https://doi.org/10.31925/farmacia.2024.6.1 **REVIEW**

METHODS OF SECURING CHEMICAL AND PHARMACEUTICAL KNOWLEDGE AND RECOMMENDATIONS FOR INTERNATIONAL INSTITUTIONS TO ENHANCE RESEARCH INTEGRITY

YAVANA GANESH [1]*, SAMUEL R. ORTEGA [1], ELLEN M. WYNKOOP [1], AARON R. MELVILLE [1], DOINA DRĂGĂNESCU [2], DENISA IOANA UDEANU [2,3], ANDREEA LETIȚIA ARSENE [2,3], BRUNO ȘTEFAN VELESCU [2], GALINA SATCHANSKA [4]

[1]*Pacific Northwest National Laboratory, Richland, Washington, USA*
[2]*"Carol Davila" University of Medicine and Pharmacy, Faculty of Pharmacy, Bucharest, Romania*
[3]*"Marius Nasta" Institute of Pneumology, Bucharest, Romania*
[4]*New Bulgarian University, Sofia, Bulgaria*

**corresponding author: yavana.ganesh@pnnl.gov*

Manuscript received: October 2024

Abstract

This paper examines strategies for securing chemical and pharmaceutical expertise in a globalised research environment, focusing on safeguarding intellectual property and preventing the misuse of sensitive and potentially dual-use information. The product of collective efforts between Pacific Northwest National Laboratory, "Carol Davila" University of Medicine and Pharmacy and New Bulgarian University, highlights the challenges and opportunities posed by cross-border research collaborations, particularly in the context of differing regulatory frameworks and research cultures. It explores current mechanisms to prevent data loss and unauthorised access to sensitive information while assessing the effectiveness of existing security measures, frameworks and international export control regimes. The approach examines the differing methodologies for promoting transparency, trust-building and mutual accountability in joint research projects to cultivate secure data-sharing practices and intellectual property. It provides recommendations for international institutions to implement security guidelines in framing research priorities, encourages continual training and education programs, and the integration of processes for monitoring research compliance. This partnership aims to advance scientific innovation while maintaining global stability, ensuring compliance with international norms and safeguarding valuable intellectual property as measures in chemical and pharmaceutical research security practices continue to expand due to international collaboration and knowledge exchange.

Rezumat

Studiul analizează strategiile de securizare a expertizei chimice și farmaceutice într-un mediu de cercetare globalizat, concentrându-se pe protejarea proprietății intelectuale, prevenirea utilizării abuzive a informațiilor sensibile și cu potențial de dublă utilizare. Rezultatul colaborării dintre *Pacific Northwest National Laboratory*, Universitatea de Medicină și Farmacie „Carol Davila" din București și Noua Universitate din Bulgaria evidențiază provocările și oportunitățile reprezentate de cercetarea transfrontalieră, în special în contextul unor cadre de reglementare și culturi organizaționale diferite. Au fost identificate mecanismele actuale de prevenire a pierderii de date și a accesului neautorizat la informații sensibile, și a fost evaluată eficacitatea măsurilor de securitate existente, a normativelor internaționale de control al exporturilor. Sunt oferite recomandări pentru instituțiile internaționale privind securitatea actului de cercetare, sunt încurajate programele de formare și educație continue și integrarea proceselor de monitorizare a conformității cercetării. S-a urmărit promovarea activităților de cercetare dezvoltare inovare, punând accent pe respectarea normelor internaționale și protejarea drepturilor de proprietate intelectuală, pe măsură ce practicile de securitate în cercetarea chimică și farmaceutică continuă să se extindă în contextul globalizării.

Keywords: chemical security, research security, intellectual property protection, chemical research integrity

Introduction

Maintaining the integrity of scientific knowledge is paramount to advancements in research, innovation and intellectual property (IP) protection. As research within fields of chemistry drives innovation across the pharmaceutical, healthcare, energy and materials science industries, the risks associated with unauthorised access to sensitive information and facilities, tampering with equipment and knowledge and the misappropriation of dual-use chemical knowledge have intensified [1]. With the convergence of cloud-based technologies and the globalization of research networks, advancements in the field of chemistry can become a double-edged sword, leading to the unintended development of harmful substances, like chemical weapons or illicit drugs. While the drive for technological developments facilitates new and emerging collaborations and data sharing among researchers, this process exposes sensitive

research and IP to the threat of misuse or unauthorised access by groups or individuals with the intent to impose harm [2]. Consequently, academic and research institutions worldwide face the challenge of developing research security guidelines that balance the culture of openness and collaboration with protection measures. As a primary contributor to chemical and pharmaceutical research, academia plays a vital role in developing measures that secure data and ensure the integrity of scientific advancements and innovation. The credibility of academic research is foundational to its impact; thus, safeguarding data against breaches and ensuring the protection of research is imperative.

