momentum
ADVANCING TELEMEDICINE ADOPTION IN EUROPE

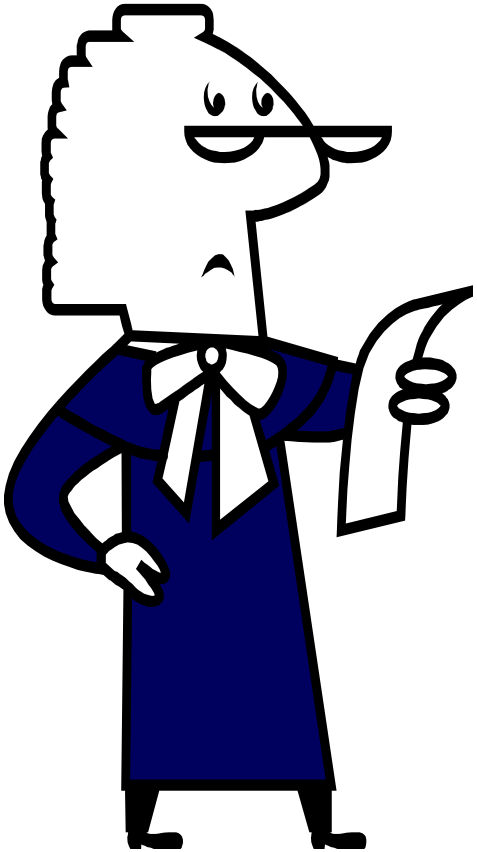
MOMENTUM
Critical Success Factors
Legal and security issues

eHealth Forum Athens
14 May 2014
Ellen K. Christiansen

Critical Success Factors for Legal and Security

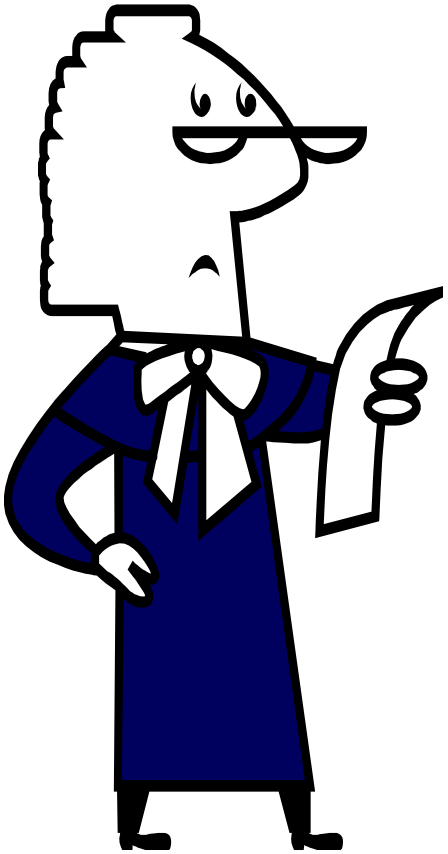
- Ensure that the telemedicine service is legal
- Involve legal, ethical, privacy and security experts from idea to routine service
- Identify and apply relevant ethical, legal and security guidelines
- Raise privacy awareness among telemedicine doers and users

Ensure that the telemedicine service is legal



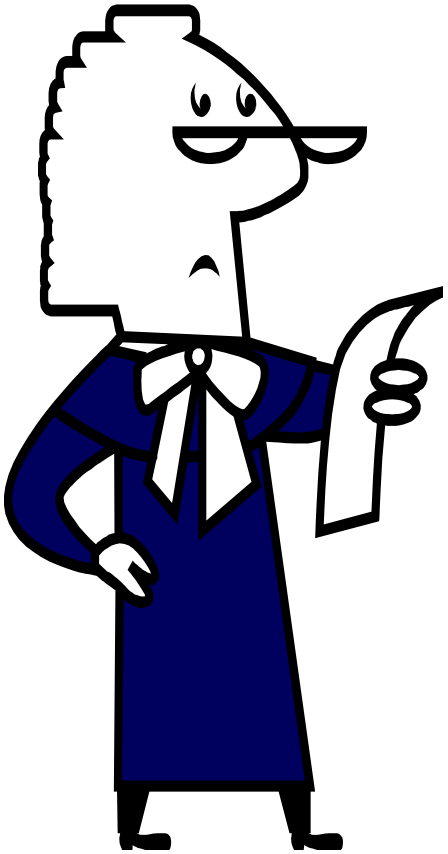
- Make sure that the telemedicine service at stake is not inhibited by law.
- Make sure that the telemedicine service at stake is not considered to be in conflict with the requirements for best practice in medicine.
- Adapt the telemedicine service in progress to the legislation and regulations in force.

Legality - Relevance for the four cases



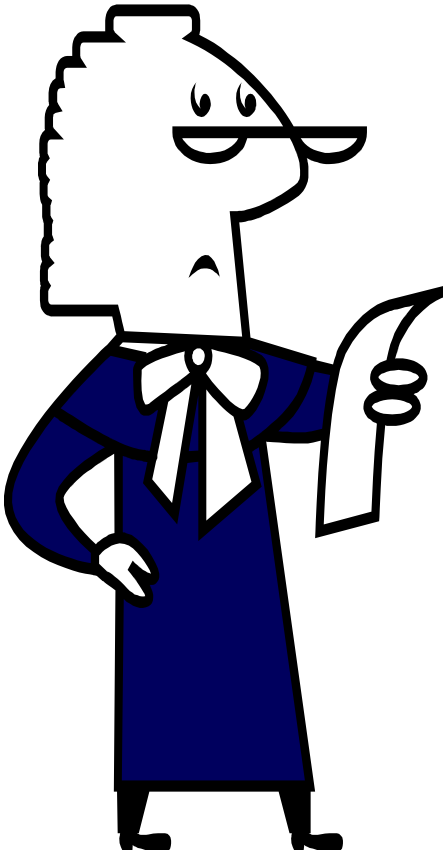
- **Maccabi Chronic Disease Telemedicine Center** – Not really a critical success factor. The “legality” of telemedicine has never been questioned.
- **RxEye, Sweden –** Legal framework is not a critical factor for RxEye. It functions within the current legal framework of teleradiology services. Contracts are the main enablers to provide the medical image reporting brokering service.

