



OPEN
COMMENT

Extending the CARE Principles: managing data for vulnerable communities in wartime and humanitarian crises

Yana Suchikova¹ & Serhii Nazarovets²

The CARE Principles (Collective Benefit, Authority to Control, Responsibility, Ethics) were developed to ensure ethical stewardship of Indigenous data. However, their adaptability makes them an ideal framework for managing data related to vulnerable populations affected by armed conflicts. This essay explores the application of CARE principles to wartime contexts, with a particular focus on internally displaced persons (IDPs) and civilians living under occupation. These groups face significant risks of data misuse, ranging from privacy violations to targeted repression. By adapting CARE, data governance can prioritize safety, dignity, and empowerment while ensuring that data serves the collective welfare of affected communities. Drawing on examples from Indigenous data governance, open science initiatives, and wartime humanitarian challenges, this essay argues for extending CARE principles beyond their original scope. Such an adaptation highlights CARE's potential as a universal standard for addressing the ethical complexities of data management in humanitarian crises and conflict-affected environments.

Introduction

The CARE Principles (Collective Benefit, Authority to Control, Responsibility, Ethics) have emerged as a cornerstone for ethically managing data related to Indigenous peoples¹. Designed to complement the technical standards of FAIR (Findable, Accessible, Interoperable, Reusable), CARE emphasizes the cultural, ethical, and social dimensions of data stewardship. These principles ensure that data governance prioritizes community well-being, respects local values, and protects the rights of vulnerable groups. While initially focused on Indigenous data, CARE's ethical imperatives can – and should – be extended to other vulnerable communities. This comment explores how the CARE Principles can be applied to data governance in conflict-affected environments, ensuring ethical stewardship of sensitive information for vulnerable populations. While the discussion is framed through the lens of the Russo-Ukrainian war – focusing on internally displaced persons (IDPs) and civilians in occupied territories – the insights presented here have broader implications for humanitarian data management in other war-affected regions. By doing so, CARE can offer a unified ethical framework for addressing the challenges of data governance in complex humanitarian contexts.

Existing approaches to data governance, such as the FAIR principles, emphasize findability, accessibility, interoperability, and reusability to enhance data sharing and reproducibility. However, these principles, as outlined in recent studies², often require extensive curatorial efforts and may not fully address ethical concerns in conflict-affected areas. The Guidelines for Research Data Integrity (GRDI)³ further highlight the risks of data misinterpretation and the necessity of maintaining accuracy and transparency. Yet, neither FAIR nor GRDI explicitly account for the agency and rights of vulnerable populations over their data. This gap underscores the relevance of the CARE principles, which prioritize collective benefit, authority to control, responsibility, and ethics in data governance⁴. By integrating CARE principles into existing frameworks, humanitarian organizations can ensure that data governance aligns with both ethical and practical considerations in high-risk contexts.

¹Berdiansk State Pedagogical University, 71100, Zaporizhzhia, Ukraine. ²Borys Grinchenko Kyiv Metropolitan University, 04053, Kyiv, Ukraine. e-mail: yanasuchikova@gmail.com; s.nazarovets@kubg.edu.ua

The vulnerabilities of war-affected populations. The Russo-Ukrainian war has displaced millions, creating one of the largest displacement crises in Europe since World War II. Simultaneously, many individuals remain in occupied territories under precarious conditions. Both groups face heightened vulnerabilities linked to the collection and misuse of their data. For IDPs, the collection of personal information to coordinate humanitarian aid often results in privacy risks, ranging from data breaches to unauthorized use for non-humanitarian purposes⁵.

For those in occupied territories, data misuse can result in repression or violence, especially if sensitive information falls into the hands of occupying authorities⁶. A striking example is the use of digital records during so-called 'filtration procedures,' where occupying forces systematically verify individuals' online activity, employment records, and prior affiliations to identify individuals deemed disloyal or politically undesirable. Reports from human rights organizations and independent investigators have documented cases where accessing certain digital content or having past government ties has led to arbitrary detentions and forced disappearances⁷.

Therefore, managing such sensitive data requires stringent ethical safeguards. Recent research highlights the importance of anonymizing participants in conflict-affected regions and mandating the destruction of sensitive information post-project to prevent harm⁸. This approach reflects a growing recognition of the critical intersection between data ethics and human security in conflict zones.

