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
Background

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

Percentage of doctors who use their mobile devices as the PRIMARY SCREEN to access patient data

- **53%** using TABLETS
- **43%**
- **37%** using PHONES

Percentage of mobile devices running OS WITH HIGH-SEVERITY VULNERABILITIES and stored patient data

- **11%**

Percentage of mobile devices with PATIENT DATA BUT NO PASSCODE

- **14%**

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
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.
Total records retrieved through database searching: First 200 Google Scholar articles retrieved. Year 2013-present, peer reviewed, English. (n = 5256)

Records after duplicates removed (Titles screened) (n = 3821)

Abstract screening (n = 527)

Records excluded (n = 431)

Full-text articles assessed for eligibility (n = 96)

Additional articles through citation search (n = 5)

Total studies included in research (n = 32 + 5 = 37)

Exclusions:
BYOD for clinical trials/education.
BYOD for practices.
Only security concerns, infections, interference or bandwidth requirements excluded.
Papers with BYOD focus- clinical photography or secure messaging excluded.
Mitigation strategy frameworks

Schlarman’s PPT Model (2006)

Distribution of studies by country

- USA: 54%
- Canada: 14%
- UK: 13%
- Australia: 11%
- Other: 5%
- Transnational: 3%
Review results - distribution by method

Distribution of studies by method

- 38% Systematic literature review
- 35% Literature review
- 13% Mixed method
- 11% Survey
- 3% Expert commentary
Review results - distribution by theme

Distribution of studies by theme

- Usage behaviour: 16%
- General issues/solutions: 43%
- Awareness: 14%
- Legal issues: 8%
- Network security issues: 6%
- People issues (Excluding awareness): 5%
- Other: 8%
Key Issues

1. Identity, Authentication and Access Control
   - No or weak authentication mechanisms
   - Access privilege abuse
   - Medical Identity Theft
   - Using malicious applications like mhealth apps
   - Poorly designed insecure applications
   - Unauthorised Access by friends or family
   - Jailbroken or outdated devices
   - Lost devices

2. Device, Application and Data Security
   - Using infected devices in PAN or LAN
   - Devices infected through insecure networks like hotspots in WAN

3. Network Security
   - Lack of clear guidelines on BYOD usage
   - Burden of managing multiple device types and OS
   - Usability issues
   - Lack of trust between employees & management to manage personal devices

4. Management and People
   - Strict regulatory requirements for health data
   - Heavy fines for PHI breaches

5. Legal (Compliance)
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 to 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.
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.
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
Important References

• [https://dl.acm.org/citation.cfm?id=3290729](https://dl.acm.org/citation.cfm?id=3290729)
• Email: twani@student.unimelb.edu.au