The Importance of Chemical Research Security

Overview and Importance of Research Security

Research security is critical to scientific research and discovery, including factors such as IP, data integrity, physical assets and material resources. Investing in robust security measures allows international institutions to foster innovation, enhance economic growth and prevent the proliferation of potentially harmful compounds and technologies. By safeguarding research practices, cutting-edge discoveries are appropriately used which mitigates the risk of unauthorised access that could impede progress across fields such as medicine, technology and security. Failure to implement robust security measures renders research vulnerable to exploitation by entities and individuals, posing significant threats to public safety and global stability. This paper delineates the dimensions of research security and advocates for international institutions to integrate core research security and data protection principles into scientific practice to ensure the integrity and sustainability of academic and non-academic research.

Considering these points, addressing robust security measures in academic laboratories and research institutions becomes vital due to the dual-use nature of advanced technologies and chemical compounds. While essential for advancements in industries such as pharmaceuticals, agriculture and materials science, these technologies and chemicals can also be misused for nefarious purposes, including chemical weapons or illicit drug development [3]. The proliferation threat and risks to national and international security of dual-use chemicals and advanced technologies remain high among non-state and state actors seeking to convert these materials into chemical weapons, including the potential for large-scale casualties and environmental damage. By accounting for these threats and the potential implications of chemical weapons development and deployment, research institutions can develop a robust security culture that includes risk management frameworks in compliance with local, national and international regulations.

Through identifying the risks involved in the research lifecycle, distinct motivations are identified that empower these threat factors. While some individuals or groups are motivated by commercial interests, seeking to acquire valuable technology or intellectual property to achieve an economic advantage over competitors, others with more malign intentions may be interested in using stolen information to develop chemical weapons to disrupt national security. These threats carry profound implications for global stability, as the misuse of sensitive information could lead to severe financial losses and enable competitors or adversaries to gain a strategic edge or economic benefit. The consequences may extend beyond immediate economic impact, potentially compromising technological leadership and weakening national resilience against external threats.

Establishing a security structure not only counters proliferation threats but also addresses commercial competitiveness. The access to sensitive information by unauthorised parties poses severe financial, reputational and ethical risks to individual researchers and institutions. To protect IP from theft or illegitimate commercial benefits, comprehensive safeguards should include physical, technical and intangible assets. Without an adequate security framework, the benefits derived from chemical research could be compromised, affecting the economy, future research investments and global competitiveness [4]. In a time of increased threats posed to innovative research, the role of institutions in vetting, safeguarding and implementing robust security measures has amplified. Ensuring the safety, security and integrity of chemical research practices requires a multifaceted and collaborative approach to physical security measures, data security protocols and comprehensive training for laboratory staff and research personnel to secure the integrity of innovation.

International Measures to Secure Research Across the European Union

Methods to secure sensitive knowledge include international research cooperation and global IP arrangements to safeguard research endeavours against the potential threat of unauthorised access or infringement. These mechanisms guide the transfer of sensitive technologies and information, reducing the risks associated with proliferation or misuse. Simultaneously, information-sharing practices aim to counter emerging threats and bolster research security efforts worldwide. From an European Union perspective, initiatives like Horizon Europe prioritize research integrity by underscoring the significance of security best practices [5], while frameworks such as the European Research Area (ERA) foster collaboration and knowledge exchange among member states to address data protection and cybersecurity challenges [6]. Organizations like EECARO guide export-controlled items and technologies for universities to comply with [7]. The following sections provide a high-level overview of programs across the European Union to address research security. University leaders are advised to use these programs as a base-

line to start developing personalised and tailored policies.

Horizon Europe. Horizon Europe, the EU's most prominent funding mechanism for research and innovation, has a budget of 95.5 billion € for 2021 - 2027, making it one of the most substantial public funding programs globally [5]. Horizon Europe seeks to protect a wide range of assets, including cutting-edge research, valuable IP and strategic technology advancements. The program mandates strict adherence to ethical guidelines and data protection regulations including research conduct and mandates compliance with EU and European Economic Area information privacy laws [8]. Horizon Europe aims to enhance transparency and facilitate cooperation among researchers while ensuring the security of proprietary information and innovation within the EU [9].

European Research Area. The European Research Area (ERA) facilitates collaboration among research institutions, businesses and governments, allowing for information sharing in IP management and research security [10]. Through programs like Horizon Europe, the ERA encourages the development of IP protection strategies, provides frameworks for the effective IP management and assists researchers in implementing security measures to protect their research findings. Beyond regulatory standardization and funding, the ERA invests in developing infrastructure and tools for secure information-sharing and collaboration, ensuring that sensitive research data is secured from unauthorised access and cybersecurity threats. By promoting open research practices and emphasizing responsible data management, the ERA balances the benefits of open access with the need to protect sensitive information and IP, creating a supportive environment for innovation and research [10].

European Export Control Association for Research Organisations (EECARO). The European Export Control Association for Research Organisations (EECARO) was developed as a community of practice to enhance compliance with export control regulations among European research institutions. Export controls are regulatory measures that govern the transfer of sensitive technologies, goods and information across national borders, ensuring that these items do not contribute to the proliferation of weapons of mass destruction or fall into the hands of entities or individuals that might pose security threats [7]. Compliance with export control regulations is uniquely complicated for research institutions because fundamental research is often exempt from export controls, while applied research is more likely to be subject to these regulations. By promoting awareness and understanding of export control regulations, EECARO helps research organizations navigate the legal landscape, ensuring that research can proceed without compromising security or breaching regulatory requirements [7].

