

Security and Trust in virtual health care communities

Petra 2009 – 2nd International Conference on
Pervasive Technologies Related to Assistive
Environments
PSPA Workshop

Anargyros Chryssanthou, Greek Data Protection Authority, ICT Auditor
Dr. Charikleia Latsiou, Greek Data Protection Authority, Lawyer
Dr. Iraklis Varlamis, Harokopio University of Athens, Dept. of Informatics &
Telematics

Structure of presentation

1. Medical virtual communities (in general)
2. A virtual medical community for patient monitoring and Tele-Healthcare
3. A risk assessment point of view (ISO 27005:2008)
4. An initial risk assessment of the virtual medical community
5. Designing an ISMS for the virtual medical community
6. Justifying the ISMS – Usage Scenarios
7. Conclusions – Future work

1. Medical Virtual Communities (a general perspective)

- **Aim** : support members' collaboration in order
 - to virtually manage the illnesses
 - to improve the quality of a patients' life
- **Members**
 - patients
 - submit online requests for advice
 - share their problems and knowledge (gained from experience)
 - doctors
 - cooperate with each other
 - supervise and support their patients
- **Characteristic examples:**
 - supportive patient communities that promote peer to peer patient communication
 - virtual communities that monitor patients and provide tele-healthcare
 - medical research communities that support the collaboration of medical professionals

2. A virtual medical community for monitoring and Tele-Healthcare

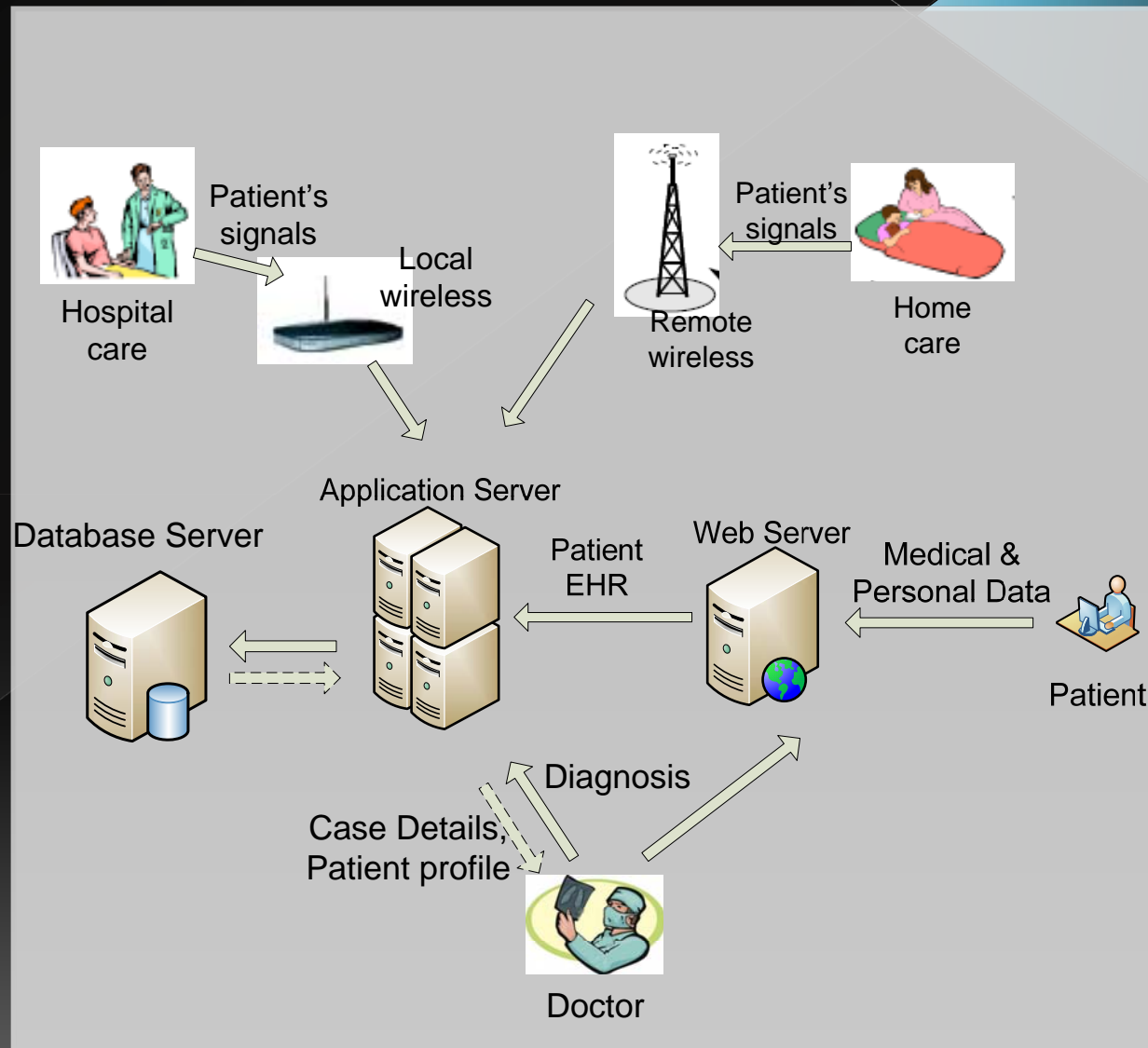
- ❑ A community where members use ICT
 - discuss their issues
 - share experiences
 - consult with experts
 - provide personal information and request for support
- ❑ A community that employs advanced & pervasive ICT technologies to provide ubiquitous services to its' members
- ❑ Active members of the community are:
 - Doctors
 - Patients
 - Third interested parties (for example patient's family members)

Community Roles

- Members of the community undertake different roles
 - patients and family members
 - facilitators
 - healthcare professionals
 - moderators for discussion and contents
 - facilitators and mentors for the community members
- Administration performed by IT experts who must be trustful community members
- Smooth operation guaranteed among other by
 - IT technical support staff
 - employees of telecommunication services provider
 - directors of the organization that hosts the community

Community structure and activities

- Health-status information is collected & transferred to the community server
- Patient members request for advice, diagnosis or treatment suggestion
- Doctor accesses patient's medical record & makes a diagnosis
- Doctor can consult also the patient directly based on patient's medical signals
- Hospital keeps records of patients' profiles & history, doctor's diagnoses, requests & advices exchanged through the portal



3. A risk assessment point of view (ISO 27005:2008)

Performing a **Risk Assessment** is the first step to protect any organization's information system.

