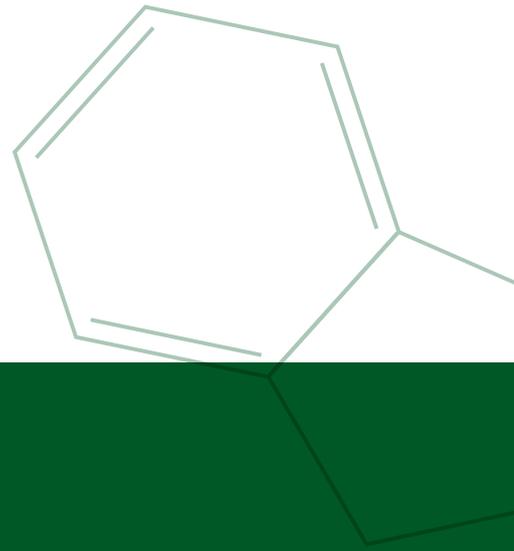
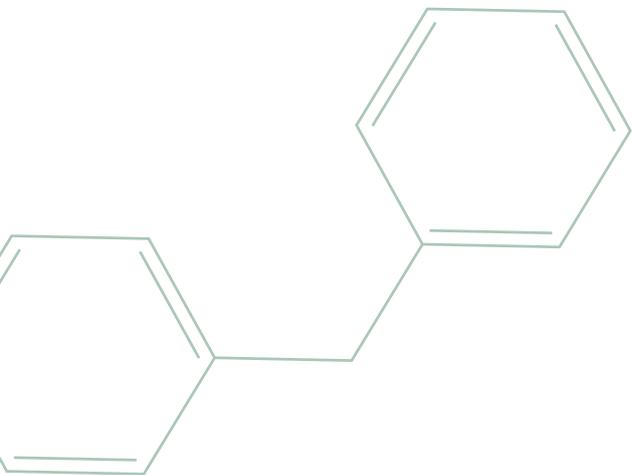




**Australian Government**  
**Australian Digital Health Agency**



*Preventing and recovering from*  
**RANSOMWARE**



*A briefing for*  
**senior managers**



*This document has been prepared for senior managers in the health sector to help increase understanding and facilitate better management of the risks posed by ransomware. A companion document, prepared for information technology (IT) teams, provides further information and outlines security measures and practices that will help healthcare organisations prevent and recover from a ransomware attack.*

## Summary

Ransomware is a type of malicious software that denies access to computers and files and demands that affected organisations make a payment to regain access to their information. CryptoLocker is a particularly virulent and widely known form of ransomware that encrypts all files located within the infected computer, its shared network drives, and any attached storage.

A ransomware attack on a healthcare organisation can potentially cause significant reputational damage, clinical safety risks, financial harm, and impact to continuity of business operations. Any network connected system could be affected, such as: desktop computers; clinical, personnel or financial information systems; databases containing digital health records; or medical devices.

Ransomware, which has become increasingly common within the health sector<sup>1</sup>, may pose a significant risk to the security and privacy of individual health information and impede organisations' ability to deliver healthcare services.<sup>2</sup> Depending on the access obtained, an attacker could also read, modify, export or publicly release digital health records.<sup>3</sup>

The comparative prevalence of ransomware in the health sector was highlighted in the Office of the Australian Information Commissioner's Notifiable Data Breaches Quarterly Statistics Report for the period October to December 2018. The percentage of ransomware-related data breaches reported for the health sector was twice that of other organisation types.<sup>4</sup> It is vital that organisations in the health sector understand their risks and are prepared to prevent and respond to ransomware attacks.