Using European Union Guidelines to Develop Tailored Policies. Despite international cooperation, illicit transfers of data and knowledge persist, posing threats to research security by exploiting advancements in emerging technology research. Measures set forth by Horizon Europe, the ERA, and EECARO are high-level guidance for universities and research organizations to comply with. Research institutions need to comply with export controls when dealing with controlled dual-use equipment or technologies, however, much of the research conducted is either basic and not controlled or is related to emerging technologies that are not yet subject to controls. Many research institutions may stop at export control compliance, but measures need to also protect research related to uncontrolled dual-use emerging technologies. EECARO sets the baseline for these functions, but universities need to identify specific technologies to protect and develop relevant export control guidance.

The ERA guidelines should be used as a basis for universities to identify specific training needs and areas for assistance. Universities conducting chemical and pharmaceutical research must use these guidelines as a baseline to develop specific and tailored policies that address the needs of their organization. The assets, research and data to protect will vary by institution, hence the importance of creating university-specific protections. Addressing these challenges demands enhanced cooperation to strengthen security practices, streamline information-sharing techniques and establish robust standards for securing research data and innovative technologies.

Overview and Importance of Chemical Security

In recent years, numerous incidents worldwide have underscored the importance of chemical security, highlighting the need for comprehensive strategies and frameworks to secure chemical facilities and research institutions [11]. For context, this paper references the April 2018 Douma, Syrian Arab Republic attacks where the Syrian "Tiger Forces" released two barrels containing toxic chlorine gas over structures in the civilian-inhabited region of Douma, killing over 40 individuals and injuring many more [12]. The operation stands out given its humanitarian implications and broadly recognised prohibitions through the deployment of chlorine gas, a non-scheduled chemical under the Chemical Weapons Convention (CWC). This instance reinforces the need for stringent safeguards for sensitive chemical information to prevent the misuse, unauthorised access or intentional release of chemical agents to maintain public safety, environmental integrity and the sustainment of international stability. In section 3.3 we further discuss case studies illustrating instances surrounding unauthorised access, violations of contractual agreements and IP theft.

Combating these threats involves adherence to international treaties and regulatory frameworks, for example, the CWC, a multilateral treaty prohibiting

the development, production, stockpiling and use of chemical weapons [13]. Beyond the CWC, other supporting bodies also play a crucial role in upholding chemical security. For example, the Globally Harmonised System of Classification and Labelling of Chemicals (GHS) standardizes the classification and labelling of chemicals to improve transportation safety and facilitate international trade [14]. Additionally, the EU's Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) regulation requires companies to identify and manage the risks linked to the chemicals they manufacture and market in the EU [15]. REACH also applies to chemicals imported or manufactured within Great Britain, known as UK REACH. These safety-focused measures, while not developed from a security perspective, ensure a comprehensive approach to chemical security, addressing various aspects of chemical production, use and disposal [15].

How does protecting research strengthen chemical security?

The convergence of chemical security and research integrity represents a critical step in protecting the international community from the misuse of dual-use chemical compounds and laboratory technology while also upholding the values of scientific innovation [16]. Ensuring the secure handling, storage and dissemination of chemical research is paramount to prevent the misuse or release of materials that could potentially cause harm. Consequently, strategies to bolster chemical security increasingly intertwine with efforts to safeguard research integrity and protect against IP infringement. The following section highlights different programs and standards within the United States and abroad to enhance security efforts through mitigation strategies and strategic partnerships.

In the United States, companies collaborate with agencies like the Cybersecurity and Infrastructure Security Agency (CISA) under the Department of Homeland Security which has a chemical security subdivision that seeks to enhance security and resilience across the chemical sector. CISA's Chemical Security subdivision offers programs like ChemLock, which works with facilities that use dangerous chemicals to provide no-cost services to understand risks and improve security measures by creating facility-specific security plans [16]. The Chemical Facility Anti-Terrorism Standards (CFATS) also fell within CISA's purview before losing funding in 2023; it was a regulatory program to enhance security at high-risk chemical facilities by overseeing the assessment of vulnerabilities and the implementation of security measures [17]. Amidst the funding setback, industry stakeholders are advocating for the reinstatement of CFATS to continue mitigating the risks associated with the misuse of harmful chemical substances [17]. In 2012, the American Chemical Society established the Safety Culture Task Force to reinforce a strong safety culture in academic institutions by promoting accountability for future scientists, teaching comprehensive laboratory safety and fostering a strong sense of responsibility among researchers to integrate safety into everyday academic practice [18].

