UKCGC

The United Kingdom Caldicott Guardian Council

Making sure data from wearable medical devices is used properly and people's confidentiality is protected:

the Caldicott Guardian's perspective

UKCGC
The United Kingdom Caldicott Guardian Council

Introduction

- Tim Kendall
- United Kingdom Caldicott Guardian Council (UKCGC)
- The role of the Caldicott Guardian

  "A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly."
- Health **and social care** (scope of devices: health, care, wellbeing/prevention)
- Seven principles
- Principle 7:

  The duty to share information can be as important as the duty to protect patient confidentiality.

UKCGC
The United Kingdom Caldicott Guardian Council

Question

- How many people here use wearable devices?

- Are you confident you know everywhere the data collected by your device is stored?

UKCGC
The United Kingdom Caldicott Guardian Council

Considerations and Context

- Patient (person, data subject) should not be surprised by use of their data.
- Data security:
  - Patches applied; anti-malware software
  - “Privacy by design” – data protection and privacy in mind at every step
  - Cyber Essentials
  - Data Security and Protection Toolkit
- Example of processing ‘likely to result in high risk’: wearable technology requires a Data Protection Impact Assessment according to Information Commissioner’s Office.
- Devices being “fit for purpose” – clinical safety (MHRA, CE mark)

UKCGC
The United Kingdom Caldicott Guardian Council

Lawfulness of Processing

- Lawfulness of processing – GDPR alternatives to consent
  - Art. 6 1(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
  - Art. 6 1(c) processing is necessary for compliance with a legal obligation to which the controller is subject
- Special categories of personal data
  - Art. 9 2(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services…
- Distinction between direct care and processing for secondary, indirect, purposes

UKCGC
The United Kingdom Caldicott Guardian Council

Examples / Case Studies

- Apple: Health app; watch
- Friend wearing heart monitoring device
- Royal Free NHS Foundation Trust / Google DeepMind
- Strava and Polar fitness cases

UKCGC
The United Kingdom Caldicott Guardian Council

Other data protection considerations

- The GDPR / Data Protection Act 2018
  - Data Controller / Data Processor
  - Right to erasure (‘right to be forgotten’)
  - Right to data portability
  - Retention…
  - Data Protection Officer
- The Common Law Duty of Confidentiality
- National data opt-out programme – applicable to other organisations than NHS Digital March 2020: purposes beyond individual care

UKCGC
The United Kingdom Caldicott Guardian Council

References

- UKCGC: www.ukcgc.uk, includes “A manual for Caldicott Guardians”
- The GDPR: gdpr-info.eu
- Data Security and Protection Toolkit: www.dsptoolkit.nhs.uk
- Information Governance Alliance GDPR guidance

UKCGC
The United Kingdom Caldicott Guardian Council

Conclusion

- Awareness of the responsibility of each member of staff:

  "Leadership Obligation 1: People: Ensure staff are equipped to handle information respectfully and safely..."

- Transparency: the data subject needs to know where their data goes, enabling sharing

- Legal, secure and safe

Thanks very much to the Health Archives and Records for inviting me to represent the UKCGC. I'm looking forward to learning more out more about wearable medical devices and related processes.