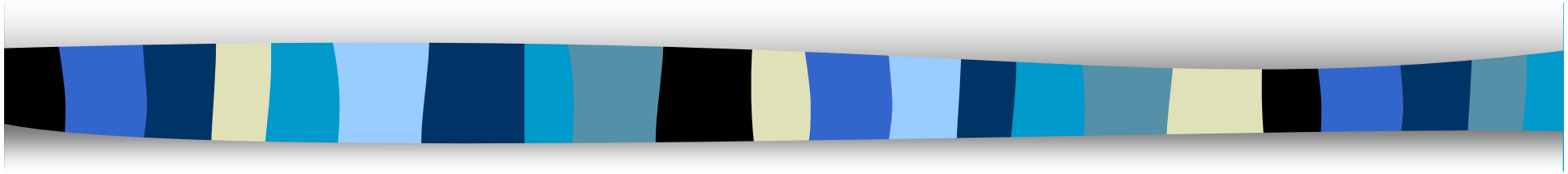
Complaints and audits at public hospitals



XIX CHW – Prague 12 –13 March 2009

Maria Michaelidou

Office of the Commissioner for Personal Data Protection

Cyprus

- Population: approx. 800,000
- 6 major hospitals (one per city)
- Several regional medical centers/ hospitals
- The largest: Nicosia General Hospital

The situation

- No electronic health system until 2008
- Before 2008 → most medical records were kept only in (manual) paper files (one for every patient)
- Processing by non-automatic means
- The personal data forms part of a filing system
- Nicosia General Hospital was relocated in 2006
- Several thousands of box files had to be moved and to be categorized → many problems – several complaints

Complaints and investigations

Case 1: Insufficient security measures at old Nicosia hospital

- After the relocation of Nicosia General Hospital in 2006 several medical files (incl. doctors reports, x-rays and encephalograms) were abandoned at the old psychiatric department without sufficient safeguards
- This incident was published in the media
- On spot investigation by our DPA
- The Ministry of Health alleged lack of synchronization with Public Works Department.
- Dec. 2007 → €2,600 fine was imposed to the controller for infringement of articles 10(1) and 10(3) for not taking the necessary confidentiality and security measures.

Complaints and investigations

Case 2: Loss of a patient's medical file

- Following the relocation of Nicosia general hospital, thousands of medical files needed to be removed and reorganized.
- A patient exercised the right of access to his medical data in Nov. 2006
- For 6 months his medical file could not be located
- Complaint submitted to our DPA
- Until June 2008 the patient's file was not found
- In July 2008 the Commissioner imposed to the data controller a fine of €2000 for not satisfying the data subject's right of access.

Complaints and investigations

Case 3: Insufficient security measures at Limassol's hospital

- A complaint was submitted in 2008 revealing that a patient or a visitor could easily have access to the laboratory results in Limassol hospital
- On spot investigation by our DPA
- Insufficient security measures
- No privacy policy to be followed by the staff
- Complete ignorance about the data protection act
- Result:: education and guidance

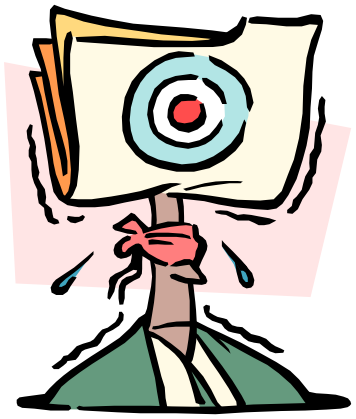
What does the law say

- Section 10(1) of Data Protection Act: The processing of data is confidential. It shall be carried out only by persons acting under the authority of the controller or the processor and only upon instructions from the controller.
- Section 10(3): The controller must take the appropriate organizational and technical measures for the security of data and their protection against accidental or unlawful destruction, accidental loss, alteration, unauthorised dissemination or access and any other form of unlawful processing.
- Section 17 of the Act on Patients Rights: specifications on the exact data that the health provider must keep for every patient in his filing system

Main issues

The DPS decides to inspect at least two hospitals regarding:

- Progress made on applying the New Electronic Health File System
- Security measures



Main issues

The inspections were focused on the following topics:

- ✓ Files management system
- ✓ Staff security policy
- ✓ Data protection Officials
- ✓ Periodic checks on measures taken
- ✓ Circulation of medical files inside the hospital
- ✓ Lawfulness of processing
  - Level of access
  - Excessive data

Comprehensive Health Information System (C.H.I.S.)

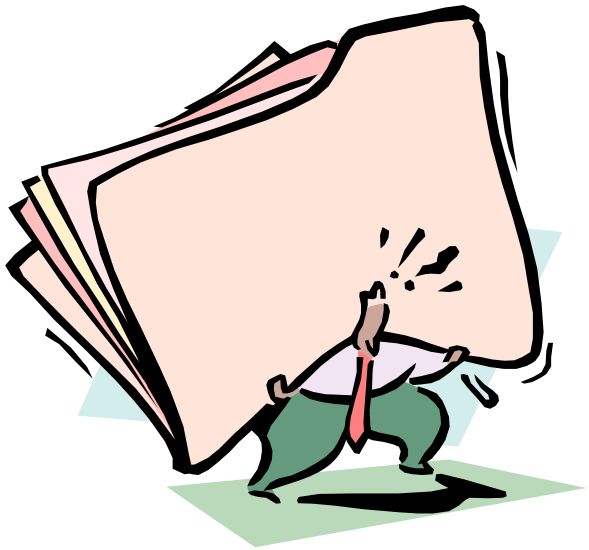
- The establishment of C.H.I.S. started in Jan. 2007 and was completed in Jan. 2009 in two hospitals
- It will allow (after its completion) an interconnection between all hospitals and medical centers via an electronic communication network (WAN)
- It provides 2 access levels to the system, depending on the user's functions and duties e.g. the administration desk officer → only demographic data
- Username and primary key → tracking on information entered into the system
- Log off after 15 minutes
- Help desk

Comprehensive Health Information System (C.H.I.S.)

Modules

- Patient's administration
- Publication of commands
- Chemical laboratories
- Pricing
- X-ray laboratories
- Patient's health record

What's next



- EU context: good practices to follow
- The DPA is currently issuing guidelines for hospitals on security measures to be taken and on the lawfulness of processing
- Audits in private hospitals in 2009 → questionnaire to all hospitals or inspection in 2 of them