In the global context of chemical research security, international organizations such as the United Nations Environment Programme (UNEP) play a crucial role in mitigating the risks posed by harmful chemicals. With a mandate focused on promoting robust policies and best practices worldwide, the UNEP actively assists countries in formulating and implementing regulations to minimize the production, utilization and disposal of harmful chemicals [19]. Through tailored technical assistance and capacity-building programs, UNEP empowers regulatory authorities and stakeholders with the knowledge and skills necessary for safe chemical handling and compliance while promoting collaboration between security experts, scientists, policymakers and industry stakeholders, allowing researchers to effectively navigate the complexities of research security while upholding the principles of scientific freedom and innovation.

The Threat Illicit Research Transfer Poses to Academic and Research Organizations

Overview of Illicit Research Transfer Threats

Threats to IP present unique challenges to innovation and information security, requiring robust measures for safeguarding intellectual property, like stringent vetting processes for collaborators, secure data management protocols and proactive cybersecurity defences to mitigate potential vulnerabilities. From an international perspective, research partnerships, including legal investments, collaborations and talent recruitment programs, often entail sharing proprietary data and intellectual property, increasing the risks of economic espionage, unauthorised technology transfer and data intrusions targeting valuable research findings. These activities are integral to economic growth and innovation, requiring a broader risk awareness and robust legal safeguards to balance the proposed benefits and risks. By addressing these considerations, stakeholders can foster an equitable approach that promotes innovation while safeguarding against vulnerabilities, supporting sustainable and secure economic development by creating a culture of transparency and accountability, securing intellectual property and advancing scientific innovation.

Stages in the Research Lifecycle Susceptible to IP Loss

The research lifecycle is susceptible to knowledge loss or misuse, especially during the conception and development of research proposals through the unintentional sharing of sensitive information with collaborators, peers or funding agencies, increasing the risk of misappropriation or unauthorised disclosure. The competitive nature of securing research funding and grants can incentivize individuals or groups to engage in unethical behaviour, such as idea poaching

or plagiarism to gain a competitive edge. Once research projects are underway, data collection and analysis represent a potential point of vulnerability, especially if working with valuable or proprietary information, which may become a target for unauthorised access by external parties seeking to exploit or replicate the findings for nefarious purposes. These points of vulnerability then become susceptible to incidents such as data breaches, cyberattacks or insider threats, which can compromise the confidentiality and integrity of research data, undermining the credibility and validity of the research outcomes. It's imperative to understand the distinction between the two types of insider threats, intentional and accidental, that pose significant risks; intentional threats can acquire, manipulate or sabotage data, while accidental threats may mishandle data or fall victim to phishing attacks, each leading to potential breaches, compromised research validity and severe reputational and financial damage. Collaborations with external partners, including industry sponsors or international collaborators, can introduce additional risks when sensitive information crosses organizational boundaries without adequate safeguards or contractual agreements.

The global nature of innovation ecosystems and the increasing interconnectedness of academic and industry sectors make it challenging to enforce IP rights effectively and prevent unauthorised knowledge transfer across international borders [20]. Fundamental challenges arise when examining legal considerations surrounding technology development, deployment and usability, particularly with licensing agreements, due diligence requirements and enforcement rights, as the private sector and universities adhere to different approaches to stakeholder protections, joint venture models and IP holding companies. To address these challenges, researchers and institutions must adopt comprehensive strategies for safeguarding IP by implementing robust security measures to protect research data, establishing clear policies and procedures for collaborative research agreements and providing education and training on ethical norms and the best practices in knowledge dissemination and commercialization.

Case Studies

Chemistry: Rafael Luque's Suspension. In 2023, Rafael Luque, a prominent figure in green chemistry, was suspended without pay for 13 years following allegations of research misconduct. Luque, known for his prolific research in green chemistry, faced suspension from the University of Córdoba for holding concurrent positions at other international institutions while under a full-time contract in Spain [21]. In this example, a conflict of interest arose when Luque assumed an external commitment, without proper approvals, at another institution that directly competed with his research obligations at his primary University. Criticisms of Luque's publication practices, including allegations of data manipulation in influential publications, highlighted breaches in scientific integrity and raised concerns about the potential impact on IP rights associated with his research findings. This occurrence highlights the difficulties in managing affiliations and ensuring compliance with contractual obligations since the competitive nature of academic rankings and funding opportunities can incentivize researchers to seek multiple affiliations, risking conflicts of interest and compromising institutional and research integrity.

University Incident: Norwegian University of Science and Technology. In 2022, at the Norwegian University of Science and Technology (NTNU) in Trondheim, a former professor was placed on trial for violations of export regulations and sanctions involving Iran. The professor, of German and Iranian descent, invited four Iranian scientists to NTNU without proper university consent, allowing them access to sensitive equipment like a scanning electron microscope intended for research on materials requiring export licenses [22]. These actions breached international sanctions and Norwegian laws governing scientific collaboration with Iran, highlighting vulnerabilities in the academic institutions' security infrastructure and the need for more stringent measures. The case underscores the importance of robust protocols to safeguard IP and prevent unauthorised access to sensitive research technologies, emphasizing the broader implications for maintaining knowledge security within academic settings [22].

