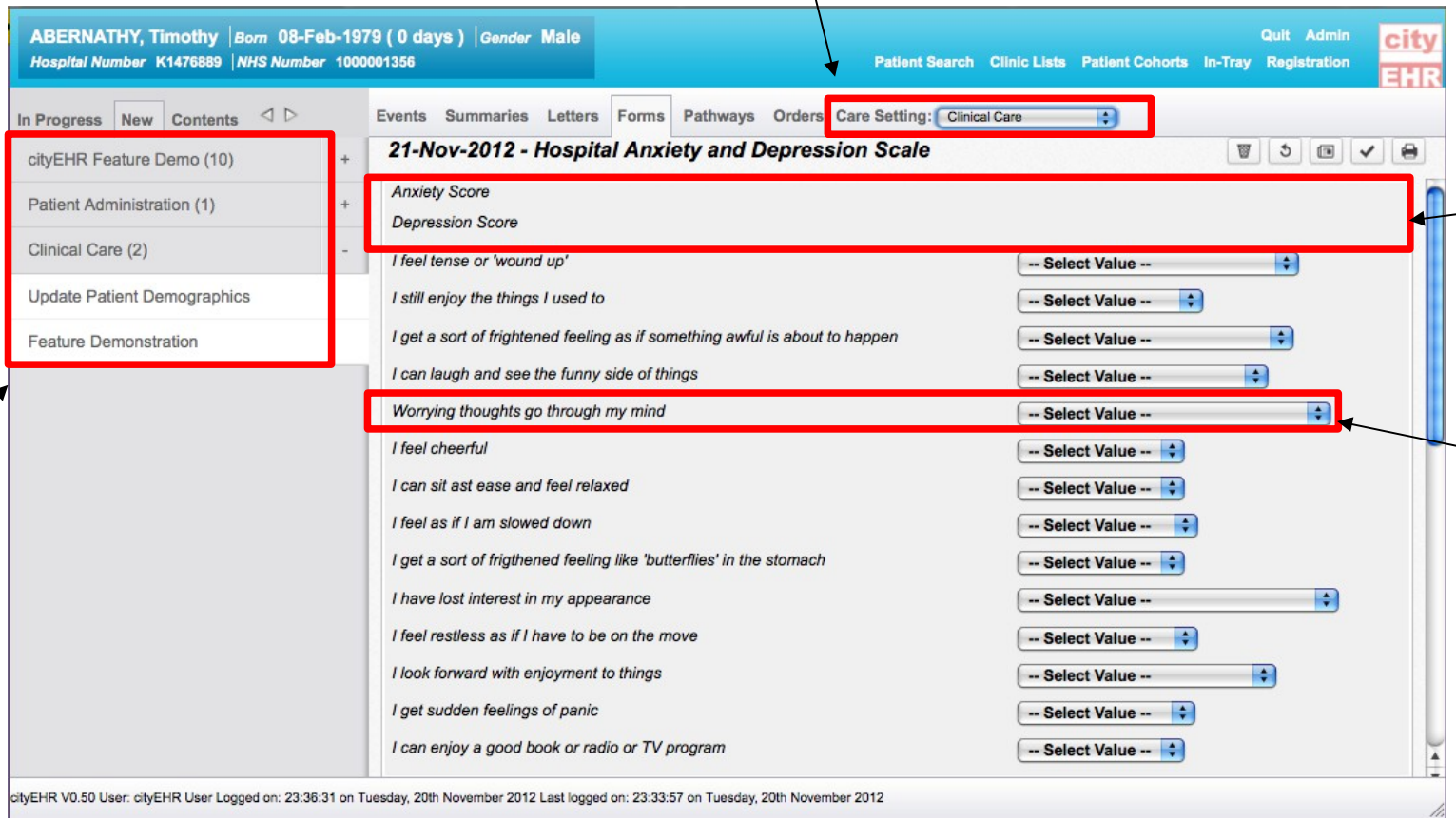
Access to Functions



System must have clear separation of user functions

With the means to configure and control access

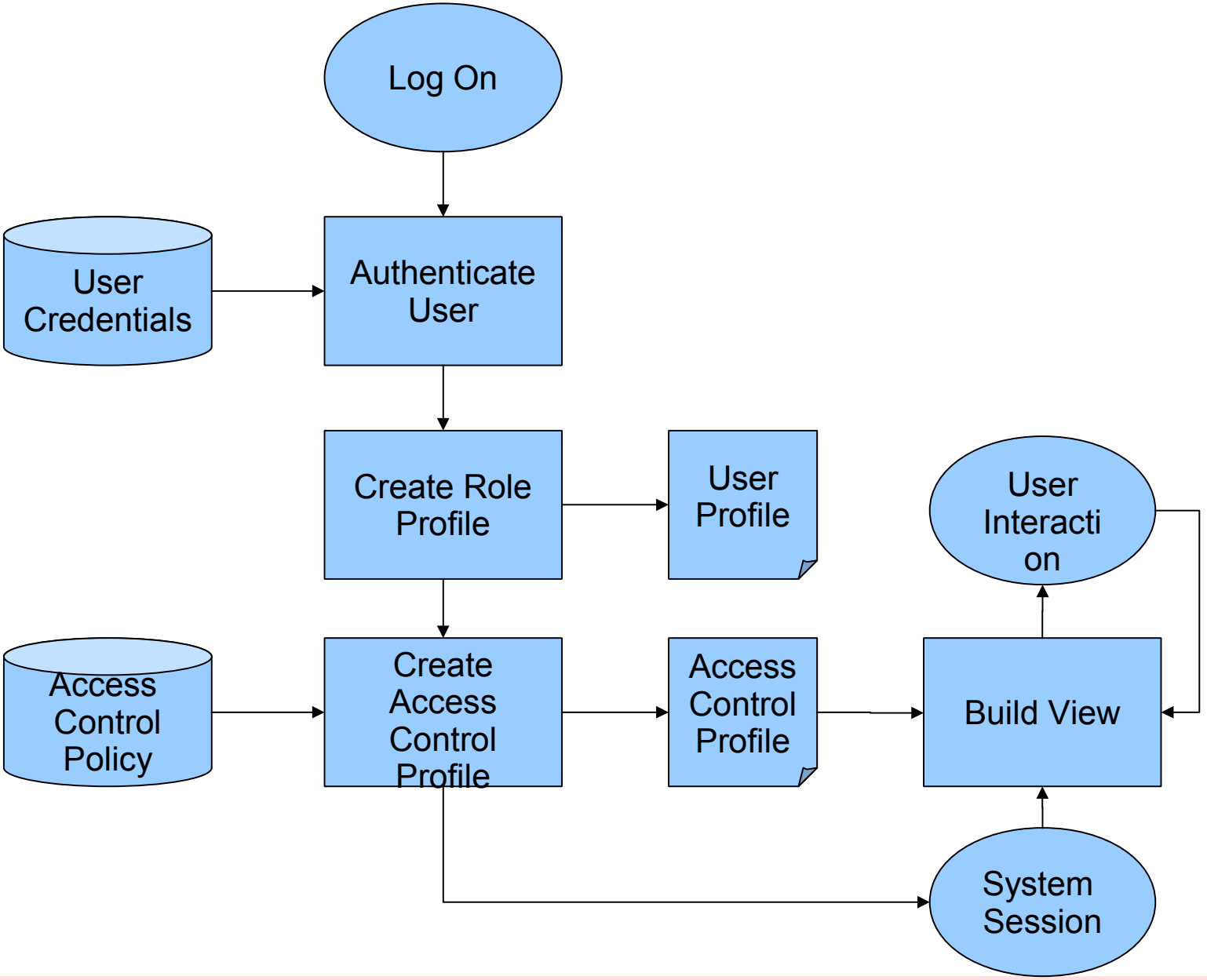
Access to Data



System must have clear identification of data components

With the means to configure and control access

Applying Access Control



Access Control Rules – XACML

XACML stands for eXtensible Access Control Markup Language. The standard defines a declarative access control policy language implemented in XML and a processing model describing how to evaluate access requests according to the rules defined in policies.