According to ISO 27005:2008, it is divided in 2 stages:

- **Risk analysis** (clause 8.2 of ISO 27005:2008)
 - ***Risk identification*** (clause 8.2.1)
 - Identification of assets to the organization's information system (clause 8.2.1.2)
 - Identification of threats (clause 8.2.1.3), existing controls (clause 8.2.1.4), vulnerabilities (clause 8.2.1.5) and consequences (clause 8.2.1.6)
 - ***Risk estimation*** (clause 8.2.2)
 - Identify level of risk for each risk identified in the previous process
- **Risk evaluation** (clause 8.3)
 - Comprises evaluating the identified risks according to selected criteria



4. An initial risk assessment of the virtual medical community

Identifying assets to the medical community – The CIA Model

- ❑ **Assets** to the proposed virtual community
 - people (active members of the community)
 - data (medical data)
 - the internal structure of the virtual community (the community's information systems as well as its physical premises)
- ❑ **Assets** need to be protected
 - The traditional **CIA** model applies here
 - **CIA** : Confidentiality, Integrity, Availability
 - A DDOS attack may lead to loss of community's availability which could even cost human life in case of an emergency due to unavailability of medical data
- ❑ **Assets** need to be assessed in the context of potential **threats** (mainly technical)
- ❑ and **consequences** (ethical, legal)

Identifying threats

- ❑ **Data breach** (Stealing of data, loss of data)
 - internal users
 - accidental (loss of USB stick containing sensitive medical data)
 - intentional (copying sensitive data to USB stick for own purposes)
 - outside malicious users (hackers, crackers, script kiddies, phishers)
 - unauthorized access to data or systems by means of a hacking attack or a Trojan horse stealing data
 - phishing attacks
 - social engineering
- ❑ Loss of functionality due to attacks (for example DDOS attack)
 - causes unavailability
- ❑ All of the above have or potentially have **legal consequences** for the perpetrator and the virtual community

Ethical - Legal Issues

□ Ethical issues

- improper use of information by doctor (to conduct experiments)
- wrong medication or consultation by doctor
- patient that harasses other patients
- violate code of ethics – cause trust issues inside the community

□ Potential legal issues for the community

- improper use of patient's data
- use of medical data for other than notified purpose
- suffering a **data breach** incident
- subject to penalties imposed from **data protection laws**

The legal state of play

□ US Government Law

- **Opt-out** policy in general (citizen has to ask to be excluded from data collection)
- Levels of protection for medical data
 - total confidentiality for some (abortions, contraception, psychological disease)
 - delegate decision to state laws for other

□ EU Law

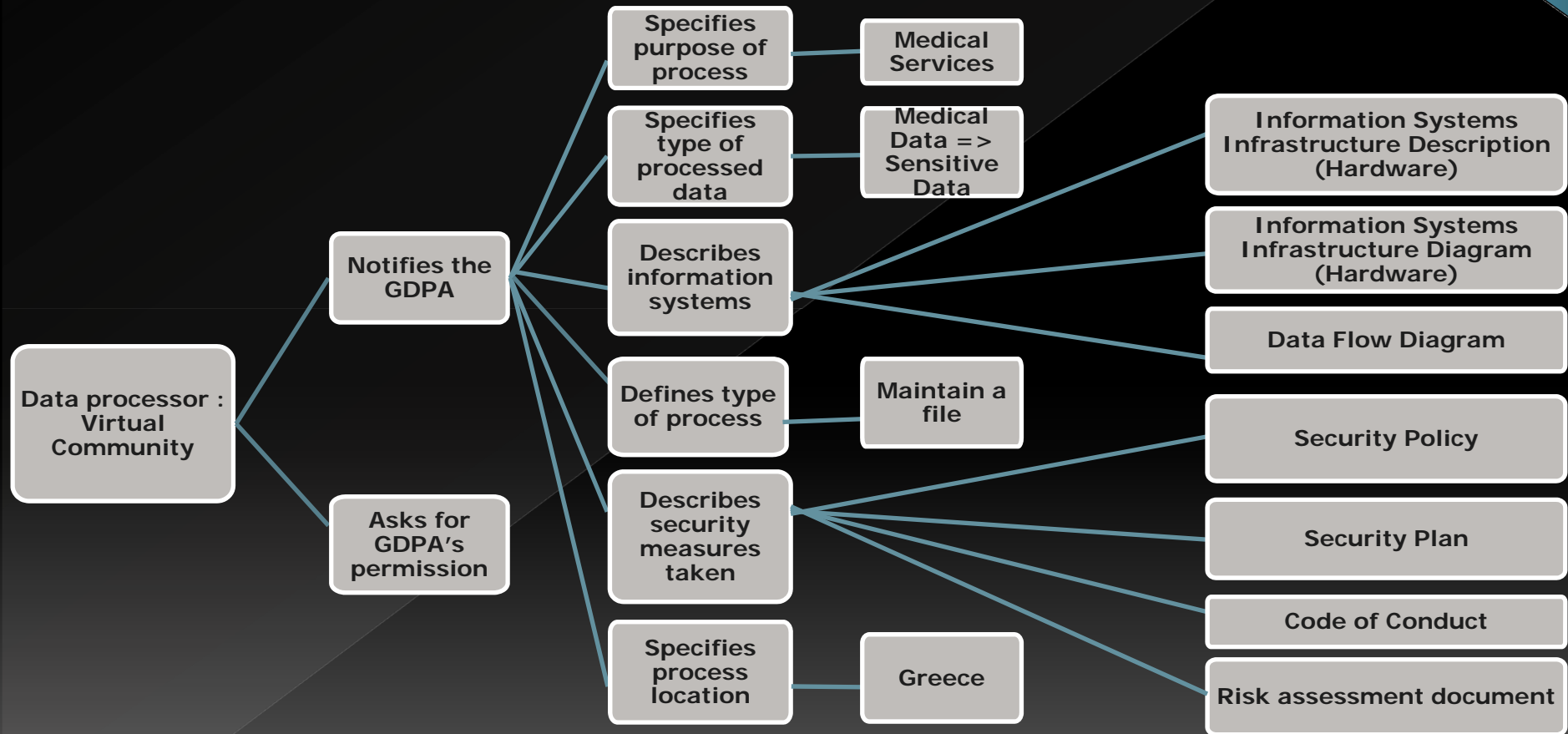
- **Opt-in** model for all personal data (citizen has to grant access)
- Only health professionals can access medical data and must protect confidentiality (Directive (95/46/EC))
- Data can be collected without consent to prevent a real danger or in a case of criminal offence (Recommendation (97) 5)
- Data can be collected and processed to preserve vital interests of the data subject or of a third person (if the law provides for this)

Greek Law 2472/1997 (Implementing the European directive))

- ❑ Medical data => **sensitive data** (article 2 paragraph b)
- ❑ Article 7 paragraph 5d allows processing of medical data by persons professionally providing health services after **permission** of the Greek Data Protection Authority (**GDPA**)
- ❑ **Data processor** needs to ask permission from the GDPA for processing medical data (article 6)
- ❑ **Data process** need to be **analog** to the **dedicated purpose** (article 4)
- ❑ **Data processor** needs to take appropriate **security measures** to protect privacy of sensitive data (article 10 paragraph 3)
- ❑ For each and every international transfer of medical data the GDPA needs to be notified and deem if transfer is allowed
- ❑ In case of illegal processing of medical data if the data processor resides in Greece he is subject to **penal, civil and administrative penalties** (articles 21-23)
- ❑ Law on medical confidentiality (law 3418/2005)