Adapting CARE to new contexts. The principles of CARE provide a flexible yet comprehensive ethical foundation that can be adapted to diverse contexts. Its emphasis on collective benefit ensures that data governance serves the well-being of communities, while authority to control empowers affected populations to govern their own data. Responsibility demands accountability from data stewards, and ethics ensures that data practices uphold the highest moral standards. These principles align closely with the needs of war-affected populations and can address critical gaps in existing data management practices.

Collective benefit. The principle of collective benefit ensures that data collection and use actively contribute to community well-being. For IDPs and residents of occupied territories, this could mean leveraging data to improve humanitarian assistance, facilitate family reunifications, and support long-term recovery efforts. Lessons from projects like FAIR Island demonstrate how aligning data governance with community-defined goals can amplify its social impact⁹. Similarly, applying CARE in the Russo-Ukrainian context ensures that the primary focus of data use is the welfare of affected populations, not external interests.

A poignant example of the potential collective benefit is the documentation of forcibly deported Ukrainian children. A recent report by the Humanitarian Research Lab identifies 314 children illegally transferred to Russia¹⁰, where they were subjected to forced re-education and naturalization, often separated from siblings and stripped of their Ukrainian identity. Such documentation is crucial for reuniting families, bringing these children back to Ukraine, and ensuring that these war crimes are meticulously recorded for international accountability. Ethically and securely collected data can serve as a powerful tool in exposing these atrocities. By integrating CARE principles into data governance, humanitarian organizations and researchers can ensure that collected data not only protects vulnerable populations, but also actively contributes to their empowerment and restitution.

Authority to control. This principle addresses the critical issue of data sovereignty. For Indigenous communities, CARE has empowered them to reclaim control over data historically misused by external entities¹¹. In the context of war, authority to control ensures that IDPs and those in occupied territories maintain autonomy over their personal information.

A compelling example of this principle in practice can be seen in how Ukrainian universities displaced due to occupation manage their online presence¹². To safeguard the identities of faculty members who remain in occupied territories but continue teaching online, Ukrainian universities have deliberately hidden their personal profiles from public access¹³. Similarly, class schedules are withheld from public access to prevent sensitive operational details from being exploited. These measures highlight the importance of secure, community-controlled access to sensitive data, ensuring that the safety and autonomy of individuals are prioritized in crisis conditions.

Digital tools that enable such protections, akin to innovations like TK Labels for Indigenous knowledge¹⁴, are vital in war contexts. By embedding the principle of authority to control into data governance, organizations can uphold the rights of vulnerable populations and safeguard them from potential harm, ensuring that data serves their interests rather than becoming a tool for persecutions.

Responsibility. Responsibility in data governance demands accountability and transparency from those collecting, managing, and using data. This is especially important in contexts of war, where mistrust of institutions is widespread. By adopting CARE, organizations managing data in the Russo-Ukrainian context would be compelled to minimize harm, ensure informed consent, and foster trust with affected communities. As Belarde-Lewis *et al.*¹⁴ highlight, responsibility includes building relationships with communities and ensuring that data practices align with their cultural and ethical values.

Responsibility in data governance must extend beyond the technical process of collection to actively fostering trust and ensuring inclusivity, particularly in regions impacted by war. As highlighted by Popova *et al.*¹⁵, universities in Ukraine are implementing policies and strategies aimed at encouraging young people to return and participate in rebuilding their communities. These efforts emphasize a holistic approach to trust-building and reintegration, focusing on documenting local needs and aspirations while fostering unity among displaced populations. By doing so, universities shape data policies that transcend mere information collection, promoting collective action and community resilience.

Applying this framework within the context of the Russo-Ukrainian war through the lens of the CARE Principles demonstrates how responsibility in data governance can be a catalyst for reconstructing societal structures and empowering affected communities. Universities play a crucial role in this process by managing a range of data, including student enrolment records, research archives, and institutional collaborations. These datasets support post-war recovery by facilitating the reintegration of displaced scholars, tracking educational disruptions, and preserving intellectual heritage amid conflict. For instance, academic records help internally displaced students resume their studies without bureaucratic obstacles, while research databases contribute to understanding long-term societal impacts of the war¹².