Legality - Relevance for the four cases



- **Teledialysis, Norway** – Liability and responsibility issues were sorted out. Measures to secure the quality and the reliability of the service were discussed and implemented. Routines for documentation of the service were adapted to the legislation in force.
- **ITHACA, Spain –** Telemedicine is *not* perceived as second-class medicine. As a complement to traditional care it poses little threat.

Legality - Summing up



For our four cases

- It has been ensured that the services are legal from the outset.
- No invincible hindrances were identified.

Involve legal, ethical, privacy and security experts from idea to routine service

Legal, ethical, privacy and security experts have knowledge of regulations relevant to telemedicine at all levels, internationally, nationally and locally. Their primary task is to assist the telemedicine doers when needed.

- Legal and security experts should be part of a multi-professional team, a coaching body, assisting the “doers”.
- The objective for experts in the legal and security sector is to adapt the telemedicine service to legislation and regulations in force, through the whole development and implementation process – from initial ideas through to routine service

Experts – Relevance for the four cases

- **Maccabi Chronic Disease Telemedicine Center –** Security and legal expertise already exist for the central EMR which is transparent to medical personnel and the patient. Ethical, privacy and security issues had already been dealt with in earlier telemedicine services.
- **RxEye, Sweden** – RxEye service represents a new and different teleradiology service. Thus, consultancy and/or presence of lawyer has been necessary.

Experts – Relevance for the four cases

- **Teledialysis, Norway** – Risk assessment was conducted initially to comply with legal requirements. That will be repeated regularly. New legal and security issues may arise at any time during the service's life span, and must be taken care of as they emerge. Medical staff has to know who they can ask.
- **ITHACA, Spain** – The service is in compliance with strict Data Protection Act (1995)

Experts – summing up

For our four cases

- All four services had experts involved at one stage of the process.
- One has stated that this was a new way to organise this kind of service.

Identify and apply relevant ethical, legal and security guidelines

There are guidelines for specific countries and for professional groups – such as doctors – that codify legislative and security measures as well as ethical and policy considerations.

- Guidelines must have been issued by trusted bodies to be relevant.
- Guidelines must be known and considered important and useful.
- The objective is to establish services in accordance with basic and accepted principles in the legal and security fields.

Guidelines - Relevance for the four cases

- **Maccabi Chronic Disease Telemedicine Center –** Operational guidelines already exist for the central EMR which is transparent to medical personnel and the patient.
- **RxEye, Sweden –** Both European and North-American Societies of Radiology have issued white paper where the principles of good practice of teleradiology are addressed. It is beneficial for the RxEye service to follow the principles of white paper.

Guidelines - Relevance for the four cases

- **Teledialysis, Norway –** Guidelines for telemedicine and responsibility/liability are issued by the government and always taken into account. In addition, «Code of Conduct for information security in the health care sector» is worked out by the health sector and is legally binding.
- **ITHACA, Spain –** The service is based on international clinical guidelines.

Guidelines – Summing up

For our four cases

- All four services have taken some sort of guidelines into account.

Raise privacy awareness among telemedicine doers and users

“Privacy awareness” is knowledge about appropriate practice when it comes to privacy and security behaviour. It is based on current ethical and legal principles.

- Awareness is achieved through education and training, introducing norms and basic principles based on existing guidelines.
- The objective is to prepare for secure telemedicine service and responsible conduct.
- Human errors, and sometimes “shortcuts” play an important role when health information goes astray. (IT systems are not always user-friendly.)

Privacy awareness – relevance for the four cases

- **Maccabi Chronic Disease Telemedicine Center –** Explicit patient consent for access to the EMR for involved personnel, is a condition of subscribing to the service, which is voluntary. Everyone accepted that access to the EMR for the staff at the centre was essential for the service.
- **RxEye, Sweden –** RxEye service de-identifies referral letters and images. Awareness of privacy is important because the patient should know where and by whom his/her medical data (incl. images) are viewed. Often the healthcare institution which uses teleradiologist from outside the organisation for reporting acquires informed consent from the patient.

Privacy awareness – relevance for the four cases

- **Teledialysis, Norway** – Duty of professional secrecy is important for the healthcare staff. If patient information goes astray due to insufficient technical security measures and/or unsatisfactory routines for handling of patient information, it might be considered as a breach of duty of professional secrecy. Brief guidelines for secure conduct were worked out for both parties in the video conferencing.
- **ITHACA, Spain –** Terms of service agreement signed. Less awareness in the patient side.

Privacy awareness – summing up

For our four cases

- All four have taken this into account, but in different ways:
  - Privacy awareness among patients is achieved by means of informed consent.
  - Privacy awareness among health professionals is related to the duty of professional secrecy.

Thank you!

ellen.christiansen@telemed.no