MEDINFO23

8 – 12 JULY 2023 | SYDNEY, AUSTRALIA

Securing Health Information: What health leaders need to know?

Dr Sheree Lloyd[1], Dr Joel Scanlan[1], Ms Louise Hayes[2]

Australian Institute of Health Service Management, University of Tasmania

Townsville Hospital and Health Service

LinkedIn

https://www.linkedin.com/in/sheree-lloyd

https://www.linkedin.com/in/joel-scanlan

https://www.linkedin.com/in/louise-hayesau

@TheInstituteDH #MEDINFO23

AIDH IMIA

Introduce yourself to your colleagues

We will discuss items in groups at our tables during this workshop, so introducing yourself in advance will save time later

Discuss what you are hoping to get out of the workshop

Acknowledgment of Country

I would like to acknowledge the Gadigal of the Eora Nation, the traditional custodians of this land and pay my respects to the Elders both past and present.

I extend that respect to Aboriginal and Torres Strait Islander peoples here today.

Introduction

- Welcome
- Introduction to speakers and facilitators
- Aims and overview of the workshop
  - Chatham House Rules
- Format of the workshop

About you

- Quick 30-second survey
  - Consent for data to be collected at workshop
  - Basic demographics
    1. What is your current job title/role?
    2. How many years have you been working in digital health?
    3. In what country do you work?

Ethics HREC code: H0029035

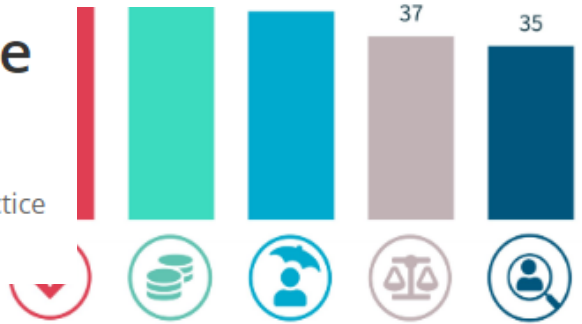
Woman dies during a ransomware attack on a German hospital / It could be the first death directly linked to a cybersecurity attack

By Nicole Wetsman
Sep 18, 2020, 5:11 AM GMT+10 | 0 Comments / 0 New

Lawsuit: Hospital's Ransomware Attack Led to Baby's Death

Suit Alleges Inability to Access Critical Fetal Monitoring Data Was Malpractice

Marianne Kolbasuk McGee (HealthInfoSec) · October 1, 2021



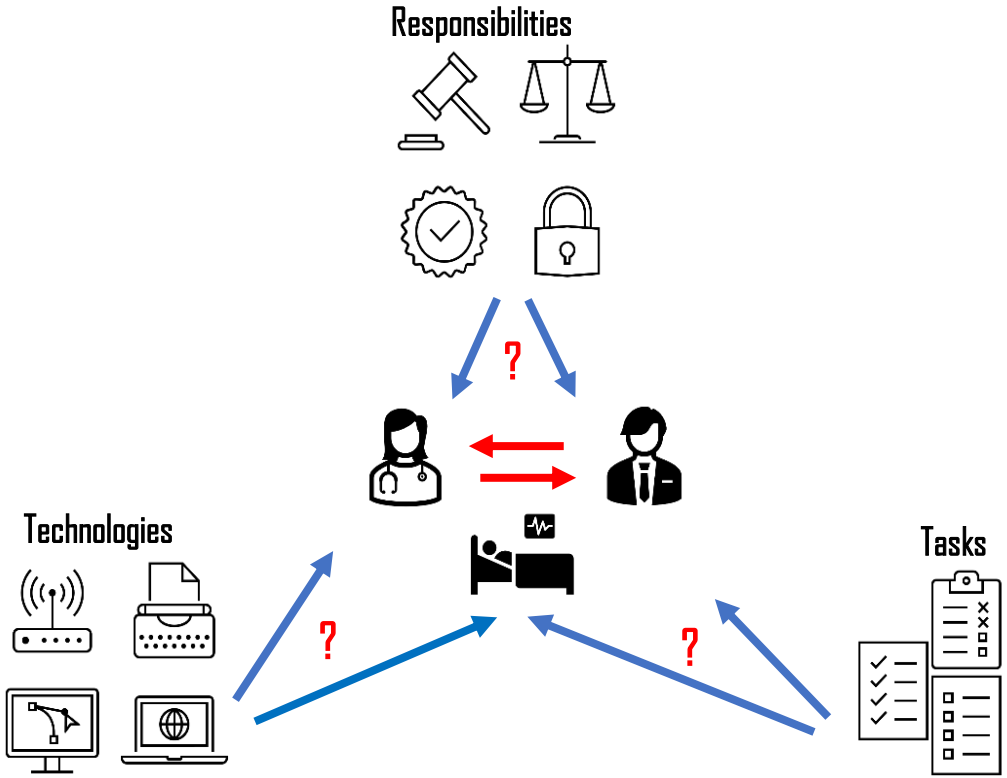
ıstitute,

ng

What is Information Security?