Ethics. The ethical dimension of CARE emphasizes the paramount importance of safeguarding the safety and dignity of individuals. In war zones, this principle becomes indispensable. Mishandling sensitive data can expose vulnerable populations to significant risks, such as targeted violence or stigmatization¹⁶. The application of CARE ensures that data governance upholds rigorous ethical standards, actively protecting individuals from harm.

Wartime conditions give rise to new vulnerable groups¹⁷, including those forcibly separated from their families, individuals unable to evacuate conflict zones, and people with disabilities who face heightened challenges in accessing aid and resources. These groups require particular attention to ensure their inclusion and protection in data practices. Ethical data governance must address these complexities by developing strategies to ensure that the unique needs of all vulnerable populations are met while mitigating harm. By adhering to CARE principles, institutions can ethically navigate these challenges, ensuring that their data practices prioritize both immediate security and long-term recovery for these at-risk groups.

Recent developments in data stewardship have acknowledged the challenges of implementing FAIR principles in practice, particularly in complex, interdisciplinary environments. A study by Fraga-González *et al.*² introduced a pragmatic “FAIR enough” approach, suggesting that incremental adoption of FAIR principles is more feasible than rigid adherence. While this model provides flexibility, it does not directly address ethical concerns regarding data sovereignty and potential risks associated with misuse of sensitive datasets. In occupied cities, open data initiatives must be carefully assessed against potential risks, as seemingly neutral datasets – such as economic indicators or migration statistics – can be repurposed for surveillance and repression. This reinforces the argument that CARE principles are essential in complementing FAIR, ensuring that ethical accountability is central to data governance¹⁸. As Plastun and Kozmenko¹⁹ highlight, the misrepresentation of stolen Ukrainian universities as Russian entities in international academic databases is not merely a technical oversight but a serious ethical failure. This erroneous attribution legitimizes the occupation, distorts the academic landscape, and allows occupying authorities to falsely claim the intellectual and institutional achievements of Ukrainian academia as their own. This is particularly critical in conflict settings, where data about internally displaced persons or vulnerable communities may be repurposed for non-humanitarian aims. In this regard, the CARE principles serve as a necessary complement to FAIR by ensuring that data governance prioritizes ethical accountability and community oversight.

Broadening CARE’s relevance and implications for global data governance. Some may contend that the CARE Principles, rooted in Indigenous contexts, are less applicable to other vulnerable groups. However, their adaptability has already been demonstrated across a variety of settings, from localized data stewardship projects to open science initiatives^{9,20}. Extending CARE to war-affected populations does not compromise their original intent; rather, it underscores their universality and relevance as a robust ethical framework.

The need to broaden the application of CARE is particularly pressing given the challenges posed by the global data economy. As conflicts and displacements become more frequent, vulnerable populations are often at risk of exploitation by systems that prioritize efficiency over ethics. For instance, in Ukraine, the drive to publish FAIR datasets – critical for transparency and scientific progress – can unintentionally expose individuals to harm if ethical considerations are overlooked. CARE ensures that data contributes to scientific advancements responsibly, balancing openness with the protection of human rights and the welfare of communities.

In Ukraine, initiatives like the 2022 Open Science Plan aim to increase transparency and competitiveness in research²¹. Metrics such as the number of FAIR datasets published have been integrated into national evaluation criteria for research institutions. While these goals reflect progress, they must be tempered by the ethical demands of wartime realities. Data concerning displaced populations, occupied territories, or sensitive areas of research should not simply adhere to standards of openness, but must also be governed with care to avoid unintended harm. CARE principles provide this crucial safeguard, ensuring a balanced approach that retains the benefits of FAIR while mitigating the risks of uncritical data sharing. It is important to note that FAIR does not inherently imply openness; rather, it promotes well-structured and machine-readable data that can be accessed under clearly defined conditions. Sensitive datasets, particularly in humanitarian contexts, can adhere to FAIR principles while remaining restricted to authorized stakeholders to prevent misuse²².

The global significance of CARE lies in its capacity to establish a standardized ethical framework for data governance across a wide range of contexts. Vulnerabilities are not limited to Indigenous populations or those affected by war; they also encompass marginalized communities, climate refugees, and individuals whose sensitive data is at risk of exploitation in sectors such as health, migration, and education. Adopting CARE globally would provide a unified ethical foundation that complements FAIR, ensuring that data governance prioritizes humanity’s collective welfare. From mitigating biases in artificial intelligence to ensuring equitable access to digital resources, CARE principles offer a universal approach for embedding ethics into the rapidly evolving data-driven landscape.

