4. Astărăstoaie V. Etică medicală și medicalizarea societății. În: (accesat: 24.07.2023).
5. Țîrdea T.N. Bioetică. Curs de bază. Chișinău: CEP „Medicina”, 2017. În: (accesat: 15.06.2023).
6. Cârstoiu C. Comunicarea farmacist-pacient. În: https://farma.com.ro/articles/2012.3-4/PF_Nr-3-4_2012_Art-10.pdf (accesat: 24.07.2023).
7. Deans Z. Ethics in pharmacy practice. In: https://www.pharmacyresearchuk.org/wp-content/ uploads/2012/11/Ethics_in_pharmacy_practice_200910.pdf (accesat: 25.08.2023).
8. Bhaswat S., Chakraborty B. Ethics in pharmacy profession. In: https://www.slideshare.net/ bhaswatchakraborty/ethics-in-pharmacy (accesat: 25.08.2023).

DIMENSIUNEA ETICĂ A SECURITĂȚII INFORMAȚIONALE ÎN SERVICII DE SĂNĂTATE MINTALĂ

Alexandru Dorosevici–Duka, doctorand
Catedra de filosofie și bioetică, Universitatea de Stat de Medicină și Farmacie „Nicoloae Testemițanu”, Chișinău, Republica Moldova
adorosevici@gmail.com

THE ETHICAL DIMENSION OF INFORMATION SECURITY IN MENTAL HEALTH SERVICES

The development of digital technologies, electronic medical records and remote medical consultations have led to an increase in digital activities in the medical field worldwide. This has created new opportunities for effective diagnosis, treatment and monitoring of health services. However, these new opportunities also present ethical issues and potential information security risks. Mental health data is among the most sensitive and unreliable, containing personal and sometimes stigmatizing information about patients. Ensuring the confidentiality of patient data is crucial to maintaining trust between patients and medical professionals. Unauthorized access, leakage or insecure storage of data can have serious consequences for patients, including breaches of confidentiality and trust in medical services. The mental health service system is an area where confidentiality is paramount, with the protection of patient privacy being

a priority. The increasing use of electronic data storage creates new vulnerabilities and risks. Healthcare organizations are required to adhere to ethical standards and strict legal regulations in the field of information security. In order to minimize these risks, it is essential to train medical personnel in information security issues, introduce modern encryption and authentication technologies, perform regular audits and regulatory audits, educate them on the ethical and legal aspects of maintaining personal data. Three categories of people who can affect the security of patient information include cybercriminals, people with an interest in patient care, and law enforcement officials who engage in illegal activities. These people can put additional pressure on healthcare professionals, which can lead to legal and ethical issues. In conclusion, the mental health service system must prioritize the protection of patient data and ensure the highest ethical standards in the field.

Introducere

La etapa actuală a dezvoltării societății umane, securitatea informațională a devenit una dintre cele mai pregnante probleme care afectează toate sferele vieții, inclusiv domeniul sănătății mintale. Dezvoltarea tehnologiilor digitale, a documentației medicale electronice și a consultațiilor medicale la distanță, a dus la creșterea activității digitale în domeniul sănătății mintale în majoritatea țărilor din lume. Acest lucru, desigur, creează noi oportunități pentru diagnosticarea, tratamentul și monitorizarea mai eficiente a beneficiarilor serviciilor de sănătatea mintală, care au devenit mai ieftine și mai accesibile pentru un număr mare de consumatori [1].

Cu toate acestea, odată cu aceste noi oportunități apar noi probleme etice și potențiale riscuri în domeniul securității informațiilor. Datele referitoare la sănătatea psihică sunt printre cele mai sensibile și intime, conținând informații personale și uneori chiar potențial compromițătoare despre pacienți, poate fi afectată de resurse limitate pentru transformarea procesului de păstrarea datelor de caracter personal și îngrijire, eroare medicală și factorul uman, siguranța software-ului și organizarea proceselor de funcționare a serviciilor de sănătate mintală. Păstrarea confidențialității datelor este esențială pentru menținerea relațiilor de încredere între pacienți și profesioniștii medicali. Scurgerile, accesul neautorizat sau stocarea nesigură a acestor date pot avea consecințe negative grave pentru pacienți, inclusiv încălcarea confidențialității și a încrederii în serviciile medicale [2].