- Attempt a definition
  - Confidentiality
  - Integrity
  - Availability
- Sometimes we want another 'A'
  - Authentication
- These are the goals that all Computer Security problems can be distilled down to

Complexity



What does a bad day look like?

- What systems or data are affected?
  - How does this impact care provision?
- Who is the cause?
  - Malicious outsiders
  - Malicious insiders
  - Accidental or environmental

Activity

- We will now in small groups discuss, and record, our perspectives in relation to the following question:

Where can things break in digital health that harm care provision?

View from the ground

- Let's assume you have the following Information Security aspects in place:
  - Policy and governance
  - Risk assessments and threat assessments
  - Education and training in cyber security for staff

- How do you protect the clinical care settings from cyber security incidents?

How do you protect a clinical care setting from cyber security incidents?

- None of these will help

How do you protect clinical care setting from cyber security incidents?

- Patients will still be sick and require care
- Clinical care will continue

View from the ground

- Understand the impact of the incident
  - e.g. technical, clinical, privacy / confidentiality
- Business continuity planning / emergency preparedness planning
- Downtime procedures
- Recovery management
  - Clinical teams to support paper to digital (reconciliation)
  - Stand down emergency
- Support for clinicians and other staff, patients and consumers.

Activity

- We will now in small groups discuss, and record, our perspectives in relation to the following question:

What are the steps we should be taking **right now** to protect health service delivery and sensitive digital assets and personal information?

Assumptions for Information Governance

- Information Governance (IG) protects the consumer, patient, citizens, funders and providers of healthcare services
- Data is ubiquitous
- Collect data once and well
- For the right purpose, in the right format in the right place and time
- Information is an asset - risk to be managed like others

Information governance (IG) is designed to

1. Support, protect information, data and technology assets and enable the benefits of digital health
2. Implement mechanisms that set the principles, policies and procedures
3. Optimise how cyber security functions are arranged and embedded into the workings of the organisation

Functions of information governance

- Information design and collection
- Records and content management
- Access
- Quality and integrity of information
- Requires a multi-stakeholder approach supported by leaders and anchored in a formal framework (International Federation of Health Information Management Associations)

Cybersecurity governance principles

- Set clear roles and responsibilities
  - Board to ward
  - Third-party suppliers and vendors
- Promote a culture of cyber resilience
  - Cyber security mindset from the top down
  - Skills and training

  (AICD Cyber Security Governance Principles)

Source : AICD https://www.aicd.com.au/news-media/company-director-magazine/all-editions/november-2022-edition.html

Cybersecurity governance principles

- Develop, implement & evolve a comprehensive cyber strategy into information governance and embed it in existing risk management practices
  - Identification of key digital assets and data
  - Assessing and enhancing organisational capability
  - Inclusion of cyber risk in risk management frameworks
- Plan for a significant cyber security incident
  - Cyber incident control plan
  - Communication strategy
  - Simulation and testing

  (AICD Cyber Security Governance Principles)

Source : AICD https://www.aicd.com.au/news-media/company-director-magazine/all-editions/november-2022-edition.html

Australian Institute of Company Directors
STRENGTHENING SOCIETY THROUGH WORLD-CLASS GOVERNANCE

Red flags

The bottom line

- Leadership for information governance
- Adoption of cybersecurity governance principles
  - Cyber security is part of culture and we play a role
- Watch/review for red flags
- Not 'set and forget' as constantly evolving risk landscape

Activity

What are the priority areas for securing information assets for the next 12 - 18 months?

- Easy wins - short term < 12 months
- Big strides - > 12 months < 18 months
- Impact - > 18 months

Reporting Back

- What our priority areas are?
  - Next 12 months?
  - Key areas that will take longer than 12 months?
  - Other interesting outcomes to share?

Way forward

- Change
  - The actions we just spoke about – we need to do them!
- Awareness
  - Cyber literacy
  - Personal role in protecting those in our care
- Action
  - Awareness without action is futile..
  - Support from leaders, managers, providers and government

Key take-home messages

- Lead and embed information governance
- Embed cyber into culture and risk management for resilience
- Plan, simulate and practice responses to an incident
- Timely, early communications of cyber security events to all stakeholders
    - Be stakeholder/consumer/patient centric and apply open disclosure approaches

Short Course Access

- Free access to the content within a **Cyber Risk Management in Healthcare** short course

- We hope to publish results so please follow us on LinkedIn or visit our UTAS discovery profiles to access the publication

Question Time