## Key points

- 1** Given that organisations in the health sector have professional and legal obligations to protect health information<sup>5</sup>, it is important that accountable senior managers understand how the risk posed by ransomware is being managed within their organisation and determine if the risk mitigations are acceptable. Suggested questions to ask your ICT team include:
  - Have existing security controls within the organisation been reviewed in light of the risk posed by ransomware? If so, what was the outcome? What is the level of risk and is it acceptable?
  - How are backups of critical systems managed and secured? Will this approach prevent backups being compromised by ransomware? When was the backup process last tested and what was the outcome?
  - What approach is taken to ensure known security vulnerabilities are addressed? Are there additional mitigation strategies that should be implemented, such as those outlined in the Australian Digital Health Agency's publication 'Patching: Protecting healthcare information by updating systems and software'?
  - Does the ICT team need additional support or resources to better manage and mitigate the organisation's risks? Are there additional mitigation strategies that should be implemented, such as those listed in the companion document, Preventing and recovering from ransomware - a briefing for IT Professionals?
- 2** Ideally, the risks posed by ransomware and other malware should be managed as part of a comprehensive information security framework or in accordance with an appropriate information security standard. There are a number of information security frameworks and standards, which organisations in the health sector can use to improve the security and resilience of their digital health systems and help meet their professional and legal obligations to protect health information.
- 3** If your organisation doesn't have the resources or expertise to assess its risks or to implement adequate security measures, it is recommended that you seek professional advice from a reputable IT service provider or information security consultant.

- 4 If ransomware does compromise your organisational systems, please note the following:
- Paying attackers is not recommended as this will encourage further attacks and does not guarantee that organisations will be able to recover affected files or avoid a data breach. It is suggested that you seek legal advice if paying the ransom is considered necessary.
  - Government agencies and businesses covered by the Privacy Act 1988 (Cth) will need to report individual health information breaches under the Notifiable Data Breaches Scheme. Refer to advice from the Office of the Australian Information Commissioner (OAIC) for details.<sup>6</sup>
  - If systems used to access or update the My Health Record system are compromised, it is possible that the security or integrity of the My Health Record system has also been compromised. For any event or situation where there is a suspected or actual data breach relating to the My Health Record system, organisations are required to notify the Australian Digital Health Agency, (the System Operator) and the OAIC.<sup>7</sup>

## References

- 1 Healthcare held to ransom. [Internet]. Available from: <http://www.cso.com.au/article/597125/healthcare-held-ransom-how-protect-australian-healthcare-systems-patients-from-cybercrime/>
- 2 Ransomware and recent variants. [Internet]. Available from: <https://www.us-cert.gov/ncas/alerts/TA16-091A>
- 3 Webcast: Prepare and respond to healthcare ransomware. [Internet]. Available from: <http://healthitsecurity.com/resources/webcasts/prepare-and-respond-to-healthcare-ransomware-attacks>
- 4 Office of the Australian Information Commissioner, Notifiable Data Breaches Quarterly Statistics Report 1 October - 31 December 2018. Available from: <https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics/notifiable-data-breaches-quarterly-statistics-report-1-october-31-december-2018.pdf>
- 5 Privacy and security of digital health. [Internet]. Available from: <https://www.digitalhealth.gov.au/using-the-my-health-record-system/maintaining-digital-health-in-your-practice/privacy-and-security-for-digital-health>
- 6 Office of the Australian Information Commissioner Notifiable Data Breaches Scheme. [Internet]. Available from: <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme>
- 7 Guide to mandatory data breach notification in the My Health Record system. [Internet]. Available from: <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-mandatory-data-breach-notification-in-the-my-health-record-system>

**Publication date:** February 2019 - second edition.

### Contact for enquiries

**Telephone:** 1300 901 001 or **email:** [help@digitalhealth.gov.au](mailto:help@digitalhealth.gov.au)

### Disclaimer

The Australian Digital Health Agency (“the Agency”) makes the information and other material (“Information”) in this document available in good faith but without any representation or warranty as to its accuracy or completeness. The Agency cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

### Document control

This document is maintained in electronic form and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

### Copyright © 2019 Australian Digital Health Agency

This document contains information which is protected by copyright. All Rights Reserved. No part of this work may be reproduced or used in any form or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems – without the permission of the Australian Digital Health Agency. All copies of this document must include the copyright and other information contained on this page.

### Acknowledgements

#### Council of Australian Governments

The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.



**Australian Government**

**Australian Digital Health Agency**

[digitalhealth.gov.au](https://digitalhealth.gov.au)