1. **Introducere**
    - Scopul Politicii
    - Domeniu de Aplicare
    - Cadru Legal (GDPR și Legislația Românească privind Protecția Datelor)
2. **Definiții**
    - Termeni Cheie (Date Personale, Prelucrare, Subiect al Datelor, etc.)
3. **Principii de Protecție a Datelor**
    - Legalitate, Echitate și Transparență
    - Limitarea Scopului
    - Minimizarea Datelor
    - Precizie
    - Limitarea Stocării
    - Integritate și Confidențialitate
    - Responsabilitate
4. **Roluri și Responsabilități**
    - Responsabilitățile Ofițerului de Protecție a Datelor (OPD)
    - Responsabilitățile Personalului
    - Responsabilitățile Procesatorului de Date
5. **Drepturile Subiectilor Datelor**
    - Dreptul la Informare
    - Dreptul de Acces
    - Dreptul la Rectificare
    - Dreptul la Ștergere („Dreptul de a fi Uitat”)
    - Dreptul de a Restrictiona Prelucrarea
    - Dreptul la Portabilitatea Datelor
    - Dreptul de Opoziție
    - Drepturi legate de Decizia Automatizată și Profilare
6. **Procedurile de Colectare a Datelor**
    - Mecanisme de Consimțământ
    - Colectarea Datelor de la Minorii
    - Categorii Speciale de Date
7. **Utilizarea și Prelucrarea Datelor**
    - Baza Legală pentru Prelucrare
    - Partajarea și Transferul Datelor
    - Acorduri de Prelucrare a Datelor
8. **Măsuri de Securitate a Datelor**
    - Garanții Tehnice
    - Garanții Fizice
    - Măsuri Organizaționale
9. **Răspuns și Notificare în Caz de Breșă de Securitate**
    - Proceduri de Detectare și Raportare
    - Evaluare și Atenuare
    - Proceduri de Notificare (către Autorități și Subiecții Datelor)
10. **Gestionarea Furnizorilor și a Procesatorilor Terti de Date**
    - Diligență Datorată
    - Contracte și Acorduri

- Monitorizare și Conformitate

11. **Evaluarea Impactului Asupra Protecției Datelor (EIPD)**
    - Când este Necesară EIPD
    - Procesul EIPD
    - Documentație și Revizuire
12. **Revizuirea și Monitorizarea Politicii**
    - Programul Regulat de Revizuire a Politicii
    - Audituri de Conformitate
    - Actualizarea Procedurilor și Practicilor

1. Introducere

În calitate de clinică medicală angajată în furnizarea de servicii de sănătate de înaltă calitate, recunoaștem importanța și responsabilitatea de a proteja datele personale ale pacienților noștri, angajaților și ale tuturor persoanelor a căror informații le prelucrăm. Această politică de protecție a datelor este concepută pentru a asigura conformitatea cu Regulamentul General privind Protecția Datelor (GDPR) al Uniunii Europene și cu legislația română aplicabilă în domeniul protecției datelor.

Scopul Politicii

Scopul acestei politici este de a stabili principiile și procedurile pe care clinica noastră le adoptă pentru a garanta că toate datele personale sunt prelucrate într-un mod legal, corect și transparent. Ne angajăm să protejăm confidențialitatea, integritatea și disponibilitatea datelor personale ale pacienților și ale altor persoane implicate, prin aplicarea unor măsuri de securitate tehnice și organizatorice adecvate.

Această politică este destinată să:

- Asigure conformitatea clinică noastră cu GDPR și cu alte legi relevante în materie de protecție a datelor.
- Protejeze drepturile și libertățile fundamentale ale persoanelor, în special dreptul la protecția datelor personale.
- Stabilească responsabilitatea și procedurile pentru gestionarea și protejarea datelor personale.
- Informeze angajații și persoanele a căror date le prelucrăm despre modul în care sunt gestionate datele lor personale și despre drepturile de care beneficiază.

Prin implementarea acestei politici, ne propunem să consolidăm încrederea pacienților și a partenerilor noștri în angajamentul nostru constant de a respecta și proteja datele personale.

Aceasta este introducerea și scopul politicii. În continuare, politica va detalia principiile de bază ale protecției datelor, rolurile și responsabilitățile personalului, drepturile subiecților datelor, precum și procedurile specifice de prelucrare și securitate a datelor.

1.2 Domeniul de Aplicare

Această politică se aplică tuturor formelor de prelucrare a datelor personale (în format electronic și fizic) efectuate de către clinica noastră medicală, inclusiv datele personale ale pacienților, angajaților, colaboratorilor și altor părți terțe. Acoperă toate procesele și sistemele prin care sunt colectate, stocate, utilizate, divulgate, transferate sau distruse aceste date personale.

Domeniul de aplicare include, dar nu se limitează la, următoarele aspecte:

- **Datele Pacienților:** Informații legate de sănătate, istoric medical, informații de contact, și orice alte date personale colectate în cursul furnizării serviciilor medicale.

- **Datele Angajaților:** Informații personale legate de angajare, inclusiv dar nu limitat la, date de identificare, informații financiare și alte date personale necesare pentru administrarea relației de muncă.
- **Datele Partenerilor și Furnizorilor:** Datele personale ale reprezentanților și angajaților entităților cu care clinica intră în relație contractuală.
- **Vizitatorii și Utilizatorii Website-ului:** Date personale colectate prin intermediul website-ului clinicii, inclusiv, dar fără a se limita la, formulare de contact și cookie-uri.