Laboratory Incident: IP Concerns. In 2010, PhD student Ruopeng Liu of Duke University was investigated by the Federal Bureau of Investigation (FBI) after concerns arose surrounding his actions and questionable interest in his advisor, Dr. David Smith's research. Liu brought Chinese colleagues to Dr. David Smith's lab, an expert in metamaterials, whose breakthrough in creating an "invisibility cloak" attracted significant military interest due to its potential defence applications [23]. This meeting led to accusations of photographing sensitive equipment and the replication of Dr. Smith's research in China. Despite Liu's claims of conducting fundamental research, U.S. law enforcement suspected him of being part of a Chinese IP infringement scheme. This incident underscores the importance of thoroughly screening research collaborators, their affiliations and their intentions to safeguard sensitive research and IP.

Methods for Securing Chemical Knowledge in the United States

In the United States, universities and research organizations employ various security protocols and access controls to safeguard knowledge, IP and sensitive research. Different methods are in place within laboratories and research institutions to manage access controls while adhering to comprehensive policies governing the handling and dissemination of IP. One example includes researchers disclosing inventions, discoveries,

or innovations to the institution's technology transfer office, which assesses commercial potential and secures appropriate IP protections like patents or copyrights. In addition to implementing security measures, research contracts and nondisclosure agreements are used to secure knowledge and IP in collaboration with industry stakeholders. These binding agreements establish guidelines for sharing confidential information while protecting intellectual property, often leading to the commercialization of research outcomes. Institutions also monitor potential security threats through cyber-security measures, employee training programs and risk assessment protocols, including data encryption, network segmentation and regular security audits.

U.S. Policies in Research Security

The United States' policies on research security are designed to protect the nation's IP through the adherence to policy mandates like the National Security Presidential Memorandum-33 (NSPM-33), issued in January 2021, advising federal research agencies to strengthen the security protocols surrounding federally funded research to secure technological advancements from espionage, unauthorised access and other threats. These policies are increasingly focused on countering foreign influence and exploitation by implementing standardised procedures for disclosure of conflicts of interest, evaluating international collaborations and enhancing cybersecurity measures. The framework also emphasizes the importance of maintaining an open and collaborative research environment while ensuring that research security measures are robust and effective [24].

In addition to NSPM-33, the U.S. federal government has enacted other measures to safeguard research. For example, the Department of Defence Office of the Under Secretary of Defence for Research and Engineering is set to release guidelines and risk matrices to ensure that research security-related risk analyses are incorporated within all grant decisions [25]. The CHIPS and Science Act, signed into law in 2022, aims to mitigate research security risks throughout the research lifecycle by developing security policies and best practices to ensure compliance with NSPM-33 [26]; with research-focused agencies like the National Institutes of Health and the National Science Foundation have developed guidelines and requirements for grant recipients to disclose foreign affiliations and funding sources [27]. These measures are part of a broader strategy to protect the U.S. research enterprise from undue foreign influence while promoting transparency, accountability and the ethical conduct of research.

Methods for Securing Chemical Knowledge in Romania

Pharmaceutical research is multidisciplinary and complex, so research laboratories generate scientific data that can have a significant impact on different areas of the health domain. Implementing security measures for chemical knowledge in pharmaceutical research laboratories within Romanian universities is a priority due to the sensitivity of data and their potential impact on public health and pharmaceutical innovation. The Faculties of Pharmacy as part of the Romanian universities have implemented several methods to safeguard intellectual property, pharmaceutical data and sensitive research information. These measures align with both national and international standards, ensuring that research integrity is maintained and that knowledge is protected against unauthorised access or misuse.

Intellectual Property (IP) Management and Protection

Romania has been part of the Unitary Patent (UP) system since the 1st of September 2024. This is an important step for recognition of the valuable resource of innovative research and also increases opportunities to participate in domestic technology markets and better integrate into the European Economic Area [28]. According to statistics published by the State Office for Inventions and Trademarks (OSIM), there has been continuous interest over the past 10 years for patent filings. Patent applications and grants from Universities of Medicine and Pharmacy in Romania have increased, with pharmacy faculties contributing significantly to this trend [29]. Several Romanian universities have developed dedicated units for IP management regarding pharmaceutical research departments. These units work to ensure that intellectual property related to new pharmaceutical compounds, chemical formulations and drug delivery systems developed in university labs is properly protected. The process typically involves close collaboration with the State Office for Inventions and Trademarks (OSIM), ensuring that research discoveries are covered under Romanian and European patent protection. In scientific projects or other scientific collaborations, non-disclosure agreements (NDAs) and strict IP clauses in partnership agreements between universities and industry or other private partners further protect sensitive chemical knowledge from being prematurely disclosed.

Collaborative Research and Knowledge Transfer Protocols

Collaboration between pharmacy departments and the private sector is essential for translating scientific research into marketable pharmaceutical products. However, these collaborations must be managed carefully to ensure that sensitive chemical knowledge is protected. Romanian universities have developed knowledge transfer offices (KTOs) that facilitate secure collaboration while safeguarding IP [30]. KTOs oversee the drafting of collaboration agreements that include confidentiality clauses and IP-sharing frameworks. These agreements ensure that the university retains control over the dissemination of chemical knowledge, even in joint groups with the pharmaceutical private sector. Additionally, joint research projects are often conducted under strict access control conditions, where

only researchers directly involved in the study have access to chemical databases or experimental results.

