
# BYOD in Hospitals
# Security Issues and Mitigation Strategies

Tafheem Ahmad Wani twani@student.unimelb.edu.au
Dr. Antonette Mendoza mendozaa@unimelb.edu.au
A/Prof. Kathleen Gray kgray@unimelb.edu.au

# Outline

Background (Research Context)

Research questions

Research methodology

Findings

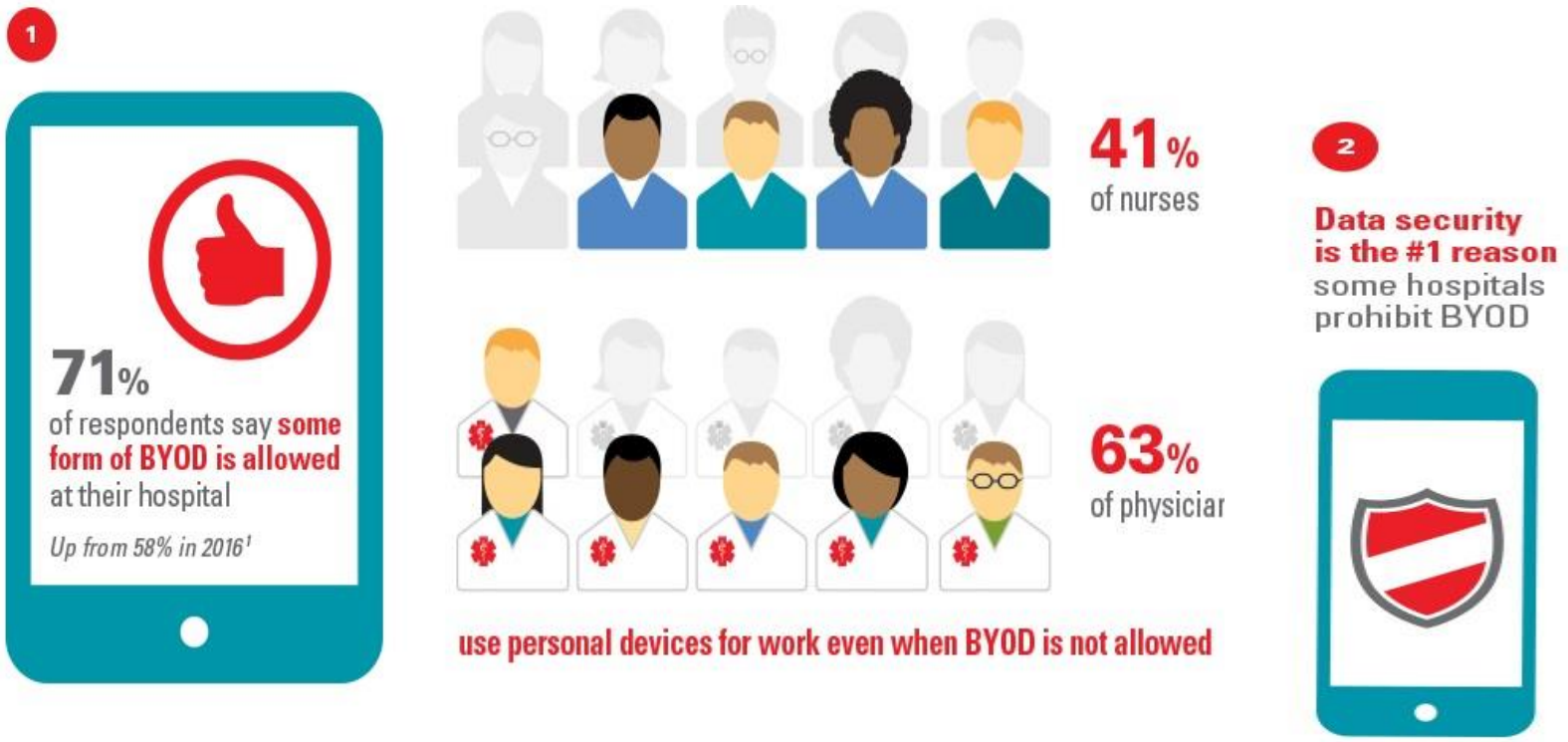
Discussion

Conclusion & Future work

Important references

# Background

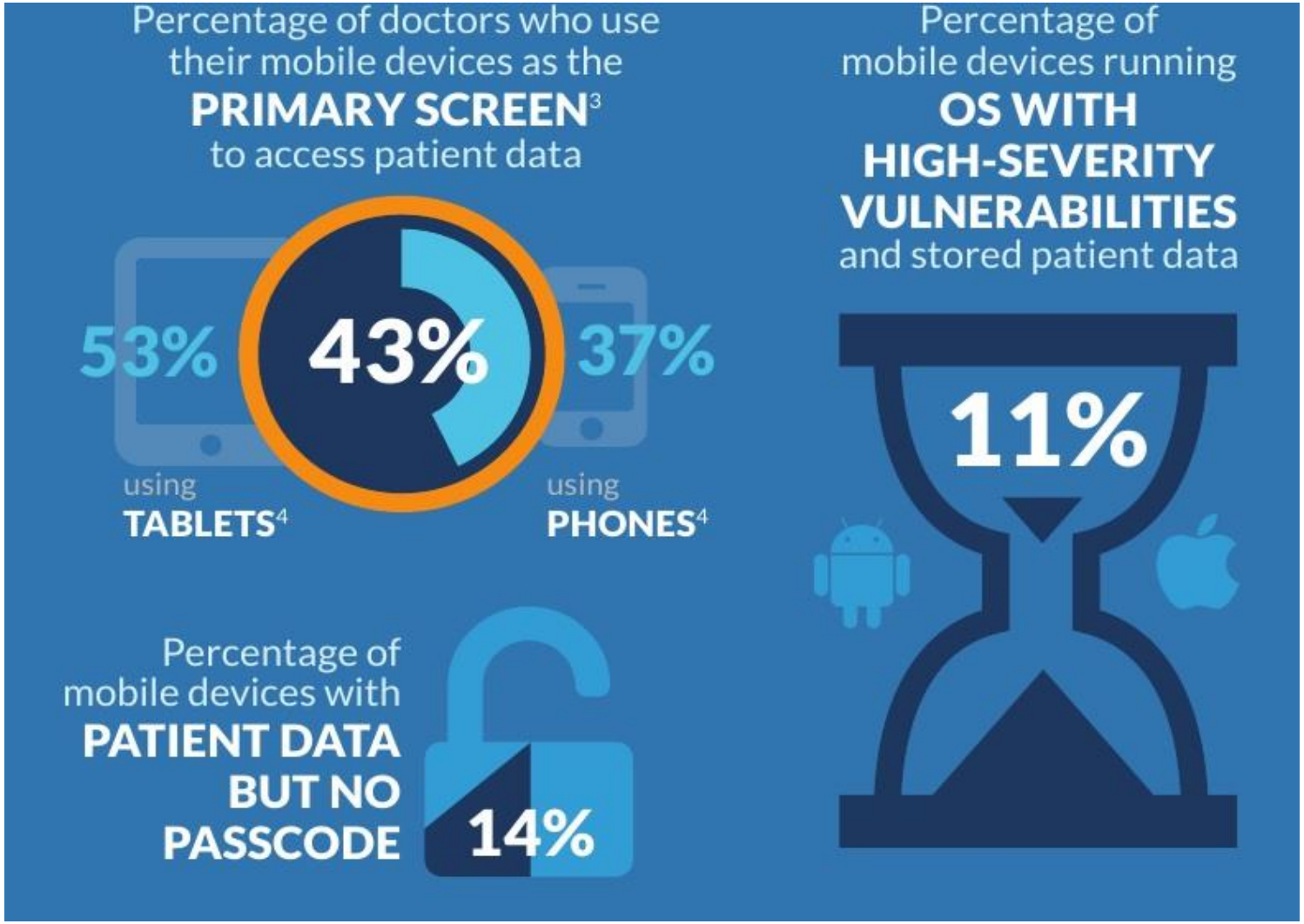
- BYOD= Personal devices at work for professional purposes.
- Increased demands-cost, time and productivity.
- Communication,photography, documentation, clinical reference.




SPOK. (2017). SPOK'S FIFTH ANNUAL MOBILITY STRATEGIES IN HEALTHCARE SURVEY: RESULTS REVEALED. Retrieved from http://www.spok.com/infographic-byod-2017

THE UNIVERSITY OF MELBOURNE

# Background




Skycure. (2016). Mobile Security Trends in Healthcare. Retrieved from https://www.skycure.com/blog/mobile-security-trends-in-healthcare/

# Challenges in health

Among biggest health IT headaches (CIO)