Această politică se aplică tuturor angajaților, colaboratorilor, partenerilor și oricăror alte părți care au acces la datele personale gestionate de clinică. Toți cei implicați în prelucrarea datelor personale sub egida clinicii sunt obligați să respecte principiile și procedurile stabilite în această politică, ca parte a responsabilităților lor.

De asemenea, politica se extinde la toate locațiile și departamentele clinicii, inclusiv filialele și birourile externe, asigurând o abordare unitară și coerentă în ceea ce privește protecția datelor personale în toate operațiunile noastre.

Prin stabilirea acestui domeniu de aplicare, ne asigurăm că toate activitățile de prelucrare a datelor personale realizate sub umbrela clinicii noastre medicale sunt efectuate în conformitate cu cele mai înalte standarde de securitate și confidențialitate, respectând legislația aplicabilă în domeniul protecției datelor.

1.3 Cadru Legal

Politica noastră de protecție a datelor este fundamentată pe un set de reglementări juridice, atât la nivel național cât și european, care guvernează colectarea, utilizarea, divulgarea, transferul și păstrarea datelor personale. În această secțiune, vom detalia principalele acte normative care formează baza legală a politicii noastre și a modului în care prelucrăm datele personale.

Regulamentul General privind Protecția Datelor (GDPR) (Regulamentul (UE) 2016/679): Este piatra de temelie a legislației privind protecția datelor în Uniunea Europeană, aplicabilă din 25 mai 2018. GDPR impune cerințe stricte privind prelucrarea datelor personale și acordă drepturi semnificative subiecților datelor. Clinicile medicale, ca și alte entități care prelucrează date personale, trebuie să asigure conformitatea cu principiile GDPR de legalitate, transparență, minimizare a datelor, exactitate, limitare a stocării, integritate și confidențialitate.

Legea nr. 190/2018 privind măsuri de implementare a GDPR: Această lege oferă clarificări și reguli suplimentare specifice pentru implementarea GDPR în România. Include dispoziții privind rolul și responsabilitățile Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum și proceduri detaliate pentru notificarea încălcărilor de securitate a datelor.

Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date: Deși multe dintre prevederile acestei legi au fost abrogate și înlocuite de GDPR, anumite aspecte specifice rămân relevante pentru

contextul local românesc, în special în ce privește prelucrările de date care nu intră sub incidența dreptului Uniunii Europene.

Legislație secundară și norme specifice sectorului medical: În adiția la legile menționate mai sus, există numeroase reglementări și norme care se aplică prelucrării datelor în contextul medical, inclusiv, dar fără a se limita la, reguli privind confidențialitatea informațiilor medicale, stocarea și arhivarea dosarelor medicale, precum și consimțământul pacienților.

Este esențial ca toate persoanele implicate în prelucrarea datelor personale în cadrul clinicii noastre să înțeleagă și să respecte aceste cadre legale pentru a asigura că activitățile noastre se desfășoară într-un mod care protejează drepturile și libertățile individuale ale subiecților datelor.

Prin alinierea la aceste reglementări, clinica noastră își reafirmă angajamentul față de respectarea standardelor cele mai înalte în materie de protecție a datelor personale și își asumă responsabilitatea de a implementa practici de prelucrare etică și legală a datelor.

2. Definiții

Această secțiune furnizează definiții pentru termenii-cheie utilizați în cadrul acestei politici, asigurând astfel o înțelegere clară și comună a conceptelor esențiale legate de protecția datelor.

Date personale: Orice informații care se referă la o persoană fizică identificată sau identificabilă („subiectul datelor”). O persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, CNP, date de localizare, adresa IP, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.

Prelucrare: Orice operațiune sau set de operațiuni efectuat asupra datelor personale sau asupra seturilor de date personale, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.

Subiectul datelor: Persoana fizică ale cărei date personale sunt prelucrate.

Consimțământul subiectului datelor: Orice manifestare de voință liberă, specifică, informată și neechivocă a subiectului datelor prin care acesta acceptă, printr-o declarație sau printr-o acțiune afirmativă clară, ca datele personale care îl privesc să fie prelucrate.

Controlor de date: Entitatea (persoană fizică sau juridică, autoritate publică, agenție sau alt organism) care, singură sau împreună cu alții, stabilește scopurile și mijloacele de prelucrare a datelor personale.

Procesator de date: Persoana fizică sau juridică, autoritate publică, agenție sau alt organism care prelucrează date personale în numele controlorului de date.

Violare a securității datelor personale: O încălcare a securității care duce la distrugerea accidentală sau ilegală, pierderea, modificarea, divulgarea neautorizată sau accesul la date personale transmise, stocate sau prelucrate în alt mod.

Date speciale (sau categorii speciale de date personale): Date care dezvăluie originea rasială sau etnică, opiniile politice, convingerile religioase sau filozofice, sau apartenența sindicală, și prelucrarea datelor genetice, datelor biometrice în scopul identificării unice a unei persoane fizice, datelor privind sănătatea sau datelor privind viața sexuală sau orientarea sexuală a unei persoane.

Aceste definiții sunt esențiale pentru înțelegerea domeniului de aplicare al politicii noastre de protecție a datelor și a responsabilităților pe care le avem în prelucrarea datelor personale. Prin asigurarea unei baze solide de cunoștințe comune, putem promova cele mai bune practici în toate activitățile noastre de prelucrare a datelor și ne putem îndeplini angajamentele față de confidențialitate și securitate.

3. Principii de Protecție a Datelor

Prelucrarea datelor personale în cadrul clinicii noastre este guvernată de principiile fundamentale stabilite în GDPR și legislația română aplicabilă. Aceste principii ne ghidază în toate activitățile de prelucrare a datelor și asigură că respectăm drepturile și libertățile fundamentale ale persoanelor ale căror date le gestionăm.