Data Encryption and Digital Security in Pharmaceutical Research

Digital security is a cornerstone in protecting chemical knowledge in university laboratories. Pharmaceutical research often generates large volumes of sensitive data, including chemical structures, pharmacological profiles and clinical trial results, which must be stored or transmitted securely. Romanian universities employ data encryption technologies to secure chemical research databases. For example, end-to-end encryption is commonly used to protect data during transfer, ensuring that sensitive research information cannot be intercepted or accessed by unauthorised entities [31]. Moreover, many pharmacy departments have implemented cloud-based solutions with multi-factor authentication (MFA) and role-based access control (RBAC) to prevent un-authorised personnel from accessing sensitive chemical data. At the European level, the main support for the development of the open science ecosystem is provided by the European Open Science Cloud (EOSC), which will be developed in the period 2021 - 2027 within the Horizon Europe research-innovation program [32]. EOSC support projects are currently underway, which have the role of stimulating the participation of the countries from various regions of Europe in the promotion, expansion and use of the resources of this ecosystem. The main modality adopted by these projects to enable participation at the national level is the National Open Science Cloud Initiatives (NOSCI) [33]. The Ministry of Research, Innovation and Digitalization is in partnership with the European Open Science Cloud (EOSC) and the universities are obliged to join and implement the policies provided for in the National Cloud for Open Science.

Compliance with Regulatory Standards and Ethical Guidelines

Compliance with Good Laboratory Practice (GLP) standards, as well as the European Medicines Agency (EMA) and Romanian National Medicines Agency (NAMMDR) guidelines is critical to maintaining the security and integrity of chemical knowledge. Romanian Universities of Medicine and Pharmacy adhere to strict regulatory standards to ensure the secure handling of hazardous chemicals and sensitive research information. In recent years, laboratories have adopted comprehensive chemical inventory management systems that allow researchers to monitor the use and disposal of chemical substances securely. These systems are essential in maintaining compliance with the REACH regulation (Registration, Evaluation, Authorisation and Restriction of Chemicals), which controls the registration and safe use of chemical substances in research. This also ensures that potentially hazardous chemical data is kept secure and that access is restricted to trained personnel only.

Physical Security Measures in University Research Labs

Physical security in pharmaceutical laboratories is another critical aspect of securing chemical knowledge. The universities have implemented a range of physical security measures to prevent unauthorised access to research facilities and sensitive chemical compounds. Key measures include access controls, surveillance systems and restricted laboratory areas, particularly where hazardous chemicals or valuable research data are stored. Additionally, the laboratories undergo regular audits to ensure compliance with safety and security standards, such as ISO/IEC 17025, which governs the competence of testing and calibration laboratories and includes guidelines for secure laboratory operations.

Methods for Securing Chemical Knowledge in Bulgaria

As an active member of the EU, Bulgaria adheres to a comprehensive framework of directives, regulations and decisions designed to address incidents of biological and chemical concern. These legal instruments form the backbone of the EU's collective efforts to ensure that member states comply with international standards and obligations aimed at preventing the proliferation, development and use of biological and chemical weapons. Like other EU member states, Bulgaria implements these frameworks by coordinating its national policies with regional strategies, enhancing cross-border collaboration to manage these threats. In recent years, the EU has also begun to adopt more stringent measures around research security, recognizing the importance of safeguarding scientific progress while preventing misuse. The following is a list of regulations and recommendations adopted by Bulgaria as a member state of the EU.

Regulations. Council Regulation (EU) 2018/1542 of the 15th of October 2018 concerning restrictive measures against the proliferation and use of chemical weapons [34]. Council Regulation (EU) 2018/1542, establishes a framework for implementing restrictive measures aimed at preventing the proliferation and the use of chemical weapons. This regulation reflects the EU's commitment to combating the threat posed by chemical weapons and ensuring compliance with international obligations. It provides for the imposition of asset freezes, travel bans and other restrictive measures against individuals and entities involved in the development, production and use of chemical weapons while emphasizing the importance of international cooperation and the need to strengthen global norms against chemical warfare.

Recommendations Council Recommendation on enhancing research security of the 23rd May 2024 [35]. On the 23rd of May 2024, the EU Council adopted a recommendation to bolster research security to protect research and innovation from misuse while maintaining

the importance of international collaboration. The recommendation emphasizes a balanced approach, promoting openness alongside the necessary safeguards for securing sensitive knowledge. The European Commission will support this effort by establishing a Centre of Expertise on Research Security and facilitating a European Flagship Conference in 2025 to review progress.