În acest articol, vom lua în considerare diverse aspecte etice ale securității informațiilor în sistemul de sănătate mintală. De asemenea, vom analiza vulnerabilitățile cu care se confruntă aceste sisteme și luăm în considerare riscurile asociate acestora. Scopul nostru final, este să înțelegem cum să asigurăm siguranța datelor mentale ale pacienților fără a le încălca drepturile la confidențialitate și îngrijire medicală de calitate, respectând valorile etice în domeniul sănătății mentale la cele mai înalte standarde.

Vulnerabilitatea informațională în sistemul de sănătate mintală

Sistemul de sănătate mintală este un domeniu al medicinei în care protecția vieții private a pacientului este cea mai mare prioritate, fiind nu mai puțin importantă decît reducerea simptomaticii psihopatologice, pentru pacienții și personalul serviciilor din domeniu. Cu toate acestea, practica medicală modernă ține pasul cu era digitală, iar datele despre sănătatea mintală a pacienților sunt din ce în ce mai mult stocate în format electronic. Acest lucru creează noi vulnerabilități și riscuri care trebuie luate în considerare și abordate. Una dintre vulnerabilitățile cheie este posibilitatea furtului de date. Datele psihiatrice pot conține informații sensibile sau stigmatizante, inclusiv diagnostice, istoricul tratamentului, rezultatele tratamentului și chiar detalii despre viața personală a pacienților. Răufăcătorii pot fi motivați să acceseze astfel de informații pentru o varietate de scopuri, inclusiv fraudă, șantaj sau vânzarea de date pe piața neagră. Siguranța poate fi compromisă și de personalul medical. Medicii, terapeuții și asistentele au acces la datele pacienților pentru a oferi îngrijiri de calitate, iar utilizarea greșită sau stocarea nesigură a datelor poate duce la scurgeri accidentale sau intenționate de informații [3]. Acest lucru poate provoca nu numai consecințe juridice grave, dar poate afecta și încrederea pacienților în serviciile medicale. Un alt aspect important al vulnerabilității este securitatea insuficientă. Sistemele care stochează date referitoare la sănătatea psihică trebuie să fie fiabile și protejate de atacurile externe. Este important de menținut sistemele informaționale actualizate și monitorizate, pentru a preveni potențialele încălcări de securitate. La rândul său pacienții se așteaptă ca datele lor personale să fie confidențiale, iar încălcarea acestei confidențialități poate cauza nemulțumiri grave și chiar consecințe legale. Prin urmare, organizațiile medicale sunt obligate să respecte cu strictețe standardele etice și legile în domeniul securității informațiilor. Pentru a minimiza vulnerabilitățile și riscurile în sistemul de sănătate mintală, este necesar să se acorde o atenție deosebită pregătirii personalului medical în

probleme de securitate a informațiilor, să se introducă tehnologii moderne de criptare și autentificare și să se efectueze revizuiri și audituri regulate ale sistemelor de securitate, iar personalul medical să fie instruit special și sensibilizat despre caracterul etic și legal al păstrării corecte a datelor de caracter personal, în Republica Moldova un rol important în divulgarea accidentală sau intenționată a datelor personale sunt dimensiunile mici a societății și relațiile strânse de familie, sau alte legături sociale. Aceste măsuri vor contribui la asigurarea protecției datelor de caracter personal ale pacienților și la menținerea confidențialității acestora, care este un drept fundamental în practicarea medicinei [5].

Riscuri în sistemele informaționale a serviciilor de sănătate mintală

Riscurile asociate cu securitatea informațiilor în sistemul de sănătate mintală au implicații ample și necesită o atenție serioasă.

Unul dintre principalele riscuri este posibila scurgere a datelor personale ale pacienților. Această scurgere poate apărea accidental din cauza defecțiunilor tehnice, a securității insuficiente sau a erorilor de procesare a datelor. În astfel de cazuri, datele pot cădea în mâini nedemne de încredere și pot fi utilizate în scopuri ilegale. Acest lucru poate încălca drepturile la intimitate ale unei persoane și poate duce la consecințe negative grave pentru pacienți.