Applying CARE to populations affected by war demonstrates its ability to address systemic vulnerabilities heightened by displacement, conflict, and the misuse of data. In such scenarios, CARE ensures that data

Principle/Framework	Main focus	Key strengths	Limitations in conflict contexts
FAIR	Findability, accessibility, interoperability, reusability	Facilitates scientific reproducibility and machine-readability	Lacks ethical and community-driven oversight
CARE	Collective benefit, authority to control, responsibility, ethics	Emphasizes ethical data use and community governance	Requires institutional commitment for implementation
ICRC rules (2019) & Handbook (2024)	Humanitarian data protection	Strict safeguards against data misuse in humanitarian operations; practical guidelines for handling biometric and cloud-stored data	Limited applicability outside humanitarian agencies
UN Privacy Principles (2018)	Data minimization, informed consent, purpose limitation	Provides a broad ethical framework for personal data governance	Lack of enforcement mechanisms in conflict zones
IHL (Buchan & Lubin, 2022; Kelemen, 2024)	Legal protections for data in armed conflicts	Addresses military misuse of personal data	Unclear legal status of digital data

Table 1. Comparative analysis of CARE, FAIR, and international humanitarian data standards in conflict-affected contexts.

governance is not solely about technical efficiency but also centres in justice, equity, and the empowerment of communities^{14,23}.

The integration of FAIR and CARE principles provides a global standard that harmonizes openness with ethical responsibility, setting a transformative model for tackling future challenges. By embedding CARE into global data governance structures, we can build systems that not only protect and empower vulnerable populations but also uphold the ethical obligations of the scientific and data management communities.

Comparative analysis of CARE, FAIR, and international humanitarian data standards. The ethical and legal landscape of data governance in humanitarian contexts is shaped by multiple frameworks, including the FAIR principles, the CARE principles, and international humanitarian data protection standards established by the International Committee of the Red Cross (ICRC) and the United Nations (UN). While each of these frameworks offers valuable guidelines, they exhibit significant differences in scope, objectives, and applicability to conflict-affected populations or humanitarian crises.

FAIR principles focus on the technical and infrastructural aspects of data reusability, ensuring that datasets are structured for long-term scientific utility²². However, they do not inherently provide guidance on ethical considerations or community control over sensitive data. Recent critiques² highlight that FAIR implementation often entails substantial financial and administrative burdens, which may be impractical in humanitarian crises. Moreover, the Guidelines for Research Data Integrity³ emphasize the risks of data misinterpretation and advocate for strict methodological controls, yet they do not address power dynamics in data governance or the agency of vulnerable populations over their information.

In contrast, the CARE principles emphasize ethical imperatives, advocating for the collective benefit of data use and the prioritization of the rights of affected communities⁴. This aligns with the ICRC’s approach to personal data protection, which underscores the need for strict limitations on data collection and use in humanitarian operations²⁴. Additionally, the ICRC’s *Handbook on data protection in humanitarian action*²⁵ provides practical guidance on implementing data protection measures in crisis settings, particularly in relation to biometric data, cloud storage, and cross-border data transfers. The handbook highlights the risks of unauthorized access and repurposing of humanitarian data, reinforcing the necessity of ethical oversight mechanisms, such as those proposed under the CARE framework. Similarly, the UN *Personal Data Protection and Privacy Principles*²⁶ emphasize the importance of data minimization, informed consent, and purpose limitation, ensuring that personal data is not repurposed in ways that could harm vulnerable populations.

Legal analyses further demonstrate gaps in current frameworks. Kelemen²⁷ highlights the absence of explicit protections for digital data in international humanitarian law (IHL), noting that electronic records do not enjoy the same safeguards as physical objects. This legal ambiguity is particularly concerning given the increasing militarization of digital data²⁸, where biometric databases and online records can become strategic assets in armed conflicts. Such concerns reinforce the argument that the FAIR framework alone is insufficient in conflict scenarios, and that the ethical and community-driven perspectives of CARE must be integrated into data governance protocols. A structured comparison of these frameworks is presented in Table 1, illustrating their key attributes and areas of overlap.