Increased risk of security breaches

Continuous proliferation of IoT devices

Continuous BYOD market growth

Strict legal requirements

Lack of peer-reviewed literature

# Research question

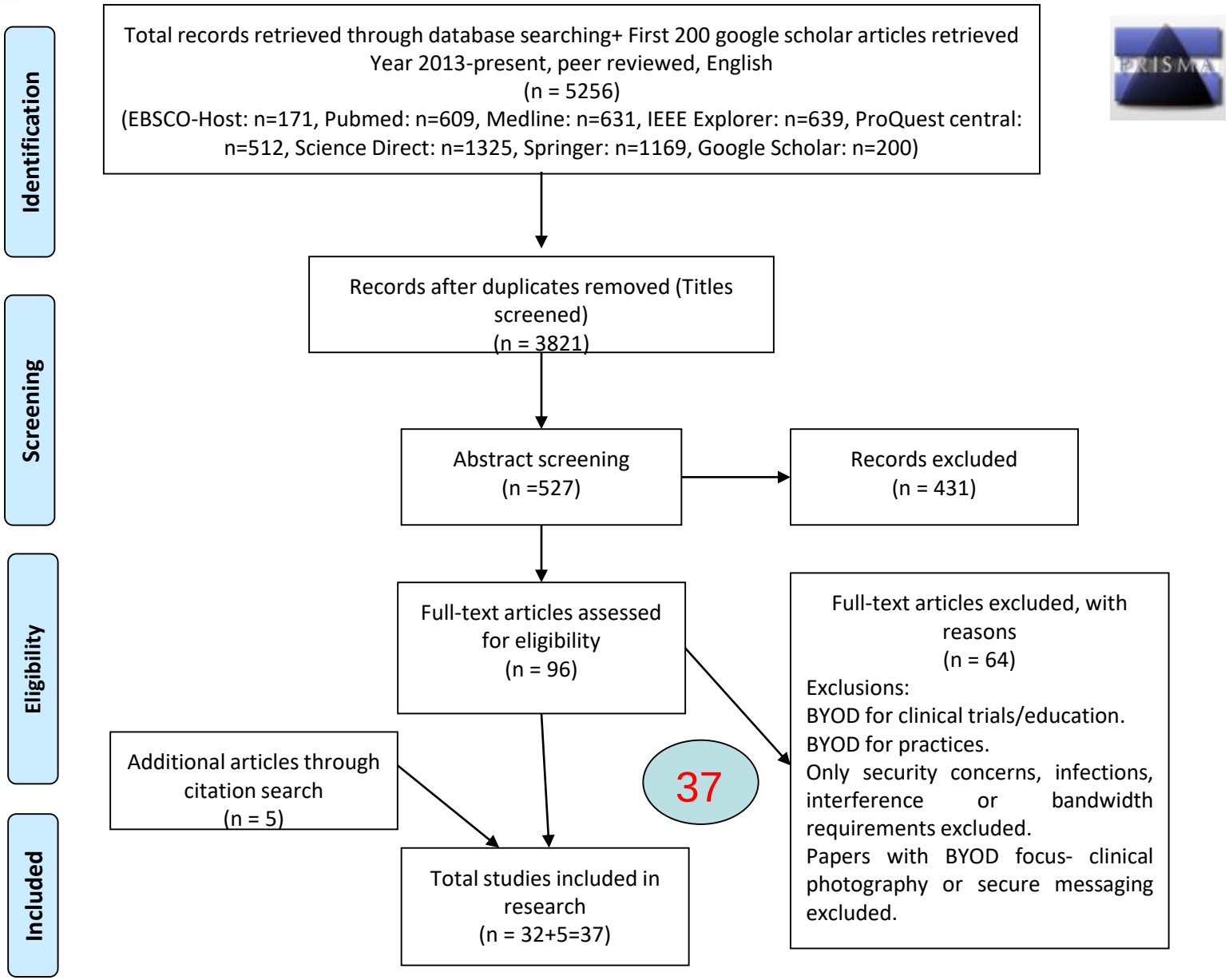
**What mitigation strategies can overcome the security issues of employee BYOD in hospitals?**