3.1 Legalitate, Echitate și Transparență

Legalitate: Toate datele personale trebuie prelucrate pe baza legalității. În practică, acest lucru înseamnă că prelucrarea se va realiza numai dacă și în măsura în care cel puțin una dintre următoarele condiții este îndeplinită: consimțământul subiectului datelor a fost obținut; prelucrarea este necesară pentru executarea unui contract la care subiectul datelor este parte sau pentru a lua măsuri la cererea subiectului datelor înainte de încheierea unui contract; prelucrarea este necesară pentru conformitatea cu o obligație legală; prelucrarea este necesară pentru protejarea intereselor vitale ale subiectului datelor sau ale altei persoane naturale; prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau în exercitarea autorității oficiale; prelucrarea este necesară pentru scopurile intereselor legitime urmărite de controlor sau de o terță parte.

Echitate: Prelucrarea datelor trebuie efectuată într-un mod echitabil. Aceasta înseamnă că subiecții datelor nu ar trebui să fie înșelați sau induși în eroare cu privire la scopurile prelucrării datelor lor personale.

Transparență: Subiecții datelor trebuie informați în mod clar, precis și într-o formă accesibilă despre colectarea și utilizarea datelor lor personale. Informațiile furnizate trebuie să includă identitatea controlorului de date, scopurile prelucrării, destinatarii datelor și drepturile subiectului datelor, inclusiv modul în care pot fi exercitate aceste drepturi.

Respectarea acestui principiu asigură că pacienții și alte persoane implicate sunt informate și că datele lor sunt prelucrate într-un mod care respectă drepturile lor fundamentale. În continuare, politica va detalia aplicarea celorlalte principii fundamentale ale protecției datelor, pentru a asigura o înțelegere cuprinzătoare și practici conforme în toate activitățile noastre de prelucrare.

3.2 Limitarea Scopului

Scopul prelucrării: Datele personale trebuie colectate numai pentru scopuri specifice, explicite și legitime și nu trebuie prelucrate ulterior într-un mod incompatibil cu acele scopuri. Prelucrarea ulterioară pentru arhivare în interes public, pentru cercetare științifică sau istorică sau pentru scopuri statistice nu este considerată incompatibilă cu scopurile inițiale, în conformitate cu GDPR.

Limitarea scopului asigură: că datele personale nu sunt folosite în moduri care nu au fost anticipate sau autorizate de către subiectul datelor. Aceasta contribuie la creșterea încrederii subiecților datelor în modul în care informațiile lor personale sunt gestionate.

Pentru a respecta acest principiu, clinica noastră:

- Definește clar scopurile pentru care datele personale sunt colectate înainte de a începe procesul de colectare.
- Documentează aceste scopuri pentru a asigura o înregistrare clară și pentru a facilita verificarea conformității.
- Se asigură că personalul implicat în colectarea datelor este conștient de aceste scopuri și nu deviază de la ele în activitățile lor de prelucrare.
- Revizuiește și actualizează regulat scopurile prelucrării pentru a se asigura că rămân relevante și justificate.

Orice utilizare a datelor personale în afara scopurilor stabilite necesită o nouă evaluare a legalității prelucrării, inclusiv obținerea unui nou consimțământ de la subiectul datelor, dacă este cazul. Prin urmare, limitarea scopului joacă un rol esențial în protejarea intimității subiecților datelor și în menținerea transparenței și a încrederii în relația dintre clinica noastră și pacienți, angajați și alte părți interesate.

3.3 Minimizarea Datelor

Principiul minimizării datelor stipulează că datele personale colectate și prelucrate trebuie să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile pentru care sunt prelucrate. Acest principiu subliniază importanța de a nu colecta mai multe date decât este absolut necesar pentru îndeplinirea scopurilor specificate.

Pentru a respecta acest principiu, clinica noastră:

- Evaluează în mod regulat tipurile de date personale pe care le colectează pentru a se asigura că numai datele esențiale pentru scopurile prelucrării sunt solicitate și păstrate.

- Implementează proceduri de revizuire și curățare a datelor pentru a elimina orice informații care nu mai sunt necesare pentru scopurile prelucrării.
- Aplică practici de "privacy by design" și "privacy by default", asigurându-se că măsurile de confidențialitate sunt încorporate în toate etapele prelucrării datelor personale și că setările implicite protejează intimitatea subiecților datelor.
- Asigură că personalul implicat în prelucrarea datelor este instruit și conștient de necesitatea de a limita colectarea și stocarea datelor la minimum necesar.

Prin aplicarea principiului minimizării datelor, clinica demonstrează angajamentul său față de respectarea intimității și protecția datelor, reducând riscurile asociate cu gestionarea datelor personale și consolidând încrederea subiecților datelor în practicile noastre de prelucrare. Această abordare minimizată asigură de asemenea o mai bună eficiență și gestionare a resurselor, evitând colectarea și păstrarea inutilă a datelor personale care nu servesc un scop legitim sau necesar.

3.4 Precizie

Principiul preciziei impune ca datele personale să fie exacte și, atunci când este necesar, actualizate; orice date inexacte, având în vedere scopurile pentru care sunt prelucrate, trebuie șterse sau rectificate fără întârziere. Acest principiu este vital pentru asigurarea calității datelor și pentru protecția drepturilor subiecților datelor.