http://en.wikipedia.org/wiki/XACML

Subjects perform *Actions* on *Resources* in a particular *Environment*

Decision - "Permit" or "Deny"

- Is this Subject authorised to perform this Action on this Resource?

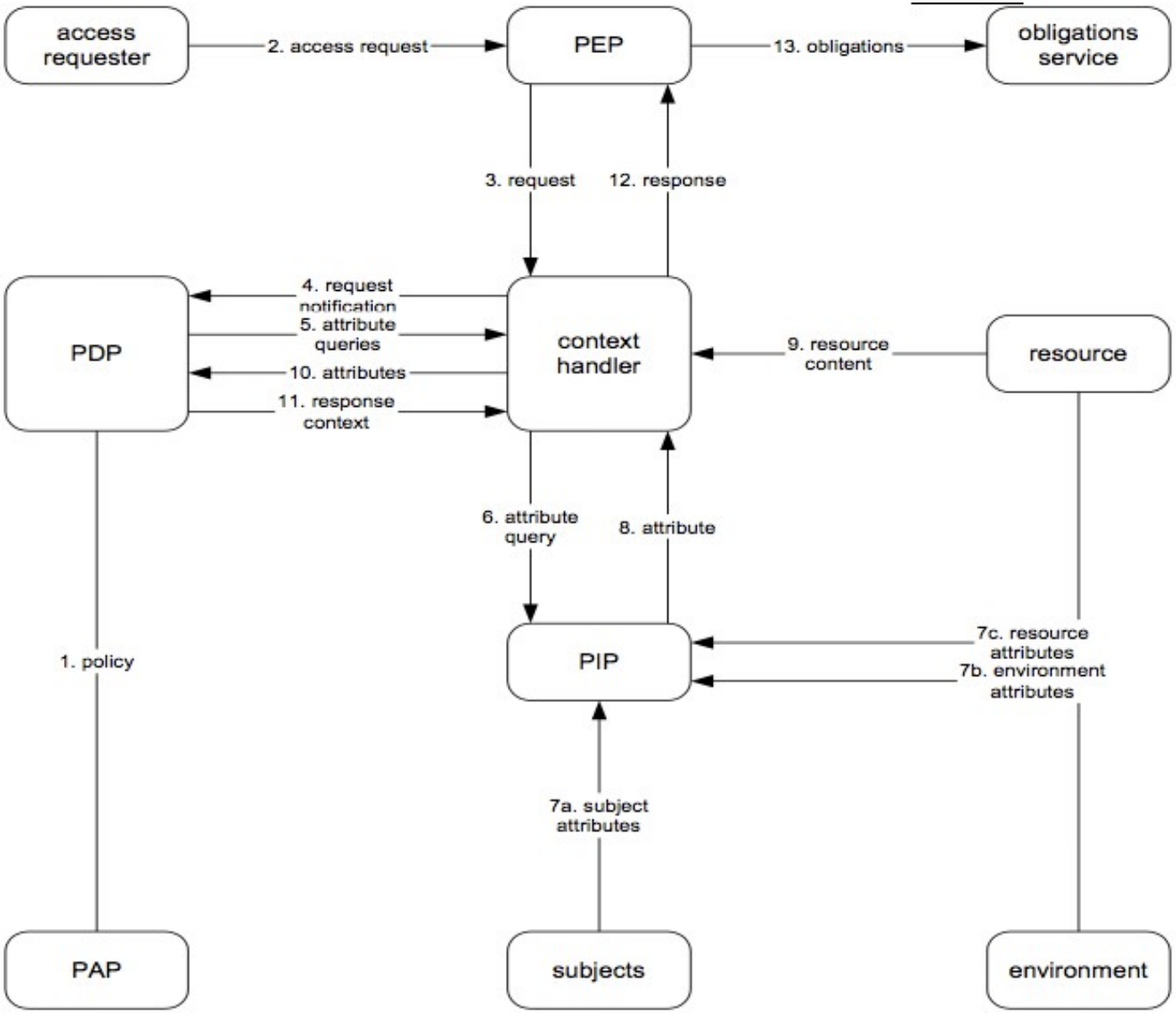
To answer this decision request, the Access Control System evaluates a set of rules which consider attributes of the subject, action, resource and environment.