Un alt risc important este teama de stigmatizare. Datele despre sănătate mentală ale unui pacient, lăsate în domeniul public, pot fi folosite pentru a discrimina la locul de muncă, la cererea de asigurare sau chiar în viața de zi cu zi. Acest lucru poate afecta foarte mult viața și bunăstarea pacienților și poate deveni o barieră în găsirea îngrijirii de care au nevoie.

În plus, riscurile includ sisteme de securitate insuficiente și accesul nedorit al personalului medical la date. Controlul slab al accesului poate duce la scurgeri de informații sau la dezvăluirea nesigură a detaliilor sensibile. Acest lucru nu numai că încalcă drepturile pacienților, dar poate duce și la probleme juridice uriașe pentru organizațiile din domeniul sănătății.

Reducerea riscurilor și asigurarea securității informațiilor în sistemul de sănătate mintală necesită acțiuni la mai multe niveluri. În primul rând, organizațiile din domeniul sănătății trebuie să investească în tehnologie și sisteme moderne de securitate, inclusiv în criptarea datelor, sisteme de autentificare și monitorizare. Formarea eficientă în domeniul securității informațiilor pentru personalul medical este, de asemenea, esențială.

Bazându-ne pe experiențe profesionale putem destinge 4 categorii de

persoane care pot atenta la securitatea informațională a pacienților

1. Răufăcătorii cibernetici specializați la vânarea și colectarea ilegală a datelor personale cu scop de a le comercializare, șantaj și alte activități ilegale.
2. Persoane fizice (rude, vecinii), interesate de starea sănătății pacientului în scop personal, de exemplu aflându-se în conflict cu scop de răzbunare, sau litigii.
3. Angajații altor instituții de stat care în dorința de a rezolva probleme de investigații, căutări, sau completarea datelor cât mai rapidă, recurg uneori la abordarea neprotocolară și neoficială a personalului medical, efectuând o presiune suplimentară asupra profesioniștilor, care pot ceda la invocare autorității persoanei ce abuzează de postul sau puterea oferită de stat.
4. Personalul medical utilizând datele de caracter personal în mod impropriu.

În plus, standardele etice și legile care guvernează accesul la datele psihice trebuie respectate cu strictețe. Aceasta include menținerea transparenței și a consimțământului pacientului în procesarea și stocarea datelor lor, precum și reducerea la minimum a accesului nesigur la informații.

Sistemul de sănătate mintală trebuie să se depună efort să mențină un nivel ridicat de securitate a informațiilor pentru a proteja drepturile și intimitatea pacienților. Acest lucru este esențial pentru menținerea încrederii între pacienți și furnizori și pentru asigurarea furnizării eficiente a îngrijirilor de sănătate mintală. Mai ales în perspectiva unificării bazelor de date și în situație când personalul medical se poate asocia cu Design-ul precar a sistemelor informaționale sau neajunsuri a protocoalelor de securitate informațională (Tubaishat 2019) [6].

Principii și recomandări etice

Asigurarea securității informațiilor în sistemul de sănătate mintală necesită respectarea unor principii etice stricte. Aceste principii nu numai că ajută la protejarea datelor pacienților, dar susțin și relații puternice între prestatori și pacienți.

Transparența este un principiu etic cheie. Pacienții trebuie să aibă o înțelegere clară a modului în care datele lor vor fi utilizate și protejate. Medicii și psihoterapeuții ar trebui să contribuie la educarea și confidențialitatea pacienților.

Consimțământul este un alt principiu etic important. Pacienții trebuie

să își dea consimțământul pentru colectarea și prelucrarea datelor lor, iar acest consimțământ trebuie să fie voluntar și bazat pe o alegere informată.

Confidențialitatea este al treilea principiu important. Medicii și personalul medical sunt obligați să păstreze confidențialitatea strictă a datelor pacienților. Aceasta include asigurarea faptului că datele sunt stocate și accesate în siguranță.