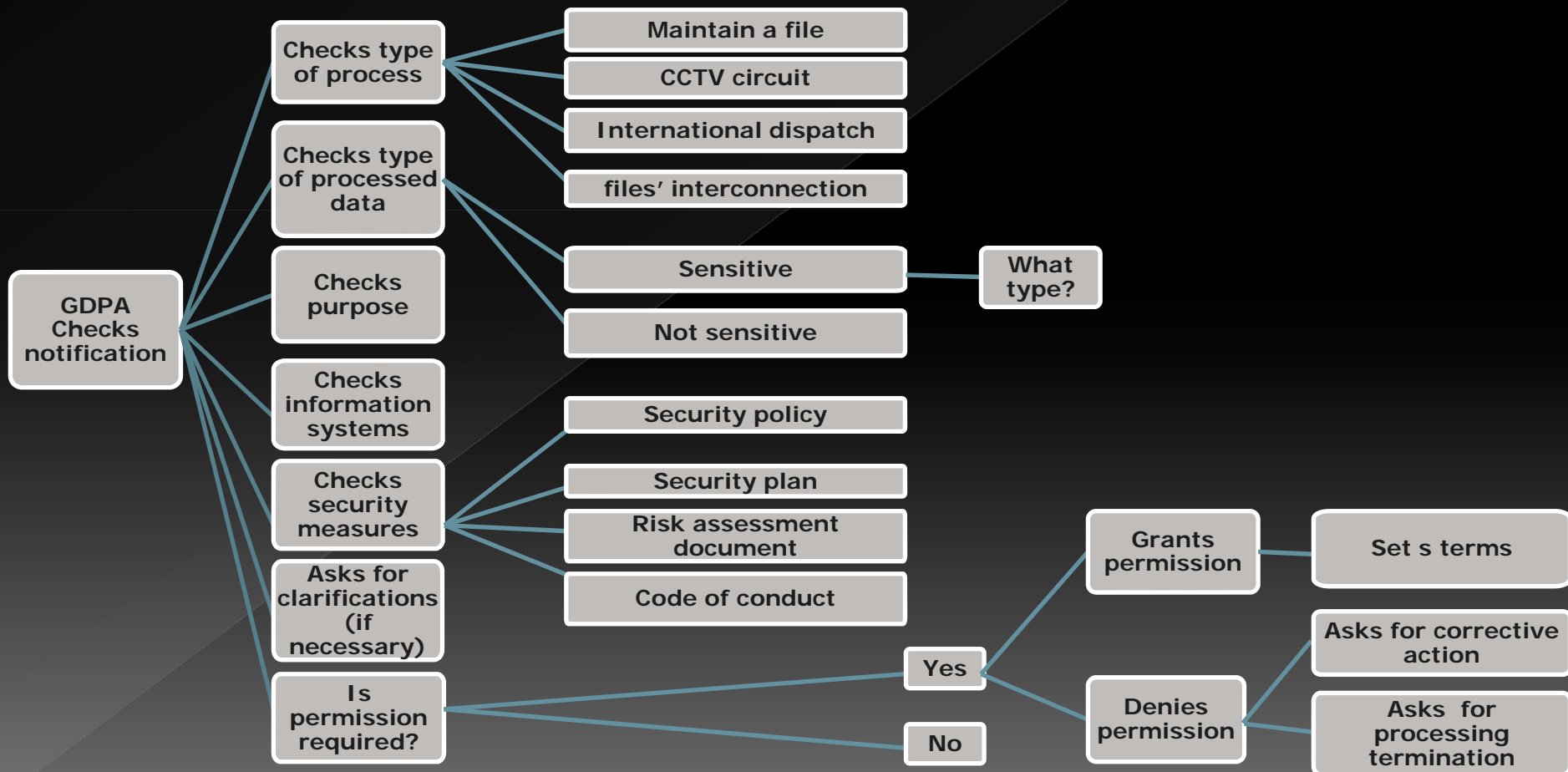
Applying Greek Law to the proposed virtual community

The Notification process



Applying Greek Law to the proposed virtual community

The GDPR Notification examination process (Granting / denying permission – setting terms)



Estimating – evaluating risks

- By estimating identified risks (clause 8.2.2 – ISO 27005:2008)
 - a DDOS attack and the permanent impairment of the systems would be rated as
 - **severe** (in regard to “**business**” impact) – LOSS OF AVAILABILITY
 - **low** (in regard to **likelihood of event**)
 - while an accidental loss of data contained on a USB stick would be rated as
 - **severe** (in regard to “**business**” impact) – LOSS OF CONFIDENTIALITY
 - **medium to severe** (in regard to **likelihood of event**)
- Evaluating the above 2 risks (clause 8.3 – ISO 27005:2008)
 - would set a **medium level of risk** to the first one (**loss of availability** => can lead to loss of life, but low likelihood)
 - and **high** to the second one (**loss of confidentiality** => can lead to identity theft, even to loss of life along with legal consequences)


Forming a risk treatment plan

- ❑ Last step of our risk assessment would be forming a **risk treatment plan** (clause 9 – ISO 27005:2008)
- ❑ Means identifying controls to be implemented to reduce, retain, avoid or transfer identified risks
- ❑ In our risk treatment plan several controls are chosen for the community's **ISMS** (Information Security Management System)
- ❑ Among others, following controls were selected in order to mitigate risk
 - Access control (A.11 – ISO 27001:2005)
 - Monitoring (A.10.10 - ISO 27001:2005)
 - Management of removable media (A.10.7.1 – ISO 27001:2005)
 - Input data validation (A.12.2.1 – ISO 27001:2005)
 - Business Continuity Management (A.14.1 – ISO 27001:2005)

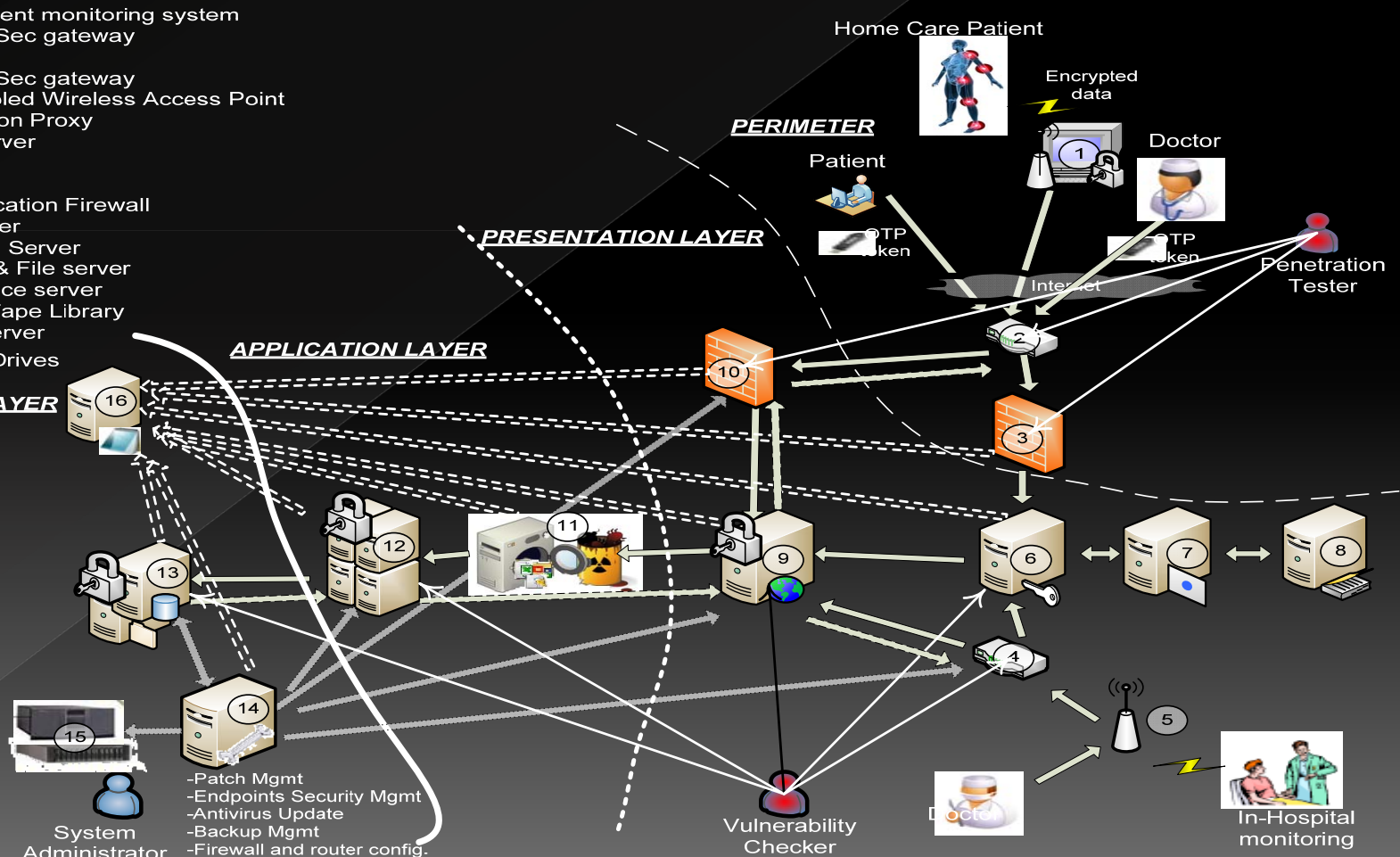
5. Designing an ISMS for the virtual medical community