It's important to note that the European Council (EC) has extended the sanctions regime against the proliferation and use of chemical weapons over the next three years. It will remain in effect until the 16th of October 2026, while the restrictive measures against specific individuals and entities were extended to 16th of October 2024, though they have now lapsed. According to the EC [36], the current sanctions target 25 individuals and three entities suspected or convicted of supporting chemical weapons proliferation. These sanctions involve an asset freeze, prohibiting EU persons and entities from making funds, financial assets, or economic resources available to the sanctioned parties. *Per* the sanctions, individuals subject to these measures are restricted from traveling, preventing them from entering or transiting through any EU member state. The regulations aim to curb the development and use of chemical weapons by limiting the resources and mobility of those involved in their proliferation. The regime is part of the EU's broader efforts to promote global security and compliance with international chemical weapons conventions.

Recommendations for International Institutions to Enhance Research Integrity

International institutions play a critical role in fostering a culture of research security, especially as global collaborations and data-sharing become increasingly prevalent. Safeguarding research across international boundaries demands a comprehensive and multifaceted approach to address the complexities and sensitivities inherent in cross-border research collaborations. To implement a robust security architecture, academic and research institutions must adopt a multifaceted approach to emphasize practical and scalable solutions. This strategic initiative should begin with establishing standardised protocols for data sharing, intellectual property protection and ethical research practices. The protocols must be adaptable to the unique needs of individual countries and research institutions while maintaining sufficient consistency to foster international trust and cooperation. In today's complex and competitive research environment, institutions are pivotal in upholding the integrity of technological innovation. Research security extends beyond merely preventing misconduct; it encompasses a culture of responsibility, transparency and trust throughout the research process. By embedding security practices at every research stage-from conception and design to execution and publication-universities and research institutions can enhance the credibility of their findings, protect their reputations and contribute to scientific innovation. To achieve this goal, the organizations should implement a range of practical measures that promote and enforce research security, including:

Establishing Clear Guidelines and Policies. Universities and research institutions must define and reinforce their commitment to research security and develop well-structured and detailed frameworks. These guidelines should be aligned with national and international research standards and articulate the institution's security framework with expectations reinforcing responsible research conduct.

Promoting Education and Training. Ensuring that researchers adhere to the security standards requires continuous education and training for all individuals involved throughout the research lifecycle, including faculty, students and administrative staff. These programs should cover data management, cybersecurity and information-sharing techniques to reinforce a security culture and assist researchers in staying vigilant in sustaining and safeguarding innovation.

Implementing Robust Oversight Mechanisms. The universities and research institutions should establish dedicated research security oversight bodies to monitor compliance with national and international standards for auditing research practices, reviewing data management protocols and identifying cybersecurity vulnerabilities.

Fostering Collaboration. Given the international collaborative nature of research, fostering information-sharing networks among universities, research institutions and funding bodies is crucial to sustaining best practices and research integrity while maintaining innovation and global stability.

Conclusions

The dual-use nature of chemical innovation-both beneficial and potentially harmful-underscores the need for a robust security architecture to protect IP, ensure ethical practices throughout the research lifecycle and prevent the misuse of sensitive information and dual-use technologies. Universities must develop new training, guidelines and policies that consider the dual-use challenge of chemical and pharmaceutical research. While the equipment, research and materials needing protection will differ by country, the threat of losing value intellectual property is shared among universities worldwide. By building off existing international frameworks, convening national and regional forums and activating local stakeholders' universities can take a multifaceted approach to bolstering chemical and pharmaceutical research security.

Balancing the culture of openness and collaboration with research security measures is not an easy challenge for universities wanting to achieve a competitive and first-mover advantage. The universities and research

laboratories worldwide are at the forefront of groundbreaking discoveries, which if transferred to malign individuals and groups, can lead to the devastating development of a chemical weapon. The convergence of chemical security with research security provides universities the unique opportunity to protect the international community against the harm caused by the misuse of dual-use chemicals and emerging technologies while upholding the tenets of scientific discovery.

This partnership between Pacific Northwest National Laboratory, USA, "Carol Davila" University of Medicine and Pharmacy, Romania, and New Bulgarian University, Bulgaria, introduced the challenges and benefits of international collaborations within different regulations and research cultures. In the United States, regulations guide universities to focus on the countering foreign influence within international collaborations, in Romania national standards encourage universities to protect against unauthorised access and data breaches, and in Bulgaria, recent EU recommendations will emphasize a balanced approach to openness and security.

Addressing research security is more than preventing misconduct and the proliferation of knowledge; it is about developing a culture of shared values, responsibilities and trust throughout the research lifecycle. We use this joint effort to encourage continuous cross-border research collaborations between like-minded organizations focused on advancing scientific developments while enforcing research security.

Acknowledgement

The development of this publication was supported by the U.S. Department of State, Chemical Security Program.

Conflict of interest

The authors declare no conflict of interest.