If the action is permitted then the decision may be qualified by advice (which should be followed) and/or obligations (which must be followed).

XACML Definitions

- Rule - A target, an effect, a condition and (optionally) a set of obligations or advice. A component of a policy
- Policy - A set of rules, an identifier for the rule-combining algorithm and (optionally) a set of obligations or advice. May be a component of a policy set
- Target - The set of decision requests, identified by definitions for resource, subject and action that a rule, policy, or policy set is intended to evaluate
- Effect - The intended consequence of a satisfied rule (either "Permit" or "Deny")
- Condition - An expression of predicates. A function that evaluates to "True", "False" or “Indeterminate”
- Predicate - A statement about attributes whose truth can be evaluated
- Attribute - Characteristic of a subject, resource, action or environment that may be referenced in a predicate or target
- Policy administration point (PAP) - The system entity that creates a policy or policy set
- Policy decision point (PDP) - The system entity that evaluates applicable policy and renders an authorization decision
- Policy enforcement point (PEP) - The system entity that performs access control, by making decision requests and enforcing authorization decisions.
- Policy information point (PIP) - The system entity that acts as a source of attribute values.
- Authorization decision - The result of evaluating applicable policy, returned by the PDP to the PEP. A function that evaluates to “Permit”, “Deny”, “Indeterminate” or “NotApplicable", and (optionally) a set of obligations and advice
- Obligation - An operation specified in a rule, policy or policy set that should be performed by the PEP in conjunction with the enforcement of an authorization decision.
- Advice - A supplementary piece of information in a policy or policy set which is provided to the PEP with the decision of the PDP.

The XACML Data Flow Model



Evaluating Conditions

If all the attributes required to evaluate a condition are available, then it can be evaluated to “Deny” or “Permit”, depending on the effect defined for the rule.

But if the conditions cannot be evaluated then the decision is deemed to be indeterminate.

Indeterminate{D}

- an “Indeterminate” from a policy or rule which could have evaluated to “Deny”, but not “Permit”

Indeterminate{P}

- an “Indeterminate” from a policy or rule which could have evaluated to “Permit” but not “Deny”

Indeterminate{DP}

- an “Indeterminate” from a policy or rule which could have evaluated to “Deny” or “Permit”.

Combining Rules

- Rule Combining Algorithms determine how rules should be evaluated together (e.g. what should happen if access control rules conflict)
- These algorithms may be specific to a particular application, but there are also some general algorithms that can be applied
- For example, some general algorithms are included in the XACML standard

The “Permit-unless-deny” combining algorithm is intended for those cases where a deny decision should have priority over a permit decision, and an “Indeterminate” or “NotApplicable” must never be the result. It is particularly useful at the top level in a policy structure to ensure that a PDP will always return a definite “Permit” or “Deny” result. This algorithm has the following behavior.

- 1. If any decision is "Deny", the result is "Deny".
- 2. Otherwise, the result is "Permit".

The "First-Applicable” rule-combining algorithm of a policy.