Implementing the community's ISMS (ISO 27001:2005)

- Going into the implementation phase of the ISO 27001:2005 PDCA (Plan – Do – check – act) cycle
- Implement a 4 tiered security architecture

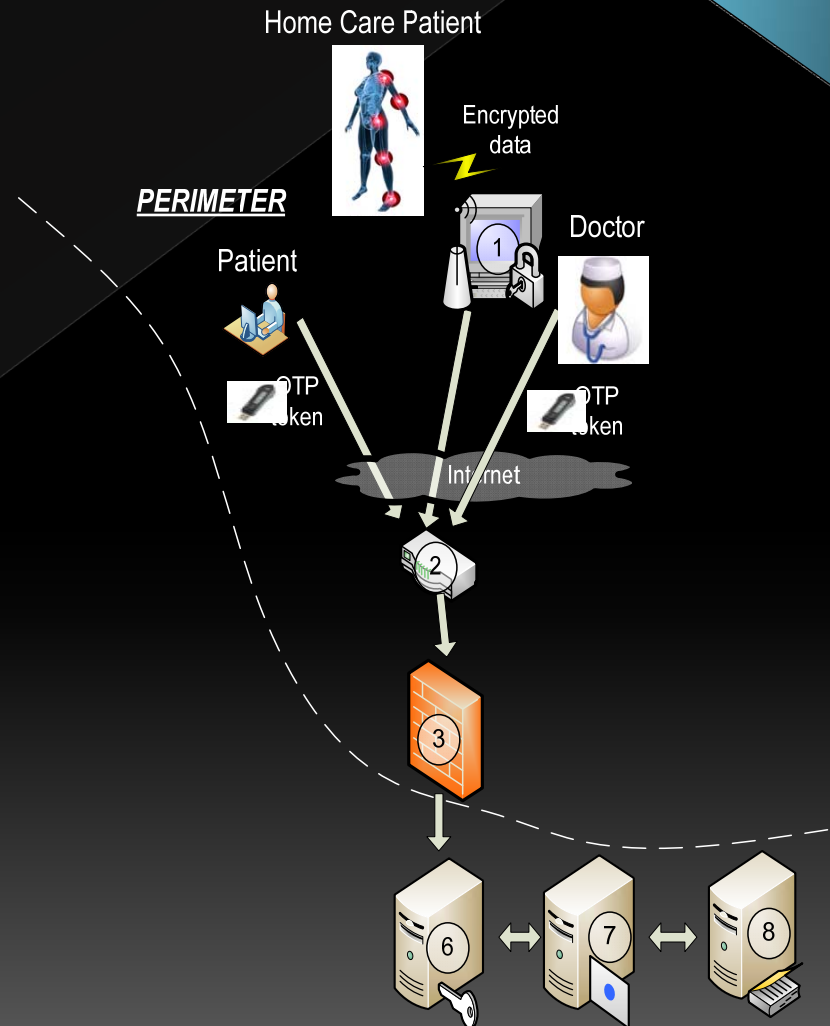
- 1: Remote patient monitoring system
- 2: Router & IPSec gateway
- 3: Firewall
- 4: Router & IPSec gateway
- 5: 802.1x enabled Wireless Access Point
- 6: Authentication Proxy
- 7: RADIUS server
- 8: LDAP
- 9: Web Server
- 10: Web Application Firewall
- 11: Content filter
- 12: Application Server
- 13: Database & File server
- 14: Maintenance server
- 15: SAN and Tape Library
- 16: Auditing server
-  Encrypted Drives

INTERNAL LAYER

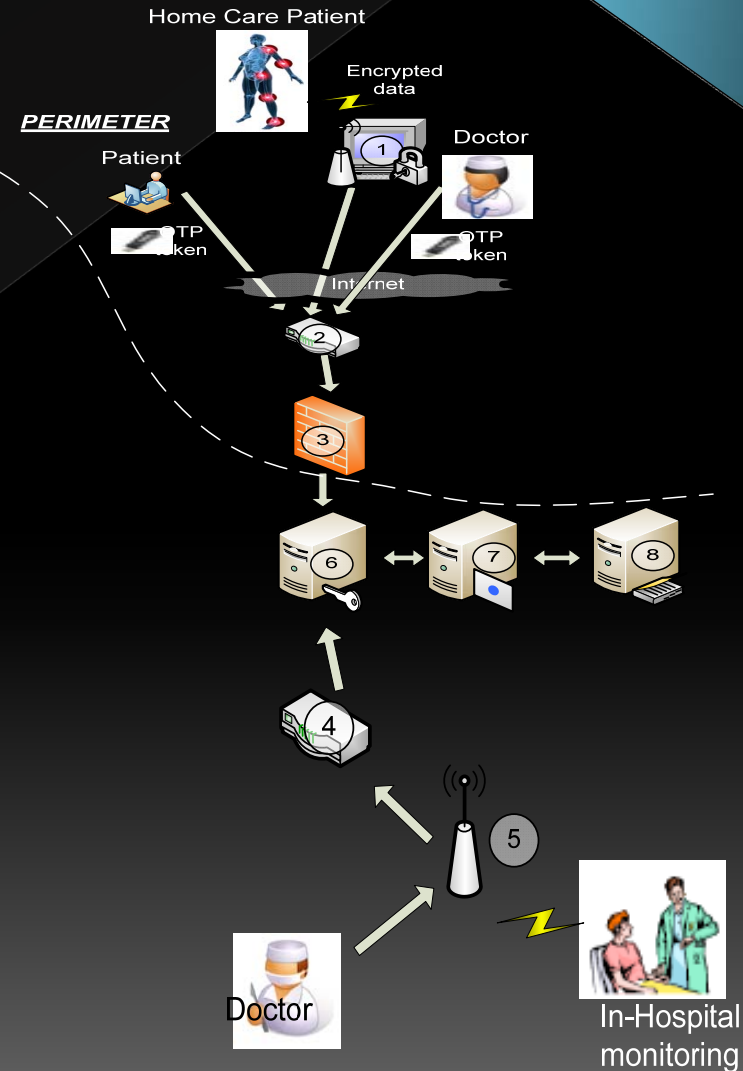


Layer 1 : The Perimeter

- ❑ In the past : protect everything behind a firewall
- ❑ Our proposed model for the community : **protect everything in its layer**
- ❑ starting from the community perimeter layer
- ❑ User uses e-token device
- ❑ to connect through the authentication proxy to the community's RADIUS server
- ❑ RADIUS server integrates with local directory (location of identity store)
- ❑ Authentication proxy comprises the enterprise validation engine
- ❑ E-token device => single sign on (user id kept on identity store, combined with OTP from e-token device => user authentication)

