npj | digital medicine

News & Views

Published in partnership with Seoul National University Bundang Hospital

https://doi.org/10.1038/s41746-024-01044-5

Can we learn from an imagined ransomware attack on a hospital at home platform?

Stephen Gilbert, Francesco Ricciardi, Tauseef Mehrali & Constantinos Patsakis

Check for updates

The hospital at home concept integrates key digital medicine technologies and concepts in a single platform approach, with telemedicine, wearables, and sensors. It could bring benefits to patients, who face lower risks from hospital infections and who want to be at home with their loved ones. Moreover, it may lead to efficiency savings, through its seamless integration of data flows, and therefore is likely to be an increasingly implemented model. But what happens when the platform succumbs to exploited platform/infrastructure vulnerabilities or cyber attacks like ransomware that have been weaponized to bring networked systems crashing down? Exploring the attack modes and their consequences could help prioritize adequate safeguards.

How critical is cybersecurity for digital medicine patient sensors, such as those used in remote patient monitoring? During the COVID-19 pandemic and subsequently, the hospital at home (HaH) concept has been increasingly adopted, particularly in the US, Switzerland, and the UK[1]. It is an innovative model that provides hospital-level care in the patient's home, supported by digital systems, remote monitoring, and telemedicine[2]. It can be used as an alternative to admission or to enable earlier discharge[3], and it has been proposed as a substitute for acute care in hospitals for specific patient populations, who would traditionally have required close hospital observation. This model also allows for a more rational use of health professionals and better addresses the shortage of professional health workers. The following simulated scenario, which has been designed with reference to realistic HaH implementations[4–7] and reports of attacks on hospital systems[8,9], explores a possible ransomware attack and its consequences for patient safety and privacy in a fictional implementation of the HaH concept. The scenario is described as a sequence of events in different settings relevant to the HaH, the interconnection of which becomes clear as the narrative progresses.

'Ward@Home' launch and development

The following events are reported in chronological order. This simulated scenario is entirely hypothetical and fictitious. Any similarity to actual persons, entities, or organizations is purely coincidental.

System launch, March 15, 2023, metropolitan area, somewhere in continental Europe. Patients in *Ward@Home*: 0

National Press office, CommiNet: "*CommiNet and TradiCare launch the* Ward@Home *program to transform regional health services*. Our partnership will deliver Ward@Home solutions via our unique virtual care platform (Fig. 1a). We use AI to collect and monitor health information remotely, working with our community care professionals. The platform detects problems with a patient in real-time, predicts the risk of worsening conditions, and notifies the patient, carers, and health care professionals, as required. Today's launch is a proud moment for CommiNet and TradiCare, and our 'doctor-led, digitally enhanced' strategy."

Pre-launch review, March 16, 2023, CommiNet corporate HQ. Patients in Ward@Home: 0

Meeting: 'Ward@Home' *platform* pre-launch system review.

Present: Senior executive and contributing project/clinical teams CommiNet & TradiCare,

Presentation, 'Summary of Risk Management', CommiNet VP of Regulatory, Quality and Compliance (VP RQC): "In the risk management report, you can see that all risks have been mitigated. All residual risks are assessed as acceptable, and the benefit-risk assessment shows a positive ratio of risk versus benefit … Indeed, we are confident that the patients in Ward@Home will receive equivalent, if not better, monitoring than in standard hospital care, particularly at night and weekends. The system is fully compliant with GDPR."

Question: IT Systems Responsible Person, TradiCare: "How has the risk of extended system downtime been mitigated?"

Answer CommiNet *VP RQC*: "*Our TightNet™ network system architecture has achieved 99.999% uptime across all our regional networks for 5 years, and the 'Ward@Home' platform software is verified and validated, passing all test sets and is compliant with the state-of-the-art cybersecurity standards.*

Answer: Chief Transformation Officer, TradiCare: "We can switch back to the current standard of care if we experience any unexpected teething problem. We will be closely monitoring the platform as it goes live. Our community teams are well-trained, and the 24/7 operation center is adequately staffed to sort out any launch issues. Our backup policies keep incremental backups daily, and we have provisioned long-term offline backups. This allows us to revert our systems almost instantly to any secure state in the past, should it be necessary."