Pentru a respecta acest principiu, clinica noastră:

- Implementează măsuri și proceduri care asigură că toate datele personale colectate și prelucrate sunt exacte și, dacă este necesar, actualizate.
- Oferă subiecților datelor posibilitatea de a verifica datele personale care îi privesc și de a solicita corectarea sau actualizarea acestora, asigurând astfel că datele sunt întotdeauna precise și complete.
- Revizuiește și actualizează datele personale la intervale regulate sau ori de câte ori este informată despre potențiale inexactități.
- Asigură implementarea de tehnici și tehnologii adecvate pentru a facilita precizia datelor, cum ar fi validarea formularului și verificarea periodică a datelor stocate.

Respectarea principiului preciziei este esențială pentru a evita prejudiciile care pot rezulta din prelucrarea datelor personale inexacte sau depășite. Este deosebit de important în domeniul medical, unde datele inexacte pot avea consecințe serioase asupra diagnosticului, tratamentului și îngrijirii pacienților. Prin urmare, clinica noastră se angajează să mențină un nivel înalt de exactitate a datelor personale, contribuind astfel la protejarea sănătății, siguranței și bunăstării pacienților.

3.5 Limitarea Stocării

Principiul limitării stocării prevede că datele personale trebuie să fie păstrate într-o formă care permite identificarea subiecților datelor numai pentru perioada necesară îndeplinirii scopurilor

pentru care datele personale sunt prelucrate. După această perioadă, datele personale trebuie șterse sau anonimizate, astfel încât subiecții datelor să nu mai poată fi identificați.

Pentru a respecta acest principiu, clinica noastră:

- Stabilește și documentează perioade de retenție pentru diferitele categorii de date personale pe care le prelucrează, ținând cont de orice cerințe legale și de nevoile operaționale.
- Revizuiește regulat datele stocate pentru a identifica și elimina informațiile care nu mai sunt necesare pentru scopurile declarate.
- Implementează proceduri de ștergere sigură și efectivă sau de anonimizare a datelor personale atunci când acestea nu mai sunt necesare, asigurând că eliminarea datelor este conformă cu cele mai bune practici și standarde de securitate.
- Informează subiecții datelor despre perioadele de retenție și despre politicile și procedurile de ștergere a datelor, oferind transparență și consolidând încrederea în practicile clinicii.

Acest principiu protejează subiecții datelor împotriva riscurilor asociate cu păstrarea nejustificată a datelor personale, inclusiv accesul neautorizat sau utilizarea abuzivă. Prin limitarea stocării, clinica noastră își demonstrează angajamentul de a gestiona datele personale într-un mod responsabil și de a respecta dreptul la intimitate al pacienților și al altor părți interesate.

3.6 Integritate și Confidențialitate

Principiul integrității și confidențialității impune ca datele personale să fie prelucrate într-un mod care asigură securitatea adecvată a datelor personale, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, distrugerii sau deteriorării accidentale, folosind măsuri tehnice sau organizatorice adecvate.

Pentru a respecta acest principiu, clinica noastră:

- Implementează măsuri tehnice avansate de securitate a datelor, inclusiv criptarea, firewall-urile și detectarea intruziunilor, pentru a proteja datele personale împotriva accesului neautorizat sau a pierderilor accidentale.
- Aplică măsuri organizatorice stricte, cum ar fi politici de confidențialitate, acorduri de nedivulgare și limitarea accesului la datele personale doar pentru personalul autorizat care are nevoie de aceste date pentru îndeplinirea sarcinilor lor.
- Organizează sesiuni regulate de formare și sensibilizare pentru toți angajații cu privire la importanța protecției datelor personale și a confidențialității, asigurându-se că sunt conștienți de responsabilitățile lor și de procedurile de securitate.
- Evaluează și actualizează periodic măsurile de securitate pentru a ține pasul cu evoluțiile tehnologice și cu noile amenințări la adresa securității datelor.

Prin asigurarea integrității și confidențialității datelor personale, clinica noastră își îndeplinește obligația de a proteja datele pacienților și ale angajaților împotriva riscurilor de securitate.

Aceasta contribuie la crearea unui mediu în care subiecții datelor pot avea încredere că informațiile lor personale sunt gestionate cu cea mai mare grijă și respect pentru intimitatea lor.

3.7 Responsabilitate

Principiul responsabilității impune ca entitatea care prelucrează date personale (controlorul) să demonstreze conformitatea cu principiile menționate anterior. Aceasta înseamnă că nu este suficient doar să respecte regulile; controlorul trebuie să fie și capabil să dovedească acest lucru oricând este necesar.

Pentru a respecta acest principiu, clinica noastră:

- Menține documentație detaliată a tuturor activităților de prelucrare a datelor, inclusiv scopul prelucrării, categoriile de date personale prelucrate și orice transferuri de date către țări terțe sau organizații internaționale.
- Implementează și menține politici și proceduri de protecție a datelor pentru a asigura și a demonstra conformitatea cu GDPR și cu alte reglementări relevante.
- Efectuează evaluări regulate ale impactului asupra protecției datelor și consultări cu autoritatea de supraveghere, atunci când este necesar, în special în cazul prelucrărilor care pot prezenta riscuri înalte pentru drepturile și libertățile subiecților datelor.
- Desemnează un Ofițer de Protecție a Datelor (OPD) responsabil cu supravegherea conformității cu legislația privind protecția datelor, gestionarea cererilor subiecților datelor și cooperarea cu autoritățile de protecție a datelor.
- Asigură că toate măsurile tehnice și organizatorice sunt revizuite și actualizate periodic pentru a reflecta cele mai bune practici și pentru a menține securitatea datelor la cele mai înalte standarde.