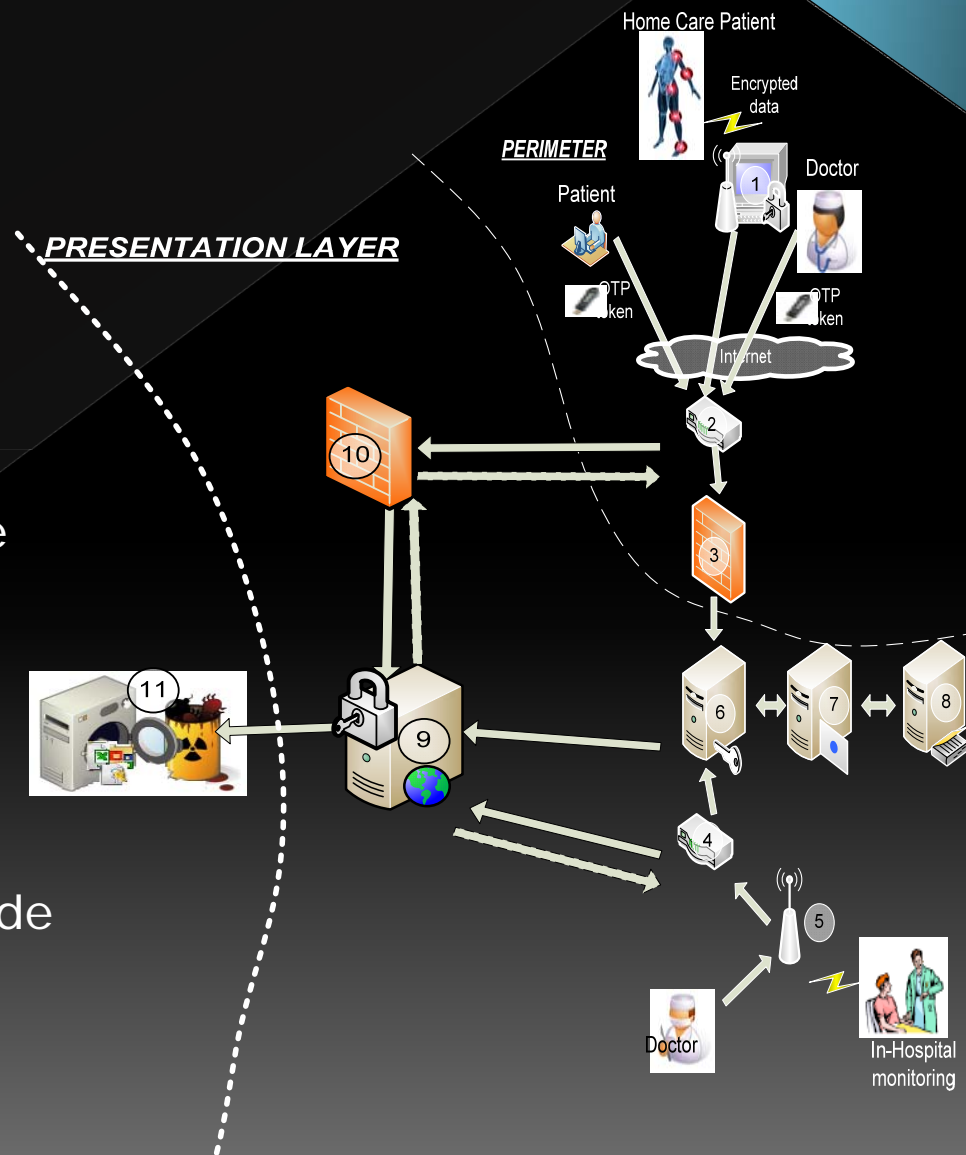


- ❑ Home-care patients
- ❑ have wireless sensors attached to their body
- ❑ to communicate with community's application server
- ❑ Encrypted signals connected to the base of the remote monitoring system
- ❑ forwarded through secure router to application server
- ❑ Doctors inside the hospital
- ❑ and patients treated inside the hospital
- ❑ use an 802.1x enabled wireless access point
- ❑ to connect through the authentication proxy to the community's Radius server (authentication server)
- ❑ Authentication server sets up an EAP-TLS session with the client using digital certificates
- ❑ for mutual authentication