Conclusion

The CARE Principles provide a robust and adaptable framework for ethical data governance, emphasizing the rights and welfare of vulnerable populations. Their application to communities impacted by the Russo-Ukrainian war highlights their broader relevance and potential as a universal ethical standard. By incorporating CARE, data practices can avoid causing harm and instead serve as tools for fostering resilience, supporting recovery, and advancing justice. This approach honours the dignity of war-affected populations and sets a transformative precedent for managing data in a world increasingly shaped by interconnected crises and conflicts.

This analysis underscores the necessity of integrating ethical and community-driven frameworks, such as CARE, into existing humanitarian and scientific data governance models. While FAIR principles remain fundamental for ensuring data usability, their limitations in conflict settings highlight the importance of complementary frameworks that prioritize accountability and affected populations’ rights. By advocating for explicit recognition of CARE within international humanitarian data policies – including ICRC and UN guidelines – this study contributes to the ongoing discourse on responsible data stewardship in crisis contexts.

In light of these insights, we urge researchers, policymakers, and organizations to actively engage in a dialogue about integrating CARE principles into their data governance frameworks. Such adoption will not only advance scientific progress but also ensure that data management prioritizes the dignity, security, and empowerment of vulnerable communities around the globe. By embedding CARE into global practices, we can build a foundation for ethical and equitable data governance in a rapidly changing world.

Received: 18 December 2024; Accepted: 4 March 2025;

