LEIDEN UNIVERSITY MEDICAL CENTER

2014 EBMT European Society for Blood and Marrow Transplantation 40th Anniversary Saving lives since 1974

Data confidentiality
Protecting privacy in medical research

Henk Jan van der Wijk
Leiden University Medical Center (LUMC)

Tuesday 1st April 2014 from 11.30 – 12.00

Data confidentiality requested topics

- Explanation of different aspects of Data Confidentiality – e.g. mail, email, storing, transfer and access to Database.
- European Legislation
- Describe set up used for Data Confidentiality
- Describe pitfalls with Data Confidentiality
- Explanation of encryption
- How to send data to EBMT offices (protected)

Privacy and confidentiality

- Privacy
  - Wikipedia: from *privo* "to deprive“, the ability of an individual or group to seclude themselves or information about themselves and thereby express themselves selectively.
  - Cambridge dictionaries: Someone's right to keep their personal matters and relationships secret.
  - Oxford dictionaries: A state in which one is not observed or disturbed by other people.
- Confidentiality
  - Wikipedia: a set of rules or a promise that limits access or places restrictions on information
- Data
  - Merriam-Webster: facts or information used usually to calculate, analyze, or plan something
- Risk
  - Wikipedia: the potential of losing something of value, weighed against the potential to gain something of value

Legislation with technological advances

- Aristotle's distinction between the public sphere of political activity and the private sphere
- 19th century: Photography and newspapers
- Now: Computer technology
  - Financial record
  - Health record
  - Telephone records
  - Social media
  - Websites and services (e.g. Google search)
  - Governmental security agencies after 9/11
  - International servers and legislation

Responsibilities for data protection

- Many parties involved in medical research
- No data ownership in legal sense, but
  - Control of the data and databases
  - Rights
    - Holder of the data on use
    - Patient on popper use and correct information
  - Obligations
    - Currently the holder of the registration has to take adequate measures for data protection
  - Intellectual property

European legislation and guidelines

- EU directives for protecting data
  - Medical Contract Bill (WGBO)
  - Data protection directive (WBP)
  - Clinical trials directive and good clinical practice directive (WMO)
  - Guidelines for other medical research such as observational studies
- New European privacy directive
  - Anyone processing personal information will be responsible for the security

General implications

- The right to know where and how personal information is being used
  - Implicit e.g. medical records
  - Explicit other use e.g. medical research
- The right to demand that their privacy sensitive information will be kept confidential
  - Secure storage
  - Access control
  - Security management
  - Audit trail

Identifiability in information

- Personal information
  - Direct identifiable information
    - Easily to relate to a person
    - Name, address, social security number, etc
  - Indirect identifiable information
    - Not directly to relate to a person, but can with some effort
    - Study number, combination of information, e.g. rare disease, birthdate, treating hospital, etc
- Anonymous information
    - Very difficult or impossible to relate to person

Information processing in medical research

- The medical research data processes
  - Gathering information
    - Medical records
    - Forms and questionnaires
  - Storing the information
    - Research database (Promise/Remedy)
  - Processing the information
    - Quality reports
    - (Statistical) analysis
  - Request follow-up data
  - Report findings to patients

Protecting medical research data

- Restrict access to the actually required data for each specific purpose
- Use privacy enhancing techniques
  - Remove identifying information
  - Replace by study number
  - Use encryption
- Informed consent: What data is stored, where is the data stored, for how long, who will have access and for what purpose will the data be used

Encryption

- Original value, e.g. “Hello”, “Mister X”
- Algorithms
  - Hash e.g. SHA256
  - Symmetric encryption e.g. AES256
  - Public-private key encryption e.g. RSA
- Key e.g. “R7NKwYw1vHU91YIg/3ewFtv6EL0mn4bHzWPwsaoqnIY=“
- Cypher e.g. “PIgnHrwxyZ0EBb1eUFmUDQ==“

Encryption use

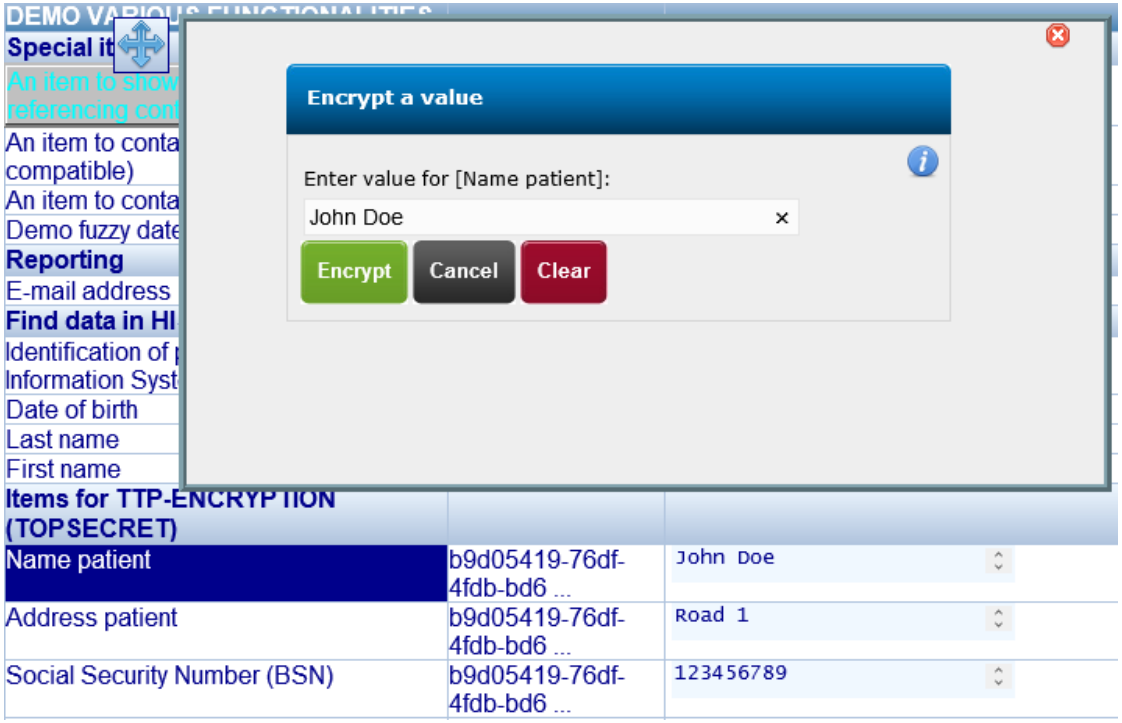
- Use for strong “password” protection of data files and messages
- Example software
  - https websites
  - Pretty Good Privacy (PGP)
  - TrueCrypt
  - Winzip
  - Special hard disks and USB sticks
  - Email S/MIME
  - Many more software products

Encryption not a complete solution

- keys/certificates vs passwords
  - Cannot be changed
  - Cannot be locked or revoked
  - Much longer, e.g. 32 characters
  - More difficult to manage
    - How to safely exchange keys?
    - What if key lost or compromised?
    - How to share access to data?
- Where to store data after decryption

TRES : Trusted Reversible Encryption Service

- Fully integrated in Clinical Data Management System (CDMS)



TRES : Trusted Reversible Encryption Service

- Dual Control – Access to identifying data only after authentication by CDMS as well as the Tres software
- Separation of duties – CDMS authorizes access to data, TTP authorizes decryption and thereby access to identification
- Split Knowledge – TTP has no access to the data and CDMS has no knowledge on decrypt permissions.
- www.zorgttp.nl

Zorg TTP
Privacy & Vertrouwen

Security awareness

- Security always involves extra work. Know that security is required and necessary and act responsible.
- Keep usernames and passwords personal and save.
- Keep paper document locked away
- Store data files on a protected network drive
- Act responsible: Make sure your computer is save, e.g. install updates, adequate virus scanner, don’t use for inappropriate websites, respond when indication of virus, etc.

Email

- Email easily forwarded and copied, so assume not save
- Password-Protection: further advice
  - 1) Password protect whatever file you need to send (access, excel, word, etc)
  - 2) Rename the file so that the file extension (.mdb, .xls, .doc, etc) is removed
  - 3) Zip the file if it is too big (optional)
  - 4) Inform the recipient what type of file it is and advise them to rename the file to add the corresponding extension. If this still does not work, please contact the Central Registry Office for help

Pitfalls – Security is more than a password

- Certification Information security: ISO 72001 / NEN 7510
- Manage every possible risk
- Processes documented and managed
  - Not just work processes, but also management processes.
- Have an Information Security Management System (ISMS)
  - Asset and risk analysis, controls, policy, measures and procedures
  - Incident registration and calamity response team
  - Audits

Conclusion

- A responsible way of working with privacy sensitive medical information for research includes:
  - Inform patients about the use of their data
  - Restrict access to the information required for each purpose
  - Protect the information from misuse

Questions?