TradiCare Annual General Meeting, January 24, 2024. Patients in Ward@Home: 573

Presentation, 'Corporate Statement', CEO TradiCare: "The healthcare sector has been under significant pressure in 2023. As a sector, we face a convergence of cost pressures and tightness in the clinical labor market with a shortage of both doctors and paramedics. TradiCare has a better economic

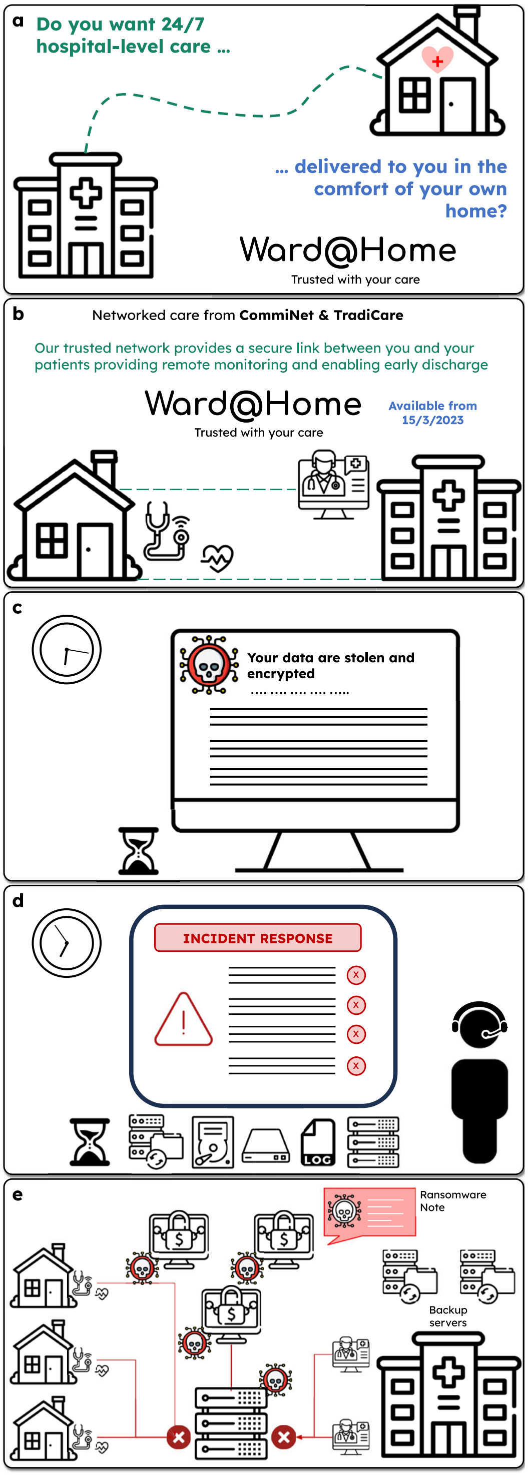

a
Do you want 24/7 hospital-level care ...
... delivered to you in the comfort of your own home?
Ward@Home
Trusted with your care
b
Networked care from CommiNet & TradiCare
Our trusted network provides a secure link between you and your patients providing remote monitoring and enabling early discharge
Ward@Home
Trusted with your care
Available from 15/3/2023
c
Your data are stolen and encrypted
d
INCIDENT RESPONSE
LOG
e
Ransomware Note
Backup servers

Fig. 1 | Storyboard of events. **a** Launch of Ward@Home service and description for patients. **b** Launch of Ward@Home service and description for physicians. **c** Ransomware attack notification message. **d** An Incident Room (IR) is established according to the Ward@Home cybersecurity procedures. **e** Description of the Ransomware attack and its effects on the Ward@Home network.

outlook than similar care systems due to our pioneering technology adoption. We will continue to leverage our digital transformation program to deliver significant cost savings and allocate our clinical personnel in the best way possible.