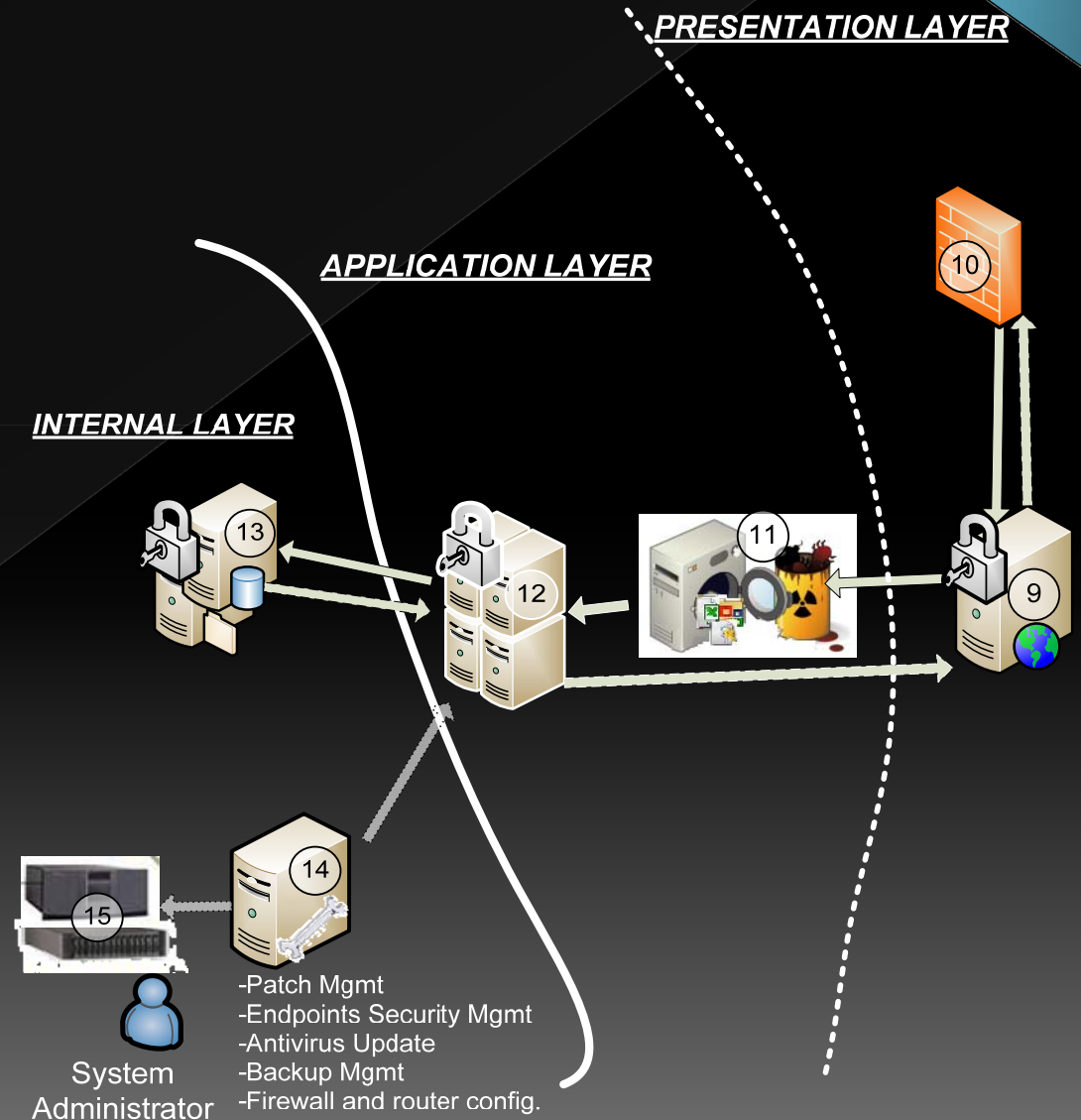
Layer 2 : Presentation Layer

- Filtering module
 - “washes-out” malicious user input
 - blocks several web attacks
 - by processing and validating user input
- Web application firewall employed
 - to distinguish legitimate traffic
 - and potential attacks such as sql injection
 - using known-attack signatures
 - and administrator – made signatures
 - records requests to database server



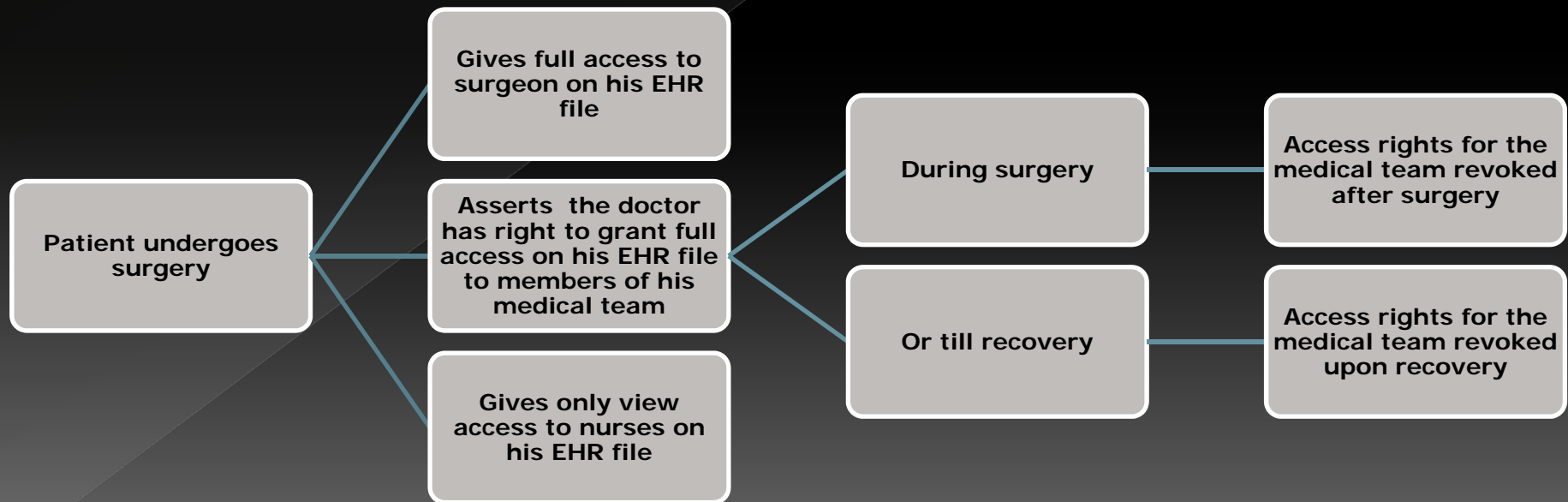
Layer 3 : Application Layer

- ❑ Access allowed only to authenticated members – third party applications and devices
- ❑ Goal of the application server is to verify user's **authorization** to access data
- ❑ Access policies, community roles, clarification of access rights are required in this layer
- ❑ Configuration of the application server done by administrator in maintenance server
- ❑ Access credentials and initial roles distributed by community's authorities
- ❑ Patients have to define later access to their own medical data or their private conversations



