Infection Control & Hospital Epidemiology (2022), **43**, 1275–1310
doi:10.1017/ice.2021.235

Letter to the Editor

Antimicrobial stewardship during a cyberattack

Lindsay M. Smith MD[1,2] and John W. Ahern PharmD[2,3]

[1]Infectious Diseases Division, University of Vermont Medical Center, Burlington, Vermont, [2]University of Vermont Larner College of Medicine, Burlington, Vermont and [3]Department of Pharmacy, University of Vermont Medical Center, Burlington, Vermont

To the Editor—On October 28, 2020, the University of Vermont Medical Center (UVMMC), a 500-bed academic medical center serving Vermont and upstate New York, was hit by the largest cyberattack against a US hospital in 2020, resulting in a complete shutdown of the internet, electronic medical record (EHR), and e-mail for 26 days.[1] When it became clear that the EHR and internet would not be readily restored, we quickly realized that our antimicrobial stewardship program (ASP) would need to change with this difficult time. Here, we describe our experience maintaining and modifying an antimicrobial stewardship program without 21st-century technology.

The daily activities of the UVMMC ASP rely on 4 main components: (1) prior authorization with a restricted formulary, (2) real-time review of patients with bacteremia, (3) real-time review of all admitted patients receiving antimicrobials, and (4) retrospective review based on indication of use at time of ordering. At UVMMC, the antimicrobial formulary is categorized into open antimicrobials, criteria-based antimicrobials, controlled antimicrobials (requiring prior authorization), and restricted antimicrobials (requiring prior authorization and infectious diseases consultation). We elected to suspend the prior authorization system due to the lack of reliable paging and communication between clinicians, fearing a delay in initiation of appropriate therapy. Antimicrobial surveillance was limited to manual review of intravenous preparations that were prepared in the pharmacy sterile-products area. To prevent unrecognized lapses in treatment, we suspended duration of treatment requirements for anti-infective orders given the unavailability of electronic reminders. A cornerstone of our program is performing at least daily review of all patients who are bacteremic and all patients who are receiving antimicrobials for real-time evaluation. With the loss of the EHR, it was not possible to perform either of these reviews in real time. During the cyberattack, we went to the microbiology laboratory every morning and directly discussed all newly positive blood cultures with the microbiology technicians. Even with direct communication, it was difficult to determine the number of positive bottles and tracking the bottles from the Gram stain to organism identification. When newly bacteremic patients were identified, this information was directly relayed to the primary team in person by the ASP team, in addition to the microbiology laboratory protocols.

With the loss of the internet and EHR, all laboratory results were delayed. Results were faxed to floors with functioning fax capability or were hand delivered. Due to the time delay, it became challenging to align vancomycin trough concentrations and timing of infusions. In addition, pharmacy pharmacokinetic dosing applications were not available. For safety, we decided to change empiric treatment for gram-positive organisms to daptomycin or ceftaroline. This required prompt coordination with pharmacy purchasers as neither are stocked in large supply at UVMMC. We had to rely on "word of mouth" to notify clinicians to only prescribe vancomycin if absolutely necessary. This notification was best done by utilizing the emergency department pharmacists to prevent vancomycin starts at the time of admission. All infectious diseases physicians and fellows were notified of the safety issue and changed all consultation patients receiving vancomycin to daptomycin or ceftaroline.

Now that our EHR and internet are restored, we are left with a data gap. We are unable to back fill the microbiology data leaving our antibiogram without data. Additionally, the paper medication administration record cannot be transcribed into the EHR; therefore, we cannot submit our antimicrobial usage data to the NHSN for this period.

We know that UVMMC was not the only hospital to suffer a cyberattack in 2020, and unfortunately, we will likely not be the last. We were not prepared for the loss of the internet and EHR, and we hope that by sharing our experience we can help others. Based on our experience, we recommend the following for an antimicrobial stewardship emergency preparedness plan:

1. Be prepared to minimize the use of antimicrobials that require dose adjustment via serum concentrations, such as vancomycin and aminoglycosides. This may require the increased use of alternative antimicrobials.
2. Review handwritten paper medication administration records carefully to ensure that patients are receiving antimicrobials as intended.
3. Designate a point person to liaise with the microbiology laboratory to track bacteremic patients.
4. Design paper flow sheets for complex patients to track laboratory and culture results and medications in real time.
5. Consider paper admission orders with sections for hospital approved antibiotics for common infectious syndromes.

Acknowledgments.

Financial support. No financial support was provided relevant to this article.

Conflicts of interest. All authors report no conflicts of interest relevant to this article.

Reference

1. The 5 most significant cyberattacks in healthcare for 2020. Becker's Health IT website. https://www.beckershospitalreview.com/cybersecurity/the-5-most-significant-cyberattacks-in-healthcare-for-2020.html. Published December 14, 2020. Accessed May 5, 2021.

Author for correspondence: Lindsay M. Smith, E-mail: Lindsay.Smith@uvmhealth.org

Cite this article: Smith LM and Ahern JW. (2022). Antimicrobial stewardship during a cyberattack. *Infection Control & Hospital Epidemiology*, 43: 1275, https://doi.org/10.1017/ice.2021.235