‘Ward@Home’ ransomware attack, July 20, 2025, Sunday

Patients in Ward@Home: 7597, of which 2991 have the status ‘close observation’

Staff at operation center: 13

Community care staff: 23 (attending patients); 13 (available)

Time: 00:06:17. Ambient temperature: 23 °C. Ward@Home operators are noticing malfunctions in their systems. The swift intervention of a technician found that some of the servers and some hosts in Ward@Home that were open had a Notepad window on their screens (Fig. 1b) displaying the message of Fig. 2.

Time: 00:06:51. Ambient temperature: 24 °C. Major incident declared to TradiCare and CommiNet by Operational Director (OD) ‘Ward@Home’. Major Incidents not transmitted to staff or patients as servers are locked. The OD telephones the executive leadership teams and all staff for whom he has personal contact details, asking them to call all their own staff contacts and to share patient contact details. An Incident Room (IR) is established according to the Ward@Home cybersecurity procedures (Fig. 1c).

The Ward@Home team tries to revert to backups; however, they realize that the short-term backup servers have been compromised. The offline backup could be used to recover most of the users’ data and is 2 weeks old. The time needed to re-install the servers and restore the backups is estimated at 2 days. The ‘Ward@Home’ services will not be available during this time (Fig. 3).

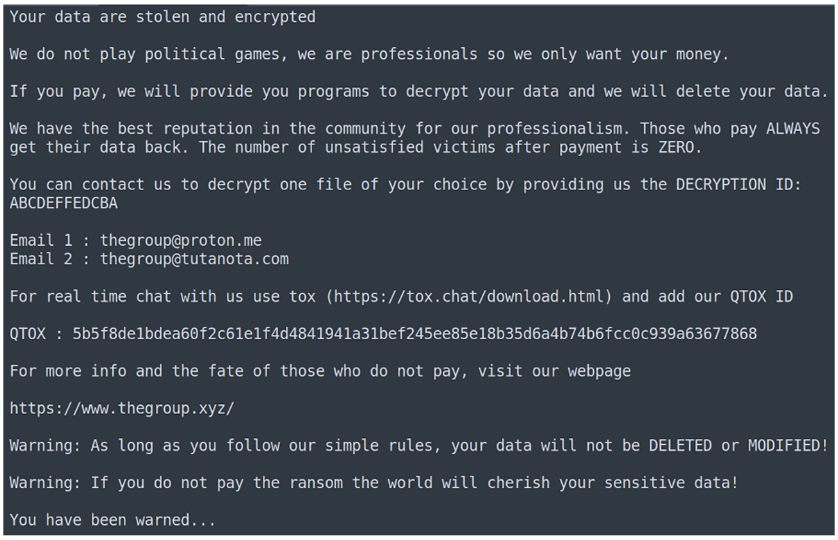
Time: 00:07:49. Ambient temperature: 27 °C. Summary of OD status report to IR:

Present: all contactable OC staff, CEO TradiCare, VP RQC CommiNet“

1. *No communication possible via ‘Ward@Home’ platform to staff or patients*
2. *All ‘Ward@Home’ patients and Operations Room phones are locked.*
3. *Available Incident Room staff: 37.*
4. *Available Community care staff: 93, with efforts made to contact more.*
5. *Staff communications are only possible via mobile phones and WhatsApp.*
6. *Lists of patients under critical care and patient addresses are encrypted: IR whiteboard created.*
7. *All contactable staff have been asked to share known vulnerable patients and their addresses and mobile numbers, if known, by WhatsApp.”*