Published online: 11 March 2025

References

1. Carroll, S. R. *et al.* Using Indigenous standards to implement the CARE principles: setting expectations through tribal research codes. *Front. Genet.* **13**, 1–10, <https://doi.org/10.3389/fgene.2022.823309> (2022).
2. Fraga-González, G. *et al.* Affording reusable data: recommendations for researchers from a data-intensive project. *Sci. Data* **12**, 258, <https://doi.org/10.1038/s41597-025-04565-0> (2025).
3. Miller, G. & Spiegel, E. Guidelines for research data integrity (GRDI). *Sci. Data* **12**, 95, <https://doi.org/10.1038/s41597-024-04312-x> (2025).
4. Global Indigenous Data Alliance. CARE principles for Indigenous data governance. *GIDA* <https://www.gida-global.org/care> (2019).
5. Tsybuliak, N. *et al.* In a stranger's house: social isolation of internally displaced people in Ukraine during wartime. *Hum. Aff.* <https://doi.org/10.1515/humaff-2024-0027> (2024).
6. Bukrieva, I. & Afanasieva, L. The Russian occupation of Melitopol, Ukraine. *J. Dev. Soc.* **39**, 236–252, <https://doi.org/10.1177/0169796X231168151> (2023).
7. Office of the United Nations High Commissioner for Human Rights. Report on the human rights situation in Ukraine, 1 September – 30 November 2024. *United Nations* <https://ukraine.ohchr.org/en/> (2024).
8. Tsybuliak, N. *et al.* Ukrainian universities at the time of war: from occupation to temporary relocation. *Torture J.* **33**, 39–64, <https://doi.org/10.7146/torture.v33i3.136256> (2023).
9. Robinson, E. *et al.* FAIR Island: real-world examples of place-based open science. *GigaScience* **12**, 1–5, <https://doi.org/10.1093/gigascience/giad004> (2023).
10. Raymond, N. A. *et al.* Russia's systematic program of coerced adoption and fostering of Ukraine's children. *Humanitarian Research Lab at Yale School of Public Health* Available at https://www.justsecurity.org/wp-content/uploads/2024/12/Russias_Systematic_Program_of_Coerced_Adoption_and_Fostering_of_Ukraines_Children.pdf (2024).
11. Carroll, S. R. *et al.* The CARE principles for Indigenous data governance. *Data Sci. J.* **19**, 1–12, <https://doi.org/10.5334/dsj-2020-043> (2020).
12. Lopatina, H. *et al.* University without walls: experience of Berdyansk State Pedagogical University during the war. *Probl. Perspect. Manag.* **21**, 4–14, [https://doi.org/10.21511/ppm.21\(2-si\).2023.02](https://doi.org/10.21511/ppm.21(2-si).2023.02) (2023).
13. Suchikova, Y. *et al.* Is science possible under occupation? Reflection and coping strategy. *Corp. Gov. Organ. Behav. Rev.* **7**, 314–324, <https://doi.org/10.22495/cgobrv7i2sip10> (2023).
14. Belarde-Lewis, M. *et al.* Centering relationality and CARE for stewardship of Indigenous research data. *Data Sci. J.* **23**, 1–16, <https://doi.org/10.5334/dsj-2024-032> (2024).
15. Popova, A. *et al.* I (don't) want to go home. Will young people return to the de-occupied territories of Ukraine? *Heliyon* **10**, e35230, <https://doi.org/10.1016/j.heliyon.2024.e35230> (2024).
16. Tsybuliak, N. *et al.* Mobilization and stigmatization: PhD admissions in wartime. *High. Educ. Res. Dev.* <https://doi.org/10.1080/07294360.2024.2424161> (2024).
17. Tsybuliak, N. *et al.* Inclusion in Ukrainian universities from an inside perspective. *Sci. Rep.* **14**, <https://doi.org/10.1038/s41598-024-69084-1> (2024).
18. Suchikova, Y. Invisible lives: occupied cities as a blind spot in geopolitical research. *Geopolit. Glob.* **5**, 35–45, [https://doi.org/10.21511/gg.05\(1\).2024.03](https://doi.org/10.21511/gg.05(1).2024.03) (2025).
19. Plastun, A. & Kozmenko, S. Stolen Ukrainian universities: an invisible Russian weapon. *Probl. Perspect. Manag.* **23**, 151–175, [https://doi.org/10.21511/ppm.23\(2-si\).2025.11](https://doi.org/10.21511/ppm.23(2-si).2025.11) (2025).
20. Carroll, S. R. *et al.* Operationalizing the CARE and FAIR principles for Indigenous data futures. *Sci. Data* **8**, 108, <https://doi.org/10.1038/s41597-021-00892-0> (2021).
21. Nazarovets, S. Ukraine approves National Plan for Open Science. *Nature* **611**, 236, <https://doi.org/10.1038/d41586-022-03583-x> (2022).
22. Wilkinson, M. *et al.* The FAIR Guiding Principles for scientific data management and stewardship. *Sci Data* **3**, 160018, <https://doi.org/10.1038/sdata.2016.18> (2016).
23. Cummins, J. *et al.* Enhancing stewardship of Indigenous Peoples' data, information, and knowledges in libraries and archives through Indigenous data governance. *Libr. Trends* **72**, 13–47, <https://doi.org/10.1353/lib.2023.a938211> (2023).
24. International Committee of the Red Cross. ICRC rules on personal data protection. *ICRC* <https://shop.icrc.org/icrc-rules-on-personal-data-protection-pdf-en.html> (2019).
25. International Committee of the Red Cross. Handbook on data protection in humanitarian action. *ICRC* <https://www.icrc.org/en/data-protection-humanitarian-action-handbook> (2024).
26. United Nations System Chief Executives Board for Coordination. United Nations personal data protection and privacy principles. *UN* <https://unsceb.org/personal-data-protection-and-privacy-principles> (2018).
27. Kelemen, B. K. Protection of (personal) data in armed conflicts. *Baltic J. Law Polit.* **17**, 1–20, <https://doi.org/10.2478/bjlp-2024-0001> (2024).
28. Buchan, R. & Lubin, A. The rights to privacy and data protection in times of armed conflict. *NATO CCDCOE Publications*. ISBN: 978-9916-9565-7-1 (2022).

Acknowledgements

The authors would like to thank all Ukrainian defenders for the possibility to finalize and publish this work. The authors are also grateful to the editor and the anonymous reviewers for their thoughtful feedback and valuable suggestions, which significantly improved the clarity and depth of this manuscript. In particular, the authors appreciate the detailed recommendations from one of the reviewers, which greatly contributed to strengthening the discussion on international humanitarian data governance.

Author contributions

The authors contributed equally to the conceptual design, literature review, writing, and editing.

Competing interests

One of the authors (YS) is an internally displaced person as a result of the Russo-Ukrainian war. This personal experience has informed and enriched the perspective of this paper but has not influenced the objectivity or impartiality of the arguments presented.

Additional information

Correspondence and requests for materials should be addressed to Y.S. or S.N.

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

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2025