# Methodology

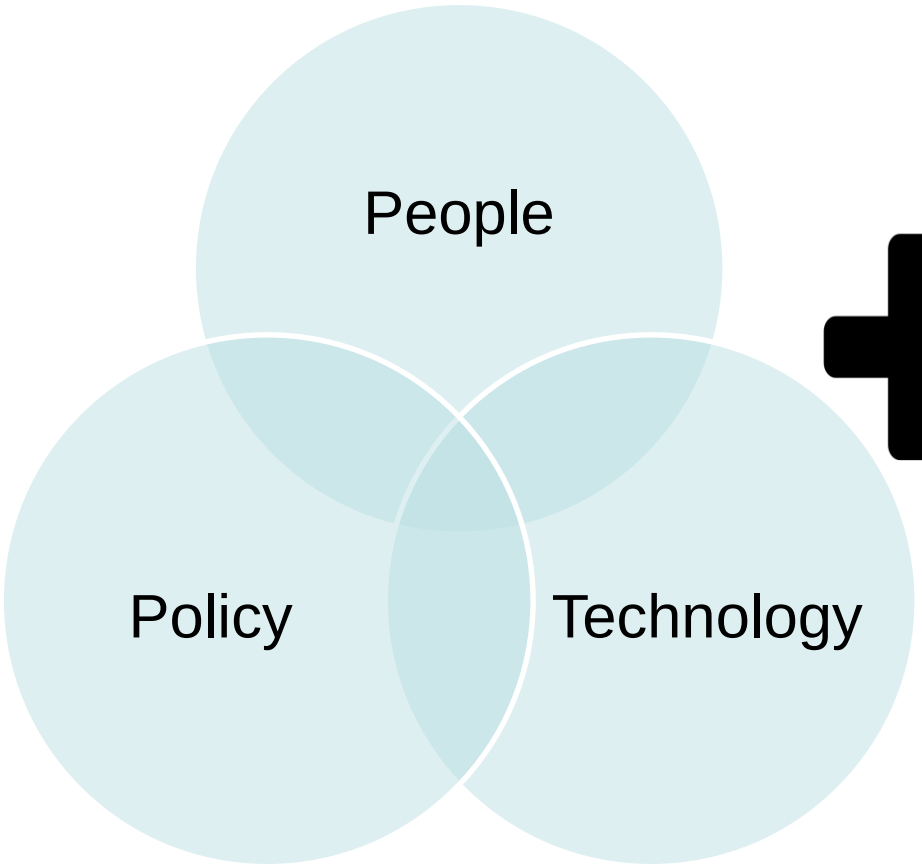
2 step process:

- Comprehensive  literature review of proposed solutions.
- Using two generic security frameworks to organise the solutions into a stepwise mitigation strategy.