Prin adoptarea principiului responsabilității, clinica noastră își afirmă angajamentul de a fi transparentă, de a menține o atitudine proactivă în protecția datelor personale și de a pune respectarea drepturilor subiecților datelor în centrul activităților sale. Aceasta implică o abordare continuă de îmbunătățire a măsurilor de protecție a datelor și o comunicare deschisă cu subiecții datelor și autoritățile de reglementare.

4. Roluri și Responsabilități

În cadrul politicii noastre de protecție a datelor, este esențial să definim clar rolurile și responsabilitățile fiecărei părți implicate în prelucrarea datelor personale. Această structură asigură că toate procesele legate de datele personale sunt gestionate într-un mod responsabil și conform cu legislația aplicabilă.

4.1 Responsabilitățile Ofițerului de Protecție a Datelor (OPD)

Clinica noastră a desemnat un Ofițer de Protecție a Datelor (OPD) care servește ca punct central de expertiză și consiliere pe teme legate de protecția datelor. Responsabilitățile OPD includ:

- **Supravegherea conformității:** Monitorizează și asigură respectarea GDPR și a altor reglementări legale în materie de protecție a datelor, precum și a politicii interne de protecție a datelor.
- **Consiliere:** Oferă consultanță și recomandări personalului clinic și managementului privind cele mai bune practici în protecția datelor și pe teme legate de prelucrarea datelor personale.
- **Instruire:** Organizează sesiuni de formare și sensibilizare pentru angajați, pentru a le îmbunătăți înțelegerea și abilitățile legate de protecția datelor personale.
- **Evaluări ale Impactului asupra Protecției Datelor (EIPD):** Conduce sau supervisează efectuarea de evaluări ale impactului asupra protecției datelor pentru prelucrările care prezintă riscuri înalte pentru drepturile și libertățile subiecților datelor.
- **Punct de contact:** Servește ca punct de contact pentru subiecții datelor care au întrebări sau solicitări legate de prelucrarea datelor lor personale și cooperează cu autoritatea de supraveghere (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal din România).

Rolul OPD este vital pentru asigurarea unei abordări coerente și eficiente a protecției datelor în cadrul clinicii noastre. Acesta contribuie la crearea unei culturi a protecției datelor și la consolidarea încrederii subiecților datelor că informațiile lor personale sunt tratate cu cel mai înalt grad de securitate și respect.

4.2 Responsabilitățile Personalului

Toți angajații clinicii noastre sunt responsabili pentru respectarea politicii de protecție a datelor și a legislației aplicabile. Fiecare membru al personalului joacă un rol crucial în protejarea datelor personale și în prevenirea încălcărilor de securitate. Responsabilitățile specifice includ:

- **Conștientizarea:** Toți angajații trebuie să fie conștienți de politica de protecție a datelor a clinicii și de procedurile relevante pentru rolul lor. Este esențial să înțeleagă importanța protecției datelor personale și impactul potențial al activităților lor asupra securității datelor.
- **Formare:** Angajații trebuie să participe la sesiunile de formare organizate de clinică sau de Ofițerul de Protecție a Datelor (OPD) și să se asigure că înțeleg bunele practici și cerințele legale în materie de protecție a datelor.
- **Protecția datelor în activitățile zilnice:** Este responsabilitatea fiecărui angajat să aplice principiile de protecție a datelor în toate activitățile de prelucrare a datelor la care participă, inclusiv minimizarea datelor, asigurarea preciziei datelor și protejarea confidențialității și integrității datelor.
- **Raportarea încălcărilor de securitate:** Angajații trebuie să raporteze orice incidente de securitate sau potențiale încălcări ale protecției datelor imediat către OPD sau către superiorul lor direct. Acest lucru permite clinicii să răspundă rapid și să minimizeze orice potențial impact negativ asupra subiecților datelor.
- **Respectarea procedurilor de acces:** Accesul la datele personale trebuie să se limiteze la personalul autorizat, în funcție de necesitățile specifice ale rolului lor. Angajații trebuie să respecte procedurile stabilite pentru accesul la date și pentru utilizarea sistemelor de informații ale clinicii.

Prin îndeplinirea acestor responsabilități, personalul contribuie semnificativ la crearea unui mediu sigur pentru datele personale gestionate de clinică și la întărirea încrederii subiecților datelor în angajamentul nostru de a proteja confidențialitatea și securitatea informațiilor lor.

4.3 Responsabilitățile Procesatorului de Date

Procesatorii de date sunt entități terțe care prelucrează date personale în numele clinicii, sub directiva și autoritatea acesteia. Aceștia pot include furnizori de servicii IT, companii de arhivare documente, firme de contabilitate și alte entități care pot avea acces sau pot gestiona date personale în cadrul activităților lor desfășurate pentru clinică. Responsabilitățile lor includ:

- **Conformitate cu instrucțiunile:** Procesatorii de date trebuie să prelucreze datele personale exclusiv conform instrucțiunilor primite de la clinică, controlorul de date. Ei nu au voie să utilizeze datele pentru propriile scopuri sau într-un mod care deviază de la instrucțiunile primite.
- **Securitatea datelor:** Trebuie să implementeze măsuri tehnice și organizatorice adecvate pentru a asigura un nivel de securitate corespunzător riscului prelucrării, protejând datele împotriva prelucrărilor neautorizate sau ilegale și împotriva pierderii, distrugerii sau deteriorării accidentale.
- **Sub-procesatorii:** În cazul în care procesatorii de date decid să subcontracteze orice parte din activitatea de prelucrare a datelor, trebuie să obțină în prealabil aprobarea scrisă a clinicii și să impună aceloraşi condiții de protecție a datelor sub-procesatorilor.
- **Notificarea încălcărilor de securitate:** Procesatorii sunt obligați să notifice clinica imediat ce devin conștienți de orice încălcare a securității datelor personale, pentru a permite clinicii să ia măsurile necesare și să îndeplinească obligațiile de raportare.
- **Asistență pentru conformitate:** Trebuie să asiste clinica în îndeplinirea obligațiilor sale legate de securitatea prelucrării, notificarea încălcărilor de securitate, evaluările impactului asupra protecției datelor și consultările prealabile cu autoritățile de supraveghere.
- **Ștergerea sau returnarea datelor:** La încheierea serviciilor, procesatorii de date trebuie să șteargă sau să returneze datele personale clinicii, la alegerea acesteia, și să distrugă orice copii, cu excepția cazului în care legislația impune stocarea datelor.