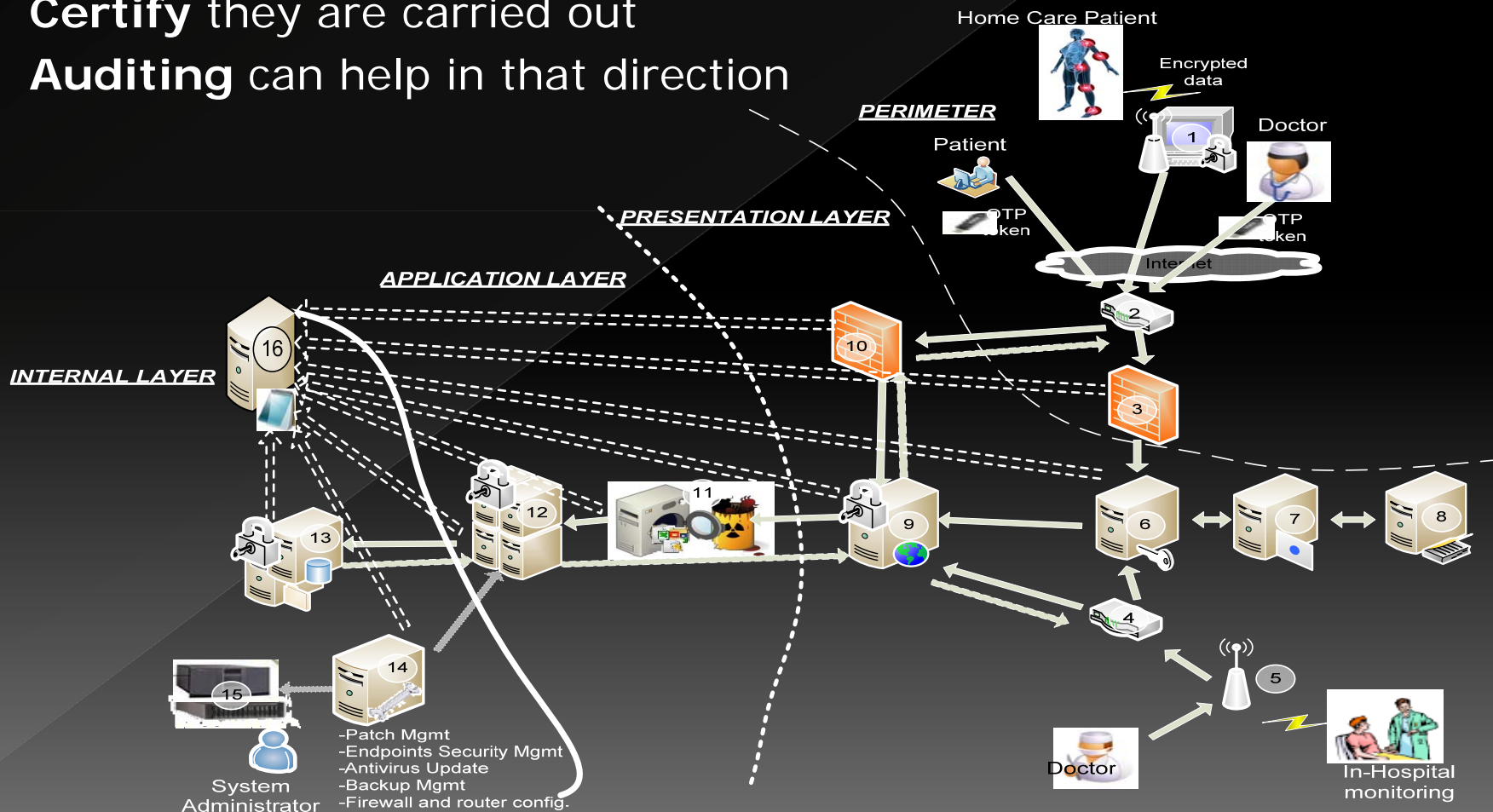
Layer 3 : Authorization process

- ❑ Flexible access model adopted
- ❑ A **semantics policy** such as SECPAL with its PKI-based SOAP encoded infrastructure for exchanging policy assertions
- ❑ ideal for access policy management
- ❑ supplemented by an overall access and behavioral policy for active members of the community
- ❑ that describes security procedures (such as login, user roles, etc) and behavioral rules



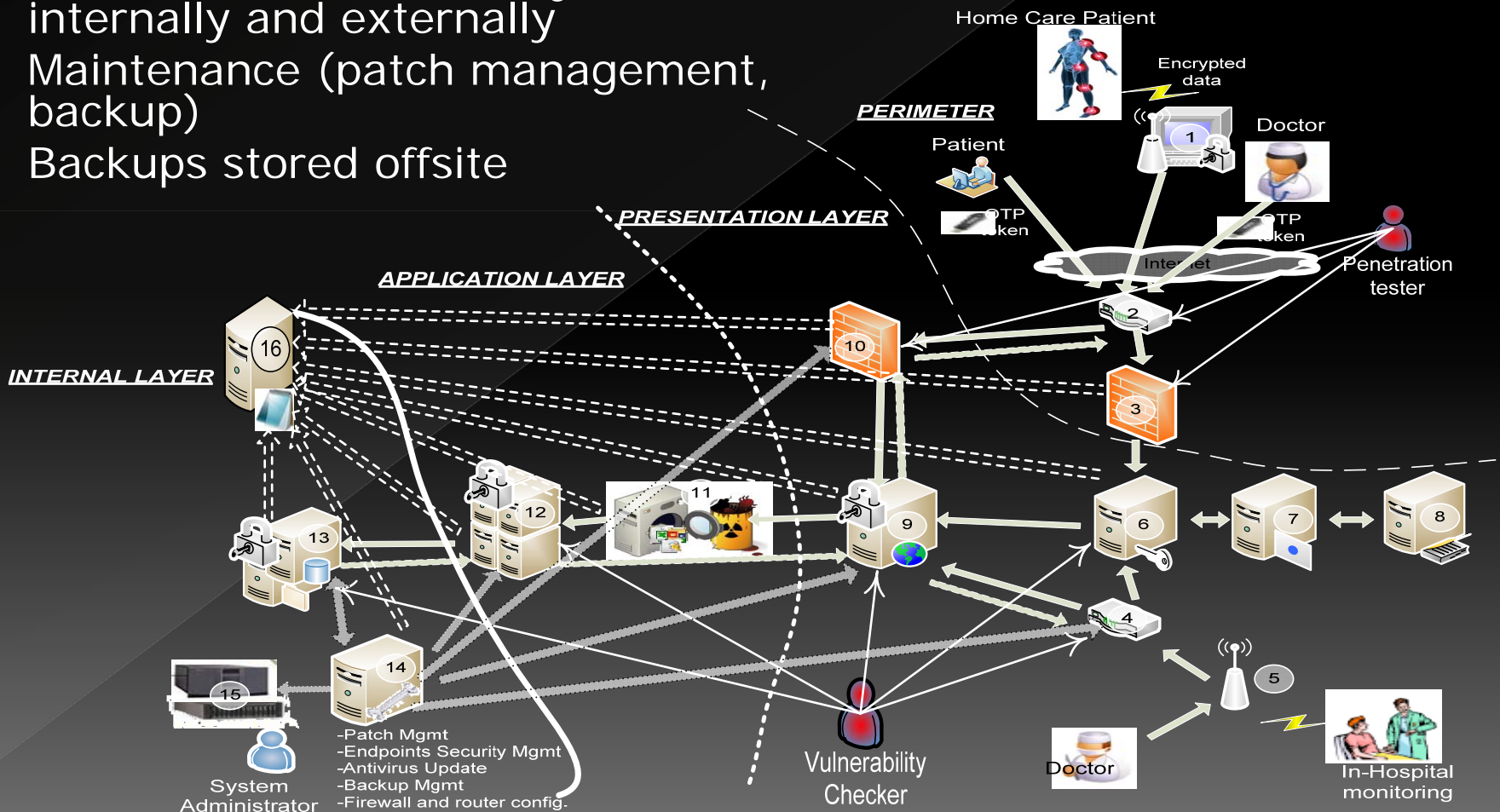
Layer 4 : Internal Layer – Auditing

- ❑ Securing the community is not enough
- ❑ **Trust** among members need to be achieved
- ❑ Define responsibilities
- ❑ **Certify** they are carried out
- ❑ **Auditing** can help in that direction



Layer 4 : Maintaining security

- ❑ All servers must have **encrypted** hard drives read in presence of hardware tokens
- ❑ **Endpoint security** in place
- ❑ **Disaster recovery plan**
- ❑ Periodic check of security level internally and externally
- ❑ Maintenance (patch management, backup)
- ❑ Backups stored offsite