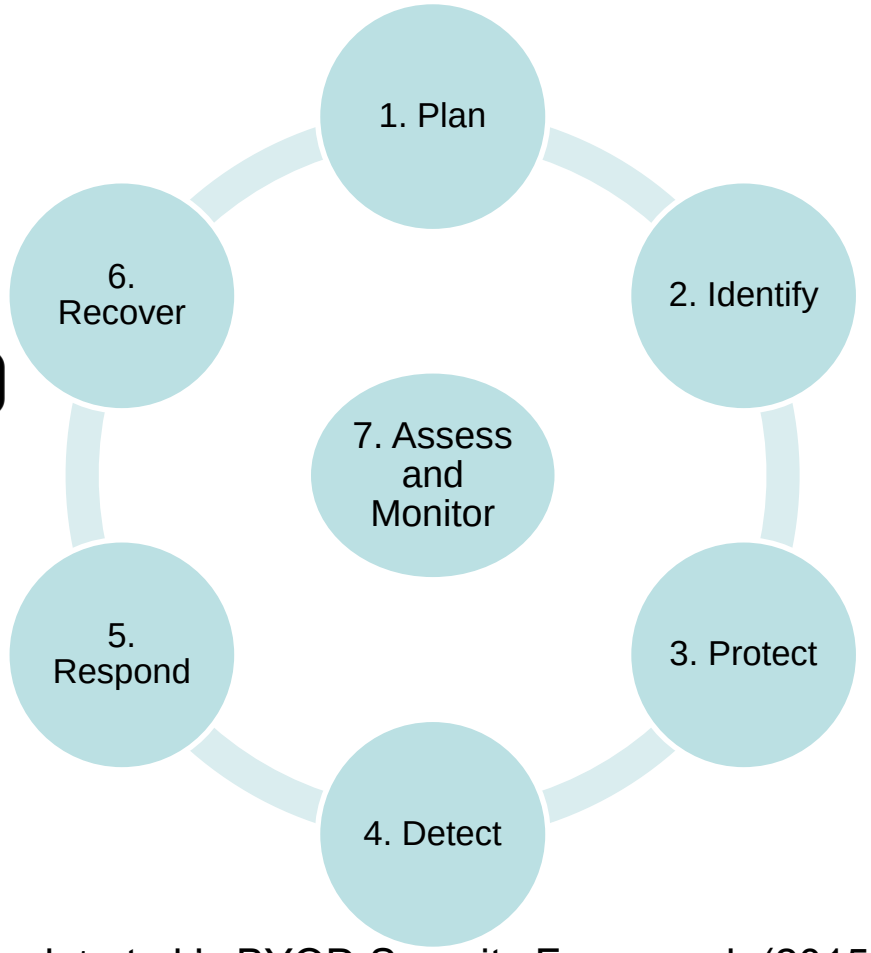
# Literature review - PRISMA Diagram



# Mitigation strategy frameworks

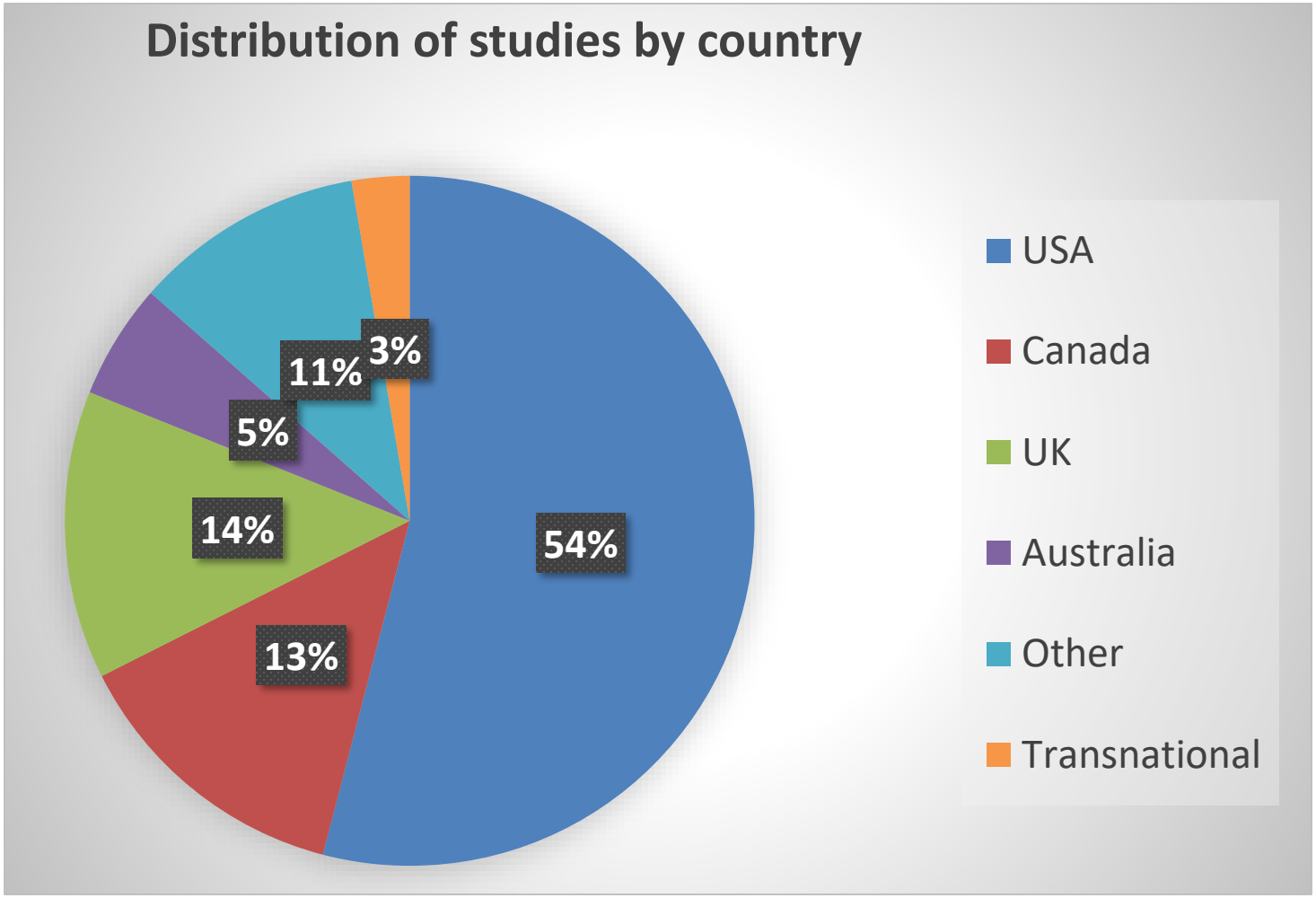



Schlarman's PPT Model (2006)