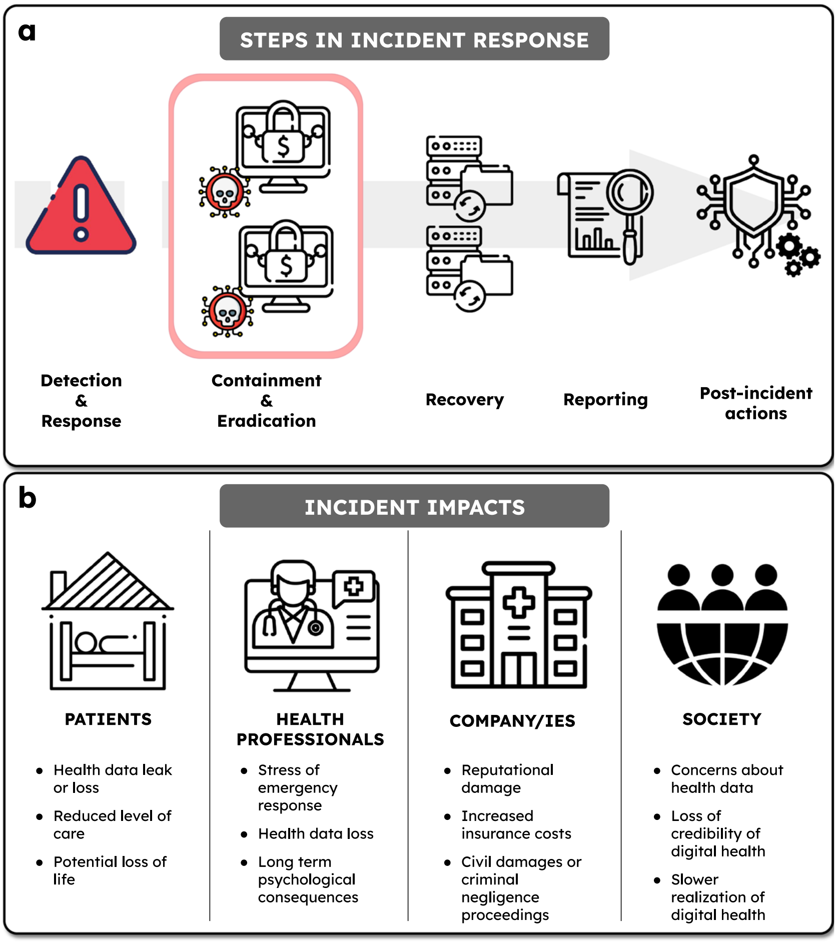
Question: OD to Clinical Duty Lead: ‘Ward@Home’: *“How many Ward@Home patients need urgent intervention or hospitalization per day.” Answer: Normally, 3%, which rose to 9% in the heat wave of July 2023, but then we had no patients in the* ‘close observation’ *status. With this afternoon’s predicted temperature of 46 °C, the best guess is 800 patients, whom we cannot identify, contact, or effectively triage according to risk. Initial reports indicate that breathing and pulse oximetry monitors are not communicating with the patient consoles, and neither patients nor staff are being alerted to worsening clinical conditions. Patients are finding it extremely difficult to contact us because the telephone lines are jammed and there are long delays in getting*

Fig. 2 | Ransomware attack notification. This message was displayed on a Notepad window on screens of Ward@Home computer terminals.



```
Your data are stolen and encrypted

We do not play political games, we are professionals so we only want your money.

If you pay, we will provide you programs to decrypt your data and we will delete your data.

We have the best reputation in the community for our professionalism. Those who pay ALWAYS
get their data back. The number of unsatisfied victims after payment is ZERO.

You can contact us to decrypt one file of your choice by providing us the DECRYPTION ID:
ABCDEFFEDCBA

Email 1 : thegroup@proton.me
Email 2 : thegroup@tutanota.com

For real time chat with us use tox (https://tox.chat/download.html) and add our QTOX ID

QTOX : 5b5f8de1bdea60f2c61e1f4d4841941a31bef245ee85e18b35d6a4b74b6fcc0c939a63677868

For more info and the fate of those who do not pay, visit our webpage

https://www.thegroup.xyz/

Warning: As long as you follow our simple rules, your data will not be DELETED or MODIFIED!

Warning: If you do not pay the ransom the world will cherish your sensitive data!

You have been warned...
```

Fig. 3 | Summary of the response to and impacts of a cybersecurity incident of the type described. **a** The steps to be undertaken in response to a cybersecurity incident. **b** Impacts of the cybersecurity attack on patients, health professionals, companies, and society.


a
STEPS IN INCIDENT RESPONSE
Detection & Response
Containment & Eradication
Recovery
Reporting
Post-incident actions
b
INCIDENT IMPACTS
PATIENTS
• Health data leak or loss
• Reduced level of care
• Potential loss of life
HEALTH PROFESSIONALS
• Stress of emergency response
• Health data loss
• Long term psychological consequences
COMPANY/IES
• Reputational damage
• Increased insurance costs
• Civil damages or criminal negligence proceedings
SOCIETY
• Concerns about health data
• Loss of credibility of digital health
• Slower realization of digital health

ambulances to them due to the heat wave and response to unrelated emergency calls. If the situation is not resolved before peak afternoon temperatures are reached, we anticipate many deaths in our patient group directly attributable to the attack. There is also a substantial data breach, and we will make a full assessment of this within a 48-hour window.”