References

1. National Academies Press. The importance of chemical research to the U.S. economy. Washington, D.C.: *National Academies Press*; 2022.
2. Securing higher education against cyberthreats: from an institutional risk to a national policy challenge, www.tandfonline.com/doi/full/10.1080/23738871.2021.1973526.
3. Identifying university chemicals that pose security risks: a simple qualitative approach. ACS Chem Health Saf., https://pubs.acs.org/doi/10.1021/acs.chas.0c00082.
4. Van Dusen V, Intellectual property and higher education: challenges. *Adm Issues J.*, 2013; 3(2).
5. European Commission. Horizon Europe, https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.
6. European Research Area Platform. European Commission, https://european-research-area.ec.europa.eu/.
7. EECARO. EECARO - European Export Control Association for Research Organisations, https://eecaro.eu/.
8. Horizon 2020 Framework Programme of the European Union. General data protection regulation (GDPR) compliance guidelines. GDPR.eu; https://gdpr.eu/.
9. European Commission. Your guide to intellectual property management in Horizon Europe https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/out-now-your-guide-intellectual-property-management-horizon-europe-2022-12-01_en.
10. European Research Area Platform, https://european-research-area.ec.europa.eu/.
11. Sen JPB, Sandhu R, Bland S, Chemical incidents. *BJA Educ.*, 2021; 21(4): 126-132.
12. OPCW. OPCW Releases Third Report by Investigation and Identification Team. www.opcw.org/media-centre/news/2023/01/opcw-releases-third-report-investigation-and-identification-team.
13. Organisation for the Prohibition of Chemical Weapons. Organisation for the Prohibition of Chemical Weapons, OPCW, www.opcw.org/node/2632.
14. United Nations Economic Commission for Europe. About the GHS | UNECE. Globally Harmonised System of Classification and Labelling of Chemicals (GHS), https://unece.org/about-ghs.
15. European Commission. REACH Regulation, https://environment.ec.europa.eu/topics/chemicals/reach-regulation_en.
16. Walters DB, Ho P, Hardesty J, Safety, security and dual-use chemicals. *J Chem Health Saf.*, 2015; 22(5): 3-16.
17. American Chemistry Council. Chemical facility anti-terrorism standards (CFATS) www.americanchemistry.com/better-policy-regulation/safety-security/chemical-facility-anti-terrorism-standards-cfats.
18. American Chemical Society. Creating safety cultures in academic institutions www.acs.org/education/students/graduate/creating-safety-cultures-in-academic-institutions.html.
19. United Nations Environment Programme. Welcome to the global framework on chemicals website, www.chemicalsframework.org/.
20. Acikalin U, Caskurlu T, Hoberg G, Phillips GM. Intellectual property protection lost and competition: an examination using large language models. *Soc Sci Res Netw.*, 2022; Rochester, NY: 4023622.
21. Ansede M, One of the world's most cited scientists, Rafael Luque, suspended without pay for 13 years. *EL PAÍS English*, 2023, https://english.elpais.com/science-tech/2023-04-02/one-of-the-worlds-most-cited-scientists-rafael-luque-suspended-without-pay-for-13-years.html.
22. Myklebust JP, Professor in lengthy trial over Iranian scientists' visits. *Univ World News.*, 2022, www.universityworldnews.com/post.php?story=20220914104835727.
23. McFadden C, Nadi A, McGee C, Education or espionage? A Chinese student takes his homework home to China. *NBC News*, www.nbcnews.com/news/china/education-or-espionage-chinese-student-takes-his-homework-home-china-n893881.
24. The White House. Presidential memorandum on United States government-supported research and development national security policy, https://trumpwhitehouse.archives.

gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/.
25. Academic research security, https://basicresearch.defense.gov/Programs/Academic-Research-Security/.
26. U.S. Department of Justice. National Security Division | Information about the Department of Justice's China Initiative and a compilation of China-related prosecutions since 2018, www.justice.gov/archives/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related.
27. National Institutes of Health. Information for foreign grants, Grants and Funding, https://grants.nih.gov/new-to-nih/information-for/foreign-grants.
28. Patent Office. Unitary patent now covers Romania, EPO.org, www.epo.org/en/news-events/news/unitary-patent-now-covers-romania.
29. State Office for Inventions and Trademarks. Statistics published in 2024, https://osim.ro/en/about-osim/who-we-are/statistics/statistics-published-in-2024.
30. Vac C, Vac L, Naş V, Research, innovation and technology transfer: concepts, worldwide experience and prospects for its development in Romanian universities. *Bull Univ Agric Sci Vet Med Cluj-Napoca Agric.*, 2015; 72.
31. Ulybyshev D, Rogers M, Kholodilo V, Northern B, End-to-End Database Software Security. *Software*, 2023; 2(2): 163-176.
32. European Commission. European Open Science Cloud (EOSC), https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/open-science/european-open-science-cloud-eosc_en.
33. Ministerul Educației. National cloud initiative for open science, https://uefiscdi.gov.ro/ro-nosci.
34. Regulation - 2018/1542, https://eur-lex.europa.eu/eli/reg/2018/1542/oj.
35. EU Member States adopt recommendations to enhance research security, https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/eu-member-states-adopt-recommendations-enhance-research-security-2024-05-23_en.
36. European Council. Chemical weapons: EU restrictive measures prolonged for an additional year. Consilium, www.consilium.europa.eu/en/press/press-releases/2023/10/09/chemical-weapons-eu-restrictive-measures-prolonged-for-an-additional-year/.