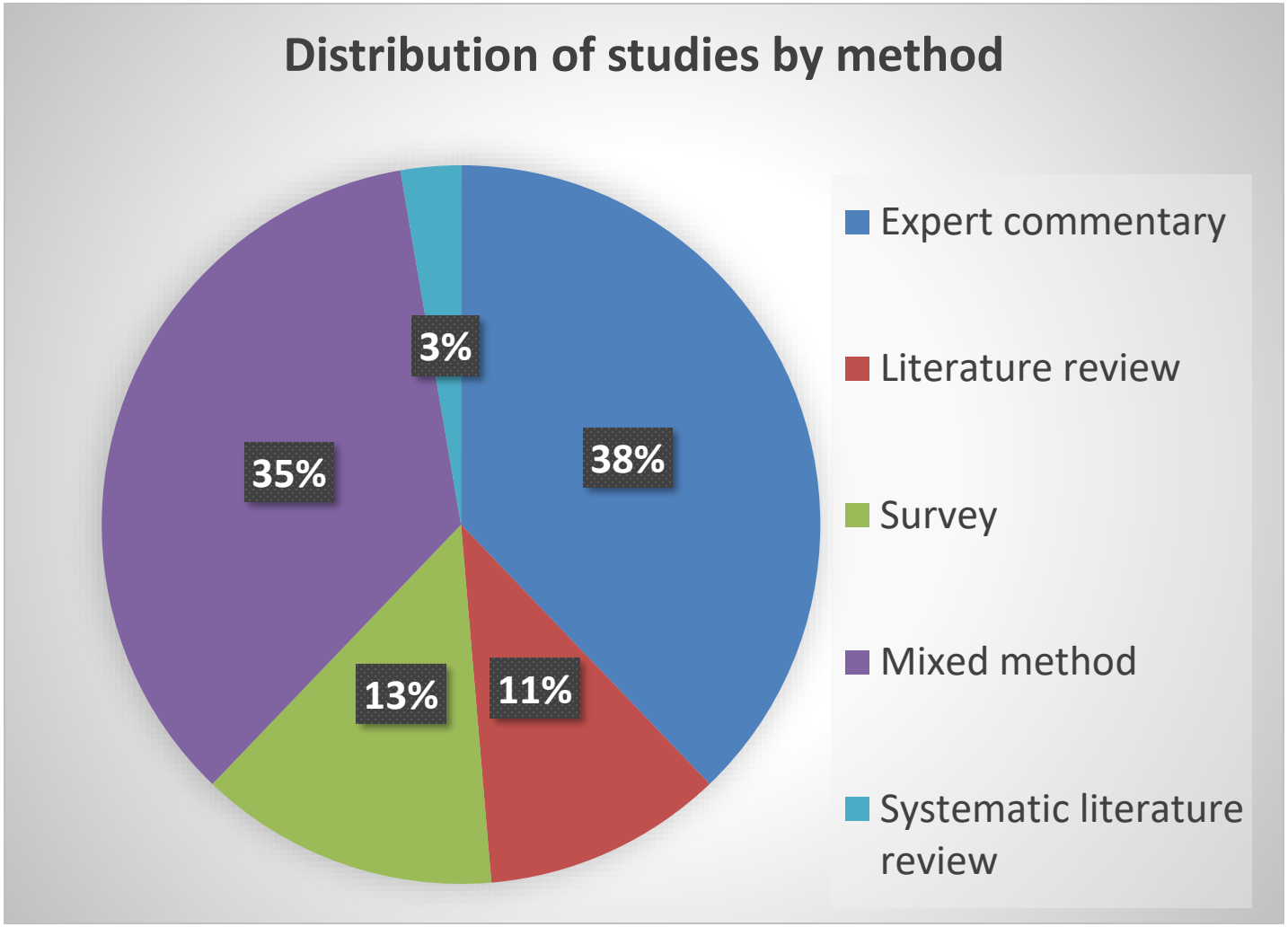



Zahadat et al.'s BYOD Security Framework (2015)