Prin respectarea acestor responsabilități, procesatorii de date joacă un rol esențial în protecția datelor personale și în asigurarea conformității continue a clinicii cu reglementările privind protecția datelor. Colaborarea strânsă și transparentă între clinică și procesatorii săi de date este crucială pentru menținerea unui standard înalt de protecție a datelor personale ale pacienților și angajaților.

5. Drepturile Subiecților Datelor

Politica noastră de protecție a datelor recunoaște și respectă drepturile subiecților datelor conform GDPR și legislației locale. Aceste drepturi sunt esențiale pentru asigurarea controlului persoanelor asupra datelor lor personale și consolidarea încrederii în practicile noastre de prelucrare a datelor.

5.1 Dreptul la Informare

Subiecții datelor au dreptul de a fi informați despre colectarea și utilizarea datelor lor personale. Aceasta include furnizarea de informații clare, transparente și ușor accesibile despre identitatea controlorului de date, scopurile prelucrării, destinatarii datelor, perioada de stocare și drepturile de care dispun subiecții datelor.

Pentru a asigura respectarea dreptului la informare, clinica noastră:

- Oferă subiecților datelor notificări de confidențialitate sau declarații privind protecția datelor la momentul colectării datelor personale. Acestea sunt concepute să fie concise, transparente, inteligibile și ușor accesibile.
- Include informații despre dreptul subiecților datelor de a avea acces la datele lor, de a le rectifica, șterge, restricționa prelucrarea, de a se opune prelucrării și de a solicita portabilitatea datelor.
- Informează subiecții datelor despre posibilitatea de a retrage consimțământul în orice moment, în cazul în care prelucrarea se bazează pe consimțământ.
- Oferă detalii despre cum să contacteze Ofițerul de Protecție a Datelor (OPD) și cum să depună o plângere la autoritatea de supraveghere, dacă subiecții datelor consideră că prelucrarea datelor lor personale încalcă GDPR.

Asigurându-ne că subiecții datelor sunt bine informați, le împuternicim să-și exercite drepturile și sporim transparența și responsabilitatea în toate activitățile noastre de prelucrare a datelor. Această abordare contribuie la crearea unei relații de încredere între clinică și pacienți, angajați și alte părți interesate.

5.2 Dreptul de Acces

Subiecții datelor au dreptul de a obține confirmarea dacă datele personale care îi privesc sunt sau nu prelucrate și, dacă da, acces la aceste date și la informații suplimentare legate de prelucrarea lor. Aceste informații includ scopul prelucrării, categoriile de date personale vizate, destinatarii sau categoriile de destinatari cărora le-au fost sau le vor fi dezvăluite datele, perioada previzionată pentru care vor fi stocate datele, existența dreptului de a solicita rectificarea sau ștergerea datelor sau restricționarea prelucrării, dreptul de a depune o plângere la o autoritate de supraveghere, și sursa datelor dacă nu sunt colectate direct de la subiect.

Pentru a asigura respectarea dreptului de acces, clinica noastră:

- Furnizează un mecanism simplu prin care subiecții datelor pot să își exercite dreptul de acces, de obicei prin solicitare scrisă adresată Ofițerului de Protecție a Datelor sau printr-un portal securizat online, dacă este disponibil.
- Răspunde la solicitările de acces fără întârzieri nejustificate și în orice caz în termen de o lună de la primirea solicitării, perioadă care poate fi prelungită cu încă două luni în cazurile complexe, cu condiția informării subiectului datelor despre această prelungire și motivele întârzierii.

- Oferă o copie gratuită a datelor personale care sunt prelucrate. Pentru orice copii suplimentare solicitate de subiectul datelor, clinica poate percepe o taxă rezonabilă bazată pe costurile administrative.
- Asigură că informațiile furnizate sunt într-un format clar și accesibil, utilizând limbaj simplu, în special atunci când informațiile sunt adresate unui copil.

Prin facilitarea accesului la datele personale și prin oferirea de informații transparente despre prelucrarea acestora, clinica își demonstrează angajamentul față de principiile de deschidere și responsabilitate. Respectarea dreptului de acces îi împuternicește pe subiecții datelor și le permite să își înțeleagă și să își gestioneze mai bine intimitatea.

5.3 Dreptul la Rectificare

Subiecții datelor au dreptul de a obține, fără întârzieri nejustificate, rectificarea datelor personale inexacte care îi privesc. În plus, având în vedere scopurile prelucrării, au dreptul de a avea completate datele personale care sunt incomplete, inclusiv prin furnizarea unei declarații suplimentare.

