[High Priority] - H0616 :   [COVID-19] The Transfer of Loaned Equipment during the COVID-19 Response Could Lead to Breach of Sensitive Information [ECRI Exclusive Hazard Report]
Medical Device Hazard Report

Published: Thursday, May 21, 2020

Geographic Regions: Worldwide

Suggested Distribution: Clinical/Biomedical Engineering, Risk Management/Continuous Quality Improvement, Information Technology

Problem:

1. Devices may contain sensitive information, including e-PHI from previous use.
    1. Disclosure of e-PHI to unauthorized entities could constitute a HIPAA violation.
    2. Disclosed credentials or network configurations could be used as intelligence in targeted hacking attacks.

ECRI Recommendations:

1. When returning or loaning devices to other facilities, remove sensitive information.
    1. Sensitive information could include:
        1. E-PHI
        2. Network configuration
        3. Credentials or digital certificates
    2. Refer to service manuals for specific procedures.
    3. Coordinate policies for custody or replacement of any removable media (e.g., USB drive, SD card) that contain sensitive information with the other party.
    4. Follow established decommissioning procedures.
2. When borrowing or receiving devices from other facilities, check devices for sensitive information before releasing them to clinical use.
3. If you discover a device containing sensitive information:
    1. Notify the originating institution/facility if any sensitive information is identified upon receipt of the equipment.
    2. Organize removal of the sensitive information before releasing it to clinical use.

Background:

1. While responding to COVID-19-related surges, facilities may transfer devices from alternative sources, including:
    1. Government entities
    2. Outside facilities (loaned)
2. Devices used in a healthcare setting could contain sensitive information, including:
    1. E-PHI
    2. Network configuration or credentials
3. Facilities should ensure that sensitive information contained on the devices, including e-PHI, is not exposed:
    1. To the receiving facility
    2. To any third party involved in the transfer
    3. If a device is lost or stolen

Comments:

- This alert is a living document and may be updated when ECRI receives additional information.

Source(s):

- 2020 May 21. ECRI researched report