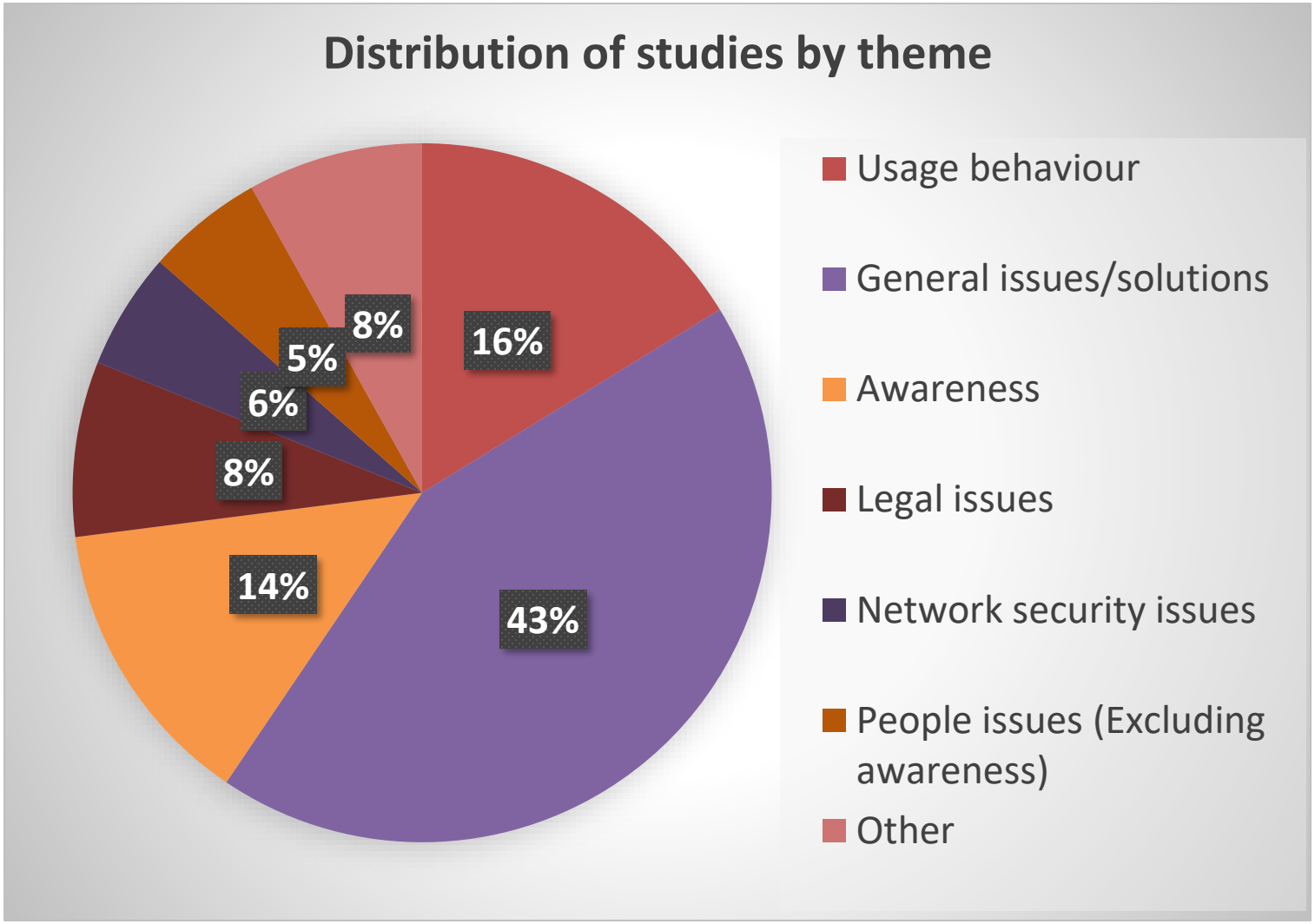
# Review results - distribution by country



# Review results - distribution by method



# Review results - distribution by theme



THE UNIVERSITY OF MELBOURNE

# Key Issues

| | | |
|---|---|---|
| 1 | Identity, Authentication and Access Control | • No or weak authentication mechanisms<br>• Access privilege abuse<br>• Medical Identity Theft |
| 02 | Device, Application and Data Security | • Using malicious applications like mhealth apps<br>• Poorly designed insecure applications<br>• Unauthorised Access by friends or family<br>• Jailbroken or outdated devices<br>• Lost devices |
| 03 | Network Security | • Using infected devices in PAN or LAN<br>• Devices infected through insecure networks like hotspots in WAN |
| 04 | Management and People. | • Lack of clear guidelines on BYOD usage<br>• Burden of managing multiple device types and OS<br>• Usability issues<br>• Lack of trust between employees & management to manage personal devices |
| 05 | Legal (Compliance) | • Strict regulatory requirements for health data<br>• Heavy fines for PHI breaches |

# 7 Steps in Mitigation Strategies

**1.Plan**

- Develop a comprehensive BYOD policy in alignment with hospital needs.
- Establish strong governance for the BYOD program with clear division of roles.
- Sign a legal user agreement with employees using BYOD.
- Choose the right technology,  especially MDM/Mobility management solution.
- Design an awareness program for employees.

**2.Identify**

- Registration and installation of security settings for BYOD devices.
- Use user group list to grant access privilege according to data need.
- Train employees through workshops, LMS, or programs to increase security awareness.

**3.Protect**

- Strict/secure authentication methods like complex passwords or 2 factor authentication.
- Single sign-on for better usability.
- Use enterprise applications with a secure design such as for safe photo sharing and communication.
- Use MDM for automatic enforcement of security controls.
- Use strong encryption methods to protect hospital data in rest and motion.
- Use VPN with virtualisation for transmission security and keeping hospital data within its infrastructure.
- Use containerisation/sandboxing to separate personal and hospital data.

# 7 Steps in Mitigation Strategies

**4.Detect**

- Develop awareness among employees about how to report security incidents.
- Encourage employees to use software such as anti-malwares, anti-virus to detect device vulnerabilities.
- Use visualisation software to understand abnormal behavior of data in order to pinpoint the source of the problem.
- Track location during work hours using MDM.