Pentru a asigura respectarea dreptului la rectificare, clinica noastră:

- Oferă subiecților datelor proceduri clare și accesibile pentru a solicita rectificarea datelor lor personale. Aceste solicitări pot fi făcute verbal sau în scris și sunt adesea adresate Ofițerului de Protecție a Datelor.
- Procesează solicitările de rectificare fără întârzieri nejustificate și, în orice caz, în termen de o lună de la primirea solicitării. Acest termen poate fi prelungit cu încă două luni în cazurile complexe, cu condiția informării subiectului datelor despre această prelungire și motivele întârzierii.
- În cazul în care clinica a divulgat datele personale în cauză către terți, ia măsuri rezonabile pentru a informa acei terți despre orice rectificare efectuată, în măsura în care acest lucru este posibil și nu implică eforturi disproporționate.
- Informează subiectul datelor despre rectificările efectuate și despre terții cărora li s-au divulgat datele, dacă acest lucru este solicitat.

Respectând dreptul la rectificare, clinica demonstrează angajamentul său față de menținerea acurateței datelor personale și își împuternicește pacienții și angajații să se asigure că informațiile lor sunt corecte și actualizate. Această practică nu numai că îmbunătățește calitatea datelor, dar și sprijină exercitarea altor drepturi de către subiectul datelor, cum ar fi dreptul la restricționarea prelucrării sau dreptul de a fi uitat.

5.4 Dreptul la Ștergere („Dreptul de a fi Uitat”)

Subiecții datelor au dreptul de a obține ștergerea datelor personale care îi privesc fără întârzieri nejustificate în anumite circumstanțe, inclusiv când datele personale nu mai sunt necesare în raport cu scopurile pentru care au fost colectate sau prelucrate, când subiectul datelor își retrage consimțământul pe care se bazează prelucrarea și când nu există alt temei juridic pentru prelucrare, când subiectul datelor se opune prelucrării și nu există motive legitime care să

prevaleze, când datele personale au fost prelucrate ilegal, sau când datele personale trebuie șterse pentru respectarea unei obligații legale.

Pentru a asigura respectarea dreptului la ștergere, clinica noastră:

- Oferă subiecților datelor proceduri simplificate pentru a solicita ștergerea datelor personale, fie prin contactarea directă a Ofițerului de Protecție a Datelor, fie prin alte mijloace puse la dispoziție de clinică.
- Evaluează fiecare solicitare de ștergere în contextul condițiilor specifice prevăzute de GDPR și legislația locală, pentru a determina eligibilitatea pentru ștergere.
- Procesează solicitările de ștergere în termen de o lună, informând subiectul datelor despre acțiunile întreprinse sau, dacă este cazul, motivele întârzierii sau refuzului de a acționa.
- În cazul în care clinica a divulgat datele personale în cauză către terți și ștergerea este justificată, ia măsuri rezonabile pentru a-i informa pe terți despre solicitarea de ștergere, astfel încât să șteargă orice link către acele date personale sau copii ale acestora.

Dreptul la ștergere oferă subiecților datelor un mijloc important de a controla datele lor personale, permițându-le să solicite eliminarea informațiilor care nu mai sunt necesare sau care au fost prelucrate ilegal. Acest drept consolidează transparența și încrederea în practicile de prelucrare a datelor ale clinicii, asigurându-se că datele personale sunt gestionate într-un mod responsabil și respectuos.

5.5 Dreptul de a Restrictiona Prelucrarea

Subiecții datelor au dreptul de a obține restricționarea prelucrării datelor personale în anumite circumstanțe. Aceasta înseamnă că prelucrarea datelor este limitată, astfel încât datele pot fi stocate, dar nu și prelucrate în alte moduri fără consimțământul subiectului datelor. Dreptul la restricționare se aplică în următoarele cazuri:

- Când exactitatea datelor personale este contestată de subiectul datelor, pentru o perioadă care permite controlorului să verifice exactitatea datelor.
- Când prelucrarea este ilegală, iar subiectul datelor se opune ștergerii datelor personale și solicită în schimb restricționarea utilizării lor.
- Când controlorul nu mai are nevoie de datele personale pentru scopurile prelucrării, dar subiectul datelor le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanță.
- Când subiectul datelor s-a opus prelucrării pe baza interesului legitim al controlorului, în așteptarea verificării dacă motivele legitime ale controlorului prevalează asupra celor ale subiectului datelor.

Pentru a asigura respectarea dreptului de a restricționa prelucrarea, clinica noastră:

- Oferă subiecților datelor mijloace accesibile pentru a solicita restricționarea prelucrării, cum ar fi formulare online, e-mail sau contact direct cu Ofițerul de Protecție a Datelor.
- Evaluează fiecare solicitare în contextul condițiilor menționate și aplică restricții acolo unde este justificat, informând subiectul datelor despre decizie.

- Marchează datele personale afectate în sistemele noastre pentru a asigura că restricționarea prelucrării este respectată efectiv, limitând accesul și prelucrarea ulterioară a acestor date.
- Informează orice terți cărora li s-au divulgat datele personale despre restricționarea prelucrării, cu excepția cazului în care acest lucru se dovedește imposibil sau presupune un efort disproporționat.

Prin aplicarea dreptului de a restricționa prelucrarea, clinica noastră demonstrează un angajament puternic față de respectarea autonomiei și preferințelor subiecților datelor în ceea ce privește gestionarea informațiilor lor personale. Această abordare crește încrederea subiecților datelor în politica și practicile noastre de protecție a datelor, consolidând astfel relația dintre clinică și clienții săi.