Corectitudinea este ultimul, dar nu în ultimul rând, principiu etic important. Toți pacienții au dreptul la acces egal la îngrijiri de sănătate mintală de calitate, iar nivelul de confidențialitate ar trebui să fie același pentru toată lumea.

Utilizarea corectă în spiritul bunelor practici a datelor de caracter personal a lucrătorilor medicali care au acces la bază de date [4.]

Pentru a îmbunătăți securitatea informațiilor în sistemul de sănătate mintală, se recomandă următoarele:

1. Elaborarea politicilor și procedurilor stricte de manipulare a datelor, bazată pe instruirea personalului din domeniul sănătății mentale cu privire la probleme de siguranță și etice.

2. Consolidarea sistemelor de monitorizare și control pentru a preveni scurgerile și abuzurile.

3. Investiția în tehnologii moderne de securitate și criptare a datelor.

4. Promovarea educației și conștientizării pacienților cu privire la securitatea și etica informațiilor.

5. Informarea colaboratorilor altor instituții privind accesul legal a datelor de caracter personal și oprirea practicilor neoficiale.

În concluzie, considerentele etice ale securității informațiilor în sistemul de sănătate mintală sunt esențiale pentru asigurarea drepturilor și bunăstării pacienților. Menținerea confidențialității, menținerea principiilor etice și implementarea recomandărilor vor ajuta la reducerea riscurilor și la crearea unui mediu sigur pentru îngrijirea sănătății mintale [7].

Referințe bibliografice

1. Berner Eta. Ethical and Legal Issues in the Use of Health Information Technology to Improve Patient Safety. In: HEC forum: an interdisciplinary journal on hospitals' ethical and legal issues, 2008, No20, pp.243-58. 10.1007/s10730-008-9074-5
2. James M. Walker, Pascale Carayon, Nancy Leveson, Ronald A. Paulus, John

Tooker, Homer Chin, Albert Bothe, Walter F. Stewart. EHR Safety: The Way Forward to Safe and Effective Systems. In: Journal of the American Medical Informatics Association, 2008, Volume 15, Issue 3, May, pp.272–277. https://doi.org/10.1197/jamia.M2618 (accesat: 25.08.2023).
3. Tariq RA, Hackert PB. Patient Confidentiality. 2023 Jan 23. In: StatPearls. Treasure Island (FL): StatPearls Publishing; 2023 Jan. PMID: 30137825. (accesat: 25.08.2023).
4. Palojoki Sari. The understanding and prevention of technology-induced errors in electronic health records: A path toward health information technology resilience. PhD Thesis. Itä-Suomen yliopisto. 2017.
5. Sittig DF, Singh H. Electronic health records and national patient-safety goals. In: N Engl J Med., 2012, Nov, No 8;367(19), pp.1854-60. doi: 10.1056/NEJMsb1205420. PMID: 23134389; PMCID: PMC3690003.
6. Tubaishat Ahmad. The effect of electronic health records on patient safety: A qualitative exploratory study. In: Informatics for Health and Social Care, 2019, Vol.44, No1, pp.79-91. DOI: 10.1080/17538157.2017.1398753
7. Lege Nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal. În: https://www.legis.md/cautare/getResults?doc_id=10607&lang=ro (accesat: 11.08.2023).

BIOETICA IN CONTEXTUL ANARHO-PRIMITIVISMULUI

Eugeniu Tocarschii, asistent unniversitar
Departamentul Filosofie si Antropologie, Universitatea de Stat din Moldova, Chișinău, R.Moldova
tocarschii.evghenii@gmail.com

BIOETHICS IN THE CONTEXT OF ANARCHO-PRIMITIVISM

Anarcho-primitivism is a trend in anarchism based on criticism of the origins and achievements of civilization. Primitivisms argue that the transition from hunting and gathering to agriculture gave rise to social stratification, coercion and alienation. They are proponents of abandoning civilization through deindustrialization, abolishing the division of labor and specialization, and abandoning large-scale technology. Modern technology is a single system in which all parts depend on each other. You can't get rid of its bad parts and leave only the good ones. No amount of laws, morals, traditions will not protect you from technology for the long