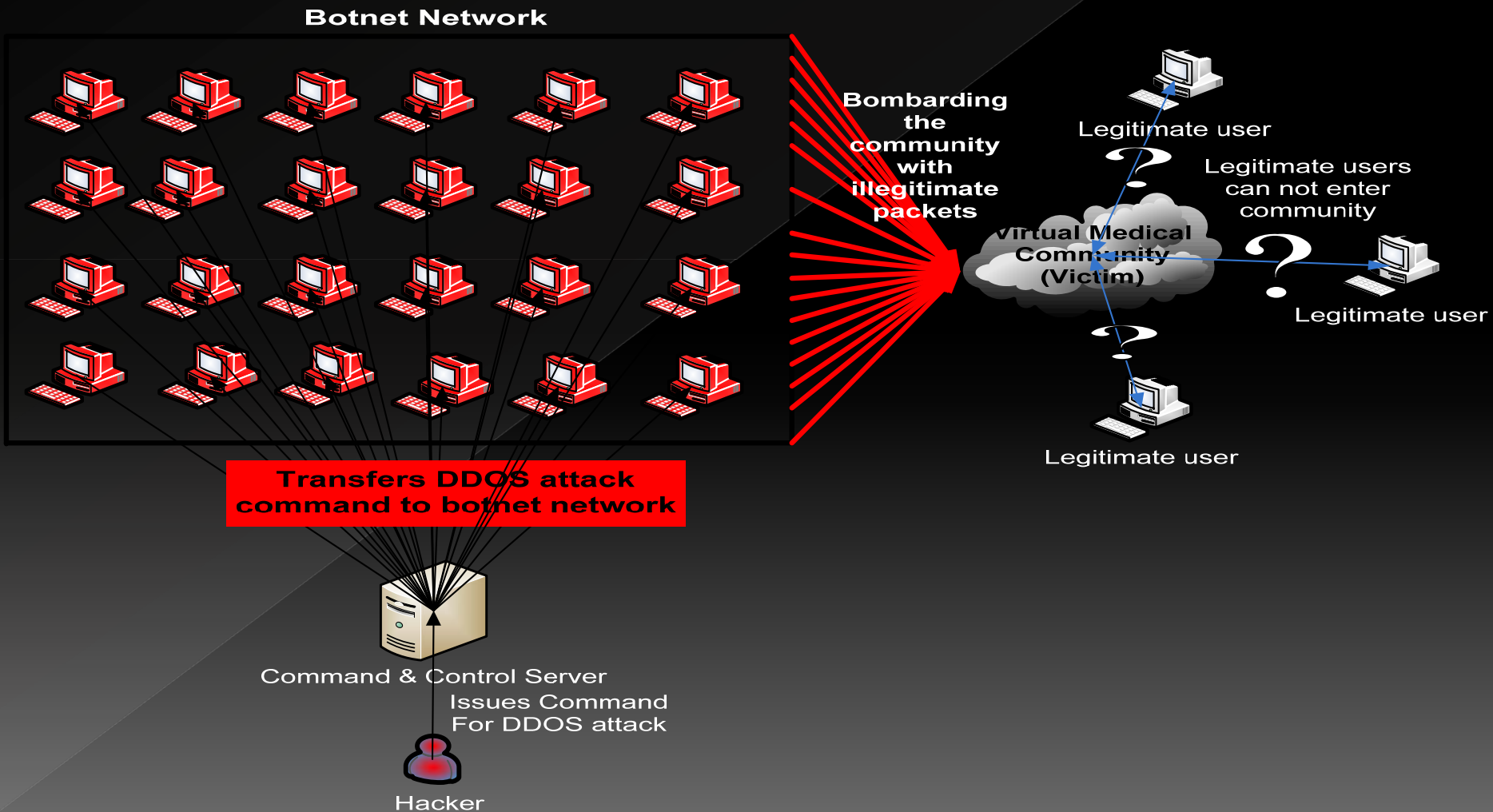




6. Justifying the ISMS – Usage Scenarios

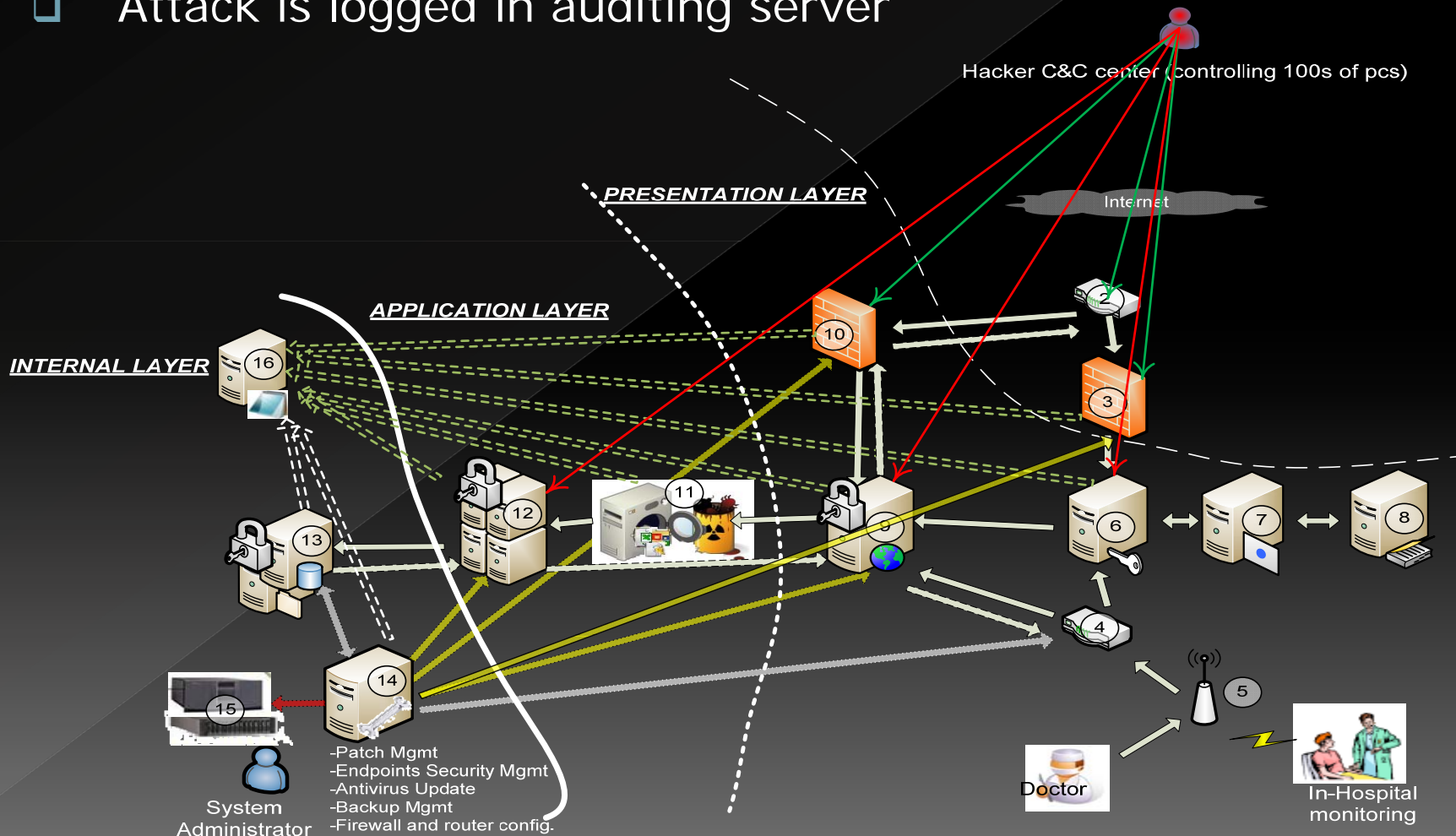
The DDOS Risk : An external attack scenario

- ❑ During risk assessment various risks were identified
- ❑ Based on those risks, their business impact and their likelihood of occurrence
- ❑ the previously presented security controls were selected
- ❑ One single exploitable vulnerability can lead the attack to success



Activating the community's defenses

- ❑ Controls applied are our firewalls and their configuration
- ❑ the applied patch management suite
- ❑ and the disaster recovery plan (in case of a zero day exploit)
- ❑ Attack is logged in auditing server



7. Conclusions – Future work

- A second glance, we presented
 - A desired infrastructure for a virtual medical community
 - through a detailed risk assessment
 - by applying security controls selected in a risk treatment plan
 - The law governing medical data
 - The structure and functionality of such a community
 - We justified through an attack scenario some of the controls
- Future plans
 - Test the selected security infrastructure against various security risk scenarios
 - Test the model over a real medical community
 - by allocating resources (time, funding and field of appliance)

**Thank you very much for your
attention**