5.6 Dreptul la Portabilitatea Datelor

Dreptul la portabilitatea datelor oferă subiecților datelor posibilitatea de a primi datele personale care îi privesc și pe care le-au furnizat unui controlor, într-un format structurat, utilizat în mod curent și care poate fi citit automat, și de a transmite aceste date unui alt controlor fără obstacole din partea controlorului căruia i-au fost furnizate datele, în condițiile în care:

- Prelucrarea se bazează pe consimțământ sau pe un contract; și
- Prelucrarea este efectuată prin mijloace automatizate.

Această facilitate este deosebit de relevantă în era digitală, asigurându-le persoanelor controlul asupra datelor lor într-un mediu digital, facilitând mobilitatea datelor între diferiți furnizori de servicii.

Pentru a asigura respectarea dreptului la portabilitatea datelor, clinica noastră:

- Înțelege și identifică datele personale care se încadrează sub domeniul de aplicare al dreptului la portabilitate și stabilește procese pentru a facilita transferul efectiv al acestor date la solicitarea subiectului datelor.
- Oferă informații și suport subiecților datelor privind modul în care pot exercita acest drept, inclusiv detalii despre formatul în care vor fi furnizate datele.
- Se asigură că datele personale sunt furnizate subiectului datelor sau transferate direct unui alt controlor, după caz, într-un mod sigur, protejând integritatea și confidențialitatea datelor în proces.
- Răspunde la solicitările de portabilitate în termen de o lună de la primire, perioadă care poate fi prelungită în funcție de complexitatea solicitării sau de numărul de cereri, asigurându-se că subiectul datelor este informat corespunzător.

Implementând dreptul la portabilitatea datelor, clinica demonstrează angajamentul său față de respectarea și împuternicirea pacienților și a altor subiecți ai datelor în era informațională, facilitând o mai bună controlabilitate și autonomie asupra datelor lor personale.

5.7 Dreptul de Opoziție

Subiecții datelor au dreptul de a se opune, în orice moment, din motive legate de situația lor particulară, la prelucrarea datelor personale care îi privesc, inclusiv la profilare, în măsura în care prelucrarea este bazată pe interesul legitim al controlorului sau pe îndeplinirea unei sarcini care servește interesului public sau în exercitarea autorității oficiale. De asemenea, subiecții datelor au dreptul de a se opune prelucrării datelor personale în scopuri de marketing direct, inclusiv profilare, în măsura în care este legată de marketingul direct.

Pentru a asigura respectarea dreptului de opoziție, clinica noastră:

- Informează subiecții datelor despre dreptul lor de opoziție într-un moment clar și separat de colectarea datelor, de obicei la prima comunicare cu subiectul datelor.
- Oferă un mecanism simplu și accesibil pentru exercitarea dreptului de opoziție, asigurându-se că subiecții datelor pot exercita acest drept fără dificultate.
- Procesează solicitările de opoziție fără întârzieri nejustificate și încetează prelucrarea datelor personale pentru scopul împotriva căruia s-a exprimat opoziția, cu excepția cazurilor în care controlorul poate demonstra motive legitime și convingătoare pentru prelucrare care prevalează asupra intereselor, drepturilor și libertăților subiectului datelor sau pentru constatarea, exercitarea sau apărarea unui drept în instanță.
- Încetează imediat prelucrarea datelor personale în scopuri de marketing direct atunci când subiectul datelor își exprimă opoziția la o astfel de prelucrare.

Implementând eficient dreptul de opoziție, clinica își manifestă respectul față de preferințele și drepturile individuale ale subiecților datelor, consolidând încrederea și transparența în relațiile cu pacienții și alte părți interesate. Acest drept le permite subiecților datelor să aibă un cuvânt de spus în modul în care informațiile lor personale sunt utilizate, oferindu-le o mai mare control asupra propriei intimități.

5.8 Drepturi legate de Decizia Automatizată și Profilare

Subiecții datelor au dreptul de a nu fi supuși unei decizii bazate exclusiv pe prelucrarea automată, inclusiv profilarea, care produce efecte juridice care îi privesc sau îi afectează în mod similar într-o măsură semnificativă. Acest drept asigură că subiecții datelor pot solicita intervenția umană în procesul decizional, pot exprima punctul de vedere și pot contesta decizia.

Pentru a asigura respectarea acestor drepturi, clinica noastră:

- Informează subiecții datelor în mod clar și transparent despre orice utilizare a deciziilor automate, inclusiv profilarea, în momentul colectării datelor personale, furnizând detalii despre logica implicată, semnificația și consecințele preconizate ale unei astfel de prelucrări pentru subiectul datelor.
- Implementează mecanisme prin care subiecții datelor pot solicita revizuirea deciziilor luate exclusiv pe baza prelucrării automate. Acest lucru include asigurarea că există o intervenție umană semnificativă în procesul decizional, acolo unde este necesar.
- Oferă subiecților datelor posibilitatea de a-și exprima punctul de vedere și de a contesta decizia automată, asigurându-se că primesc o justificare clară pentru decizia luată și că au acces la informații despre pașii pe care îi pot urma pentru a contesta decizia.

- Evaluează și validează periodic sistemele de prelucrare automată pentru a asigura că nu sunt părtinitoare și nu au un impact negativ nejustificat asupra subiecților datelor.

Prin respectarea acestor drepturi, clinica își demonstrează angajamentul de a folosi tehnologiile de prelucrare a datelor într-un mod care respectă autonomia și drepturile subiecților datelor, promovând transparența și responsabilitatea în toate activitățile sale de prelucrare. Acest lucru ajută la construirea unei relații de încredere între clinică și pacienți, asigurându-se că tehnologia este folosită într-un mod care servește interesul pacienților și respectă drepturile lor fundamentale.

6. Procedurile de Colectare a Datelor

Pentru a asigura conformitatea cu GDPR și legislația