**5.Respond**

- Blacklist applications known to cause security issues.
- Selectively wipe hospital data in case of theft using containerisation.
- Train employees about standard operating procedure to respond to common security threats.

**6.Recover**

- Use hospital owned private cloud to backup patient data.
- Develop SLAs in case of lack of funding to own private data.
- Use virtualisation and containerisation o minimise hospital data processing on personal devices.
- Employees and management should access each other's data only when required.

**7.Assess & Monitor**

- Periodically review BYOD policy in view of changing security requirements.
- Continuously monitor vendors against designed SLA's.
- Periodically test and approve new devices and communicate to the relevant parties.
- Deprovision repeatably violating devices or devices of employees leaving organisation.

# Discussion

- Overall, the success of a BYOD security program in hospitals is likely to be dependent on how well the balance between security and usability is achieved, given the time-sensitive nature of the work which hospital employees perform.
- A combination of policy control measures, technological solutions, and better people management in a highly regulated hospital industry is likely to be the ideal solution to mitigate BYOD security concerns in hospitals.

# Limitations

BYOD term in research vocabulary addressed in different ways.

Non-English, grey literature, and peer reviewed literature before 2013 has been omitted.

Most studies found were expert commentaries.

Clinical photography and secure messaging excluded from the study.

# Conclusion

- The paper took a broad perspective and tried to highlight the technical, managerial and social issues of BYOD security in hospitals and corresponding mitigation strategies using two frameworks.
- This research needs to be validated through real-life studies in hospitals.
- This research can be beneficial for- hospital senior management/policy developers, hospital IT department, healthcare professionals, informatics researchers.

# Future Work

More studies in real hospital settings

BYOD in resource-constrained settings

BYOD in Australian hospitals

THE UNIVERSITY OF MELBOURNE

# Important References


- Al Ayubi, S. U., Pelletier, A., Sunthara, G., Gujral, N., Mittal, V., & Bourgeois, F. C. (2016). A Mobile App Development Guideline for Hospital Settings: Maximizing the Use of and Minimizing the Security Risks of "Bring Your Own Devices" Policies. JMIR MHealth and UHealth, 4(2). https://doi.org/10.2196/mhealth.4424
- Burns, A. J., & Johnson, M. E. (2015). Securing Health Information. *IT Professional, IT Prof.*, (1), 23. https://doi.org/10.1109/MITP.2015.13
- Filkins, B. L., Kim, J. Y., Roberts, B., Armstrong, W., Miller, M. A., Hultner, M. L., … Steinhubl, S. R. (2016). Privacy and security in the era of digital health: what should translational researchers know and do about it? *American Journal of Translational Research*, *8*(3), 1560–1580.
- Johnson, K. (2014). An IT CEO talks about the BYOD trend. *Biomedical Instrumentation & Technology*, 54–56. https://doi.org/10.2345/0899-8205-48.s1.54
- Marshall, S. (2014). IT Consumerization: A Case Study of BYOD in a Healthcare Setting. *Technology Innovation Management Review*, 14.
- Martinez, K., Borycki, E., & Courtney, K. L. (2017). Bring Your Own Device and Nurse Managers' Decision Making. *CIN: Computers, Informatics, Nursing*, *35*(2), 69. https://doi.org/10.1097/CIN.0000000000000286
- Moyer, J. e. (2013). Managing Mobile Devices in Hospitals: A Literature Review of BYOD Policies and Usage. *JOURNAL OF HOSPITAL LIBRARIANSHIP*, (3), 197.
- Sansurooh, K., & Williams, P. (2014). BYOD in ehealth: Herding cats and stable doors, or a catastrophe waiting to happen? *Australian EHealth Informatics and Security Conference*. https://doi.org/10.4225/75/5798284331b46
- Smith, K. A., Zhou, L., & Watzlaf, V. J. M. (2017). User Authentication in Smartphones for Telehealth. *International Journal Of Telerehabilitation*, *9*(2), 3–12. https://doi.org/10.5195/ijt.2017.6226
- Stephens, K., Zhu, Y., Harrison, M., Iyer, M., Hairston, T., & Luk, J. (2017). Bring Your Own Mobile Device (BYOD) to the Hospital: Layered Boundary Barriers and Divergent Boundary Management Strategies. https://doi.org/10.24251/HICSS.2017.426
- Williams, J. (2014). Left to their own devices how healthcare organizations are tackling the BYOD trend. *Biomedical Instrumentation & Technology*, *48*(5), 327–339. https://doi.org/10.2345/0899-8205-48.5.327

# Contact


- https://dl.acm.org/citation.cfm?id=3290729
- Email: twani@student.unimelb.edu.au