Corrigenda and Addenda

Correction: Unveiling Patient-Level Harms and At-Risk Clinical Groups During Hospital Cyberattacks: Systematic Review of Global Case Studies and Social Media Data

Isabel Straw[1], MPH, MD, PhD; Deepak Kumar[1], PhD; Seoyoung Kweon[1], MSc; Jordan Selzer[2], MD; Christian Dameff[3], MD; Jeffrey Tully[4], MD

[1]Department of Computer Science and Engineering, University of California San Diego, San Diego, CA, United States
[2]Department of Emergency Medicine, George Washington University, Washington, DC, United States
[3]Department of Emergency Medicine, University of California San Diego, San Diego, CA, United States
[4]Department of Anesthesia, University of California San Diego, San Diego, CA, United States

Corresponding Author:

Isabel Straw, MPH, MD, PhD
Department of Computer Science and Engineering
University of California San Diego
9500 Gilman Dr
San Diego, CA 92093
United States
Phone: 1 858-534-2230
Email: isabelstraw@doctors.org.uk

Related Article:
Correction of: https://www.jmir.org/2026/1/e88257

J Med Internet Res 2026;28:e114623; doi: 10.2196/114623

In "Unveiling Patient-Level Harms and At-Risk Clinical Groups During Hospital Cyberattacks: Systematic Review of Global Case Studies and Social Media Data" [1], the authors noted one error.

The file previously attached as Multimedia Appendix 4 was a duplicate of Multimedia Appendix 5. This has been replaced with the proper file (included here as Multimedia Appendix 1).

The correction will appear in the online version of the paper on the JMIR Publications website together with the publication of this correction notice. Because this was made after submission to PubMed, PubMed Central, and other full-text repositories, the corrected article has also been resubmitted to those repositories.

Multimedia Appendix 1

Corrected file for Multimedia Appendix 4: Extracts from the full Cyberattack Impacts, Patient Harms, and Emergency Response (CIPHER) database with examples of identified patient-level harms from the academic literature (column 1) and the social media data (column 2), categorized by clinical domains (numbered as Sections for reference throughout the text). Quotes are provided from the authors of the academic paper alongside the respective reference, or from the social media post alongside the respective subreddit. Social media data posts are deidentified (references to usernames are removed) and any personal details or reference to specific providers/vendors are replaced with asterisks; quotes are numbered (eg. Q1.1) for reference throughout the text.
[DOCX File (Microsoft Word File), 3342 KB-Multimedia Appendix 1]

References

1. Straw I, Kumar D, Kweon S, Selzer J, Dameff C, Tully J. Unveiling patient-level harms and at-risk clinical groups during hospital cyberattacks: systematic review of global case studies and social media data. J Med Internet Res. Sep 28, 2026;28:e88257. [doi: 10.2196/88257] [Medline: 42809354]

This is a non–peer-reviewed article; submitted 16.Oct.2026; accepted 16.Oct.2026; published 04.Nov.2026

Please cite as:
Straw I, Kumar D, Kweon S, Selzer J, Dameff C, Tully J
Correction: Unveiling Patient-Level Harms and At-Risk Clinical Groups During Hospital Cyberattacks: Systematic Review of Global Case Studies and Social Media Data
J Med Internet Res 2026;28:e114623
URL: https://www.jmir.org/2026/1/e114623
doi: 10.2196/114623

© Isabel Straw, Deepak Kumar, Seoyoung Kweon, Jordan Selzer, Christian Dameff, Jeffrey Tully. Originally published in the Journal of Medical Internet Research (https://www.jmir.org), 04.Nov.2026. This is an open-access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work, first published in the Journal of Medical Internet Research (ISSN 1438-8871), is properly cited. The complete bibliographic information, a link to the original publication on https://www.jmir.org/, as well as this copyright and license information must be included.