Summary

We address the question: when the HaH meets a systemic ransomware attack (or other similar cybersecurity or major network event cueing massive outage), can that be labeled a Black Swan event[10], i.e., an unpredictable event that is beyond what is typically expected of a situation and has potentially severe consequences? This article predicts such events, so by definition, they cannot be labeled as unpredictable ‘Black Swans’ in the future. This article is not designed to create alarm or to hinder the development of the HaH model, but rather to highlight the need for careful risk assessment, planning, monitoring, and defense-in-depth approaches to protect this care model against cybersecurity vulnerabilities[11]. If a HaH system is vulnerable to attack, this would turn the very scalability and inherent benefit of the system on its head resulting in a systematic incident involving many patients. Large cybersecurity incidents that cripple critical infrastructure, including health system infrastructure, are no longer rare[12,13]. Identified healthcare system cybersecurity vulnerabilities, which are also components of HaH systems include cyber-medical systems, electronic consultation services, and Internet of Medical Things (IoMT) devices, particularly when these systems are not updated with security patches The former two systems are vulnerable to ransomware and denial of service (DoS) attacks, while IoMT is vulnerable to DoS attacks[12,13]. Recent policy announcements and guidelines recognize the criticality of the cybersecurity challenge in medicine[14]. In the healthcare sector between 2018 and 2022, there has been a 278% increase in large cybersecurity breaches involving ransomware[15]. Actions that can be taken by to protect HaH systems include the careful identification of attack modes, the redesign of the entire system networked systems adopting defense in depth and zero trust principles (a series of layered defensive mechanisms designed to protect health data and systems with deeper layers protecting if higher layers succumb to attack)[16], choice of IoMT subcomponents developed according to the best practices of design for resilience to cybersecurity threats[14] IoMT ‘fleet’ oversight management with risk assessed approaches for over-the-air patching of IoMT device vulnerabilities[16], and adequate and repeated training for personnel and, if needed, patients[12,13]. If a HaH system succumbs to a situation as severe as the fictional one described above, the consequences we described are realistic, patient deaths and severe harm, the inability of clinicians to deliver care, and a loss of confidence and trust in healthcare systems; setting aside criminal proceedings for failing to protect patients under their care.

Cybersecurity risks in the healthcare system that are now developing around digital technologies, particularly as they relate to HaH approaches, should be recognized as critical infrastructure risks that could in themselves cause a major public health emergency. These risks no longer just relate to data loss or danger to the individual patient and should be placed on the highest level of priority with the introduction of new modes of networked care delivery, and budgets should be prioritized for their delivery.

Stephen Gilbert[1] ✉, **Francesco Ricciardi**[2], **Tauseef Mehrali**[3] & **Constantinos Patsakis**[4]
[1]Else Kröner Fresenius Center for Digital Health, TUD Dresden University of Technology, Dresden, Germany. [2]IRCCS Casa Sollievo della Sofferenza, San Giovanni Rotondo, Italy. [3]Ada Health GmbH, Berlin, Germany. [4]University of Piraeus and Athena Research Center, Dimitriou, Greece.
✉e-mail: stephen.gilbert@tu-dresden.de

Received: 23 November 2023; Accepted: 5 February 2024;
Published online: 20 March 2024

References

1. Deloitte. *Hospital at Home. A Model with a Future* (Deloitte, 2022).
2. British Geriatrics Society. *Bringing Hospital Care Home: Virtual Wards and Hospital at Home for Older People (Position Statement)* (British Geriatrics Society, 2022).
3. Lasserson, D. & Cooksley, T. Virtual wards: urgent care policy must follow the evidence. *BMJ* **380**, 343 (2023).
4. Gilbert, S. Digital respiratory healthcare regulation (eds Pinnock, H., Poberezhets, V. & Drummond, D.). In *Digital Respiratory Healthcare* (European Respiratory Society, 2023).
5. Hakim, R. Realising the potential of virtual wards. (2023).
6. Greenhalgh, T. et al. Remote management of covid-19 using home pulse oximetry and virtual ward support. *BMJ* **372**, n677 (2021).
7. O’Malley, E.-J., Hansjee, S., Abdel-Hadi, B., Kendrick, E. & Lok, S. A Covid-19 virtual ward model: a preliminary retrospective clinical evaluation from a UK district general hospital. *J. Prim. Care Community Health* **13**, 21501319211066667 (2022).
8. McGlave, C. C., Nikpay, S. S., Henning-Smith, C., Rydberg, K. & Neprash, H. T. Characteristics of short-term acute care hospitals that experienced a ransomware attack from 2016 to 2021. *Health Aff. Sch* **1**, qxad037 (2023).
9. McGlave, C. C., Neprash, H. & Nikpay, S. *Hacked to Pieces*? *The Effects of Ransomware Attacks on Hospitals and Patients*. SSRN Scholarly Paper https://doi.org/10.2139/ssrn.4579292 (2023).
10. Taleb, N. N. *The Black Swan* (Random House, 2009).
11. Medicine, T. L. R. Digital health: balancing innovation and cybersecurity. *Lancet Respir. Med.* **9**, 673 (2021).
12. Alawida, M., Omolara, A. E., Abiodun, O. I. & Al-Rajab, M. A deeper look into cybersecurity issues in the wake of Covid-19: a survey. *J. King Saud Univ.—Comput. Inf. Sci.* **34**, 8176–8206 (2022).
13. He, Y., Aliyu, A., Evans, M. & Luo, C. Health care cybersecurity challenges and solutions under the climate of COVID-19: scoping review. *J. Med. Internet Res.* **23**, e21747 (2021).
14. US FDA. *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Guidance for Industry and Food and Drug Administration Staff* (US FDA).
15. Healthcare Sector Cybersecurity. I*ntroduction to the Strategy of the U.S. Department of Health and Human Services* (Healthcare Sector Cybersecurity, 2023).
16. Sun, Y., Lo, F. P.-W. & Lo, B. Security and privacy for the internet of medical things enabled healthcare systems: a survey. *IEEE Access* **7**, 183339–183355 (2019).

Acknowledgements

This work was supported by the European Commission under the Horizon Europe Program, as part of the project CYMEDSEC (101094218). This work was also supported by the COST Action GoodBrother, Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living (CA 19121). The content of this article does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the authors.

Author contributions

S.G., F.R., T.M., and C.P. developed the concept of the manuscript. S.G. wrote the first draft of the manuscript. S.G., F.R., T.M., and C.P. contributed to the writing, interpretation of the content, and editing of the manuscript, revising it critically for important intellectual content. S.G., F.R., T.M., and C.P. had final approval of the completed version. S.G., F.R., T.M., and C.P. take accountability for all aspects of the work and ensure that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

Competing interests

F.R. and C.P. declare no nonfinancial interests and no competing financial interests. T.M. declares no nonfinancial interests and a competing financial interest as the Vice President of Medical Safety & Regulatory Affairs at and holds share options in, Ada Health GmbH. S.G. declares a nonfinancial interest as an Advisory Group member of the EY-coordinated “Study on Regulatory Governance and Innovation in the Field of Medical Devices” conducted on behalf of the DG SANTE of the European Commission. S.G. declares the following competing financial interests: he has or has had consulting relationships with Una Health GmbH, Lindus Health Ltd., Flo Ltd, Thymia Ltd., FORUM Institut für Management GmbH, High-Tech Gründerfonds Management GmbH, and Ada Health GmbH and holds share options in Ada Health GmbH. S.G. is a News and Views Editor for npj Digital Medicine. S.G. played no role in the internal review or decision to publish this News and Views article.

Additional information

Correspondence and requests for materials should be addressed to Stephen Gilbert.

Reprints and permissions information is available at
http://www.nature.com/reprints