- Each rule SHALL be evaluated in the order in which it is listed in the policy.
- For a particular rule, if the target matches and the condition evaluates to "True", then the evaluation of the policy SHALL halt and the corresponding effect of the rule SHALL be the result of the evaluation of the policy (i.e. "Permit" or "Deny").
- For a particular rule selected in the evaluation, if the target evaluates to "False" or the condition evaluates to "False", then the next rule in the order SHALL be evaluated.
- If no further rule in the order exists, then the policy SHALL evaluate to "NotApplicable".

Some Examples

An NHS Trust has policies for “Clinician Use of Patient Records” and “Patient Rights to Access of their Health Record”

Rules in “Clinician Use of Patient Records” :

- Any clinician can see any record for the purposes of clinical care
- Data that puts clinicians at risk should not be shared with patients

Rules in “Patient Rights to Access of their Health Record”

- Any patient may have access to their own record
- A patient may request that access is denied for any named clinician

Practical Application

Practical Application in an NHS Trust

People involved

- Patients
- Clinicians
- Managers

- Information Security Manager
- Data Protection Officer
- Caldicott Guardian
- Head of Information Governance

Information Security Policy

- Specifies Trust's responsibilities
- Provides framework of standards and procedures
- Needs Senior Management support

- Includes
  - Information Classification
  - Laptop Policy
  - Third Party Connection
  - Remote Access
  - Back-up Procedures
  - Fax policy
  - Acceptable Use of Internet and E-mail

e.g. Mid Yorkshire Hospitals NHS Trust

http://www.midyorks.nhs.uk/NR/rdonlyres/A4010A2B-65BD-4EFD-8F43-CE6BE5839961/68209/infosecpolicy.pdf

Information Security - Key Issues

- Virus protection
- Intrusion detection
- Off site equipment - encryption
- Business continuity
- Disposal of equipment

- Behaviour

BS 7799 compliance

- First a UK, now an ISO standard (ISO 27000 series) that covers
  - Best practices for Information Security Management
  - Information Security Management Systems - Specification with guidance for use.
  - Risk analysis and management
- A long-haul procedure, usually takes two years to reach compliance.
- Gap analysis
- Security Improvement Programme
- Action Plan
- Certification

Compliance with Data Protection Act

- Protocols for collection, processing and storage of information.
- Protocols for dealing with requests for access to records.
- Retention and destruction of records
- Information Sharing Protocols
- Information for Data Subjects

- Issues related to consent
- Medical research

Compliance with Caldicott

- Use of the NHS number
- Active role of the Caldicott Guardian to monitor information flows
- Awareness of staff

References and Further Reading

References and Further Reading

1. "NHS confidentiality code of practice". (2003) Department of Health. http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100550

2. The Caldicott Committee (December 1997). "The Caldicott Report". Department of Health. http://confidential.oxfordradcliffe.net/caldicott/report.

3. American College of Radiology. (2009) ACR–SIIM Practice Guideline for Electronic Medical Information Privacy and Security. Available online at: http://www.acr.org/SecondaryMainMenuCategories/quality_safety/guidelines/med_phys/electronic_medical_info.aspx

4. JJ Longstaff, MA Lockyer, J Nicholas (2003) The Tees Confidentiality Model: an authorisation model for identities and roles. ACM SACMAT 2003, Como, Italy, June 2003.

5. Mike Howse. (2007) Security Matters. The British Journal of Healthcare Computing & Information Management. Available online at: http://www.bjhcim.co.uk/features/2007/703005.htm

References and Further Reading

1. Connecting for Health (2006). “Sealed Envelopes” Briefing Paper: “Selective Alerting” Approach. Available online at: http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/confidentiality/sealedpaper.pdf
2. J Longstaff (2009). Messages and Overrides – enhancements to Sealed Envelope authorisation. BCS. HC 2009. Available online at: http://www.health-informatics.org/HC2009/P10_Longstaff.pdf
3. Department of Health (2000). The NHS Plan: a plan for investment, a plan for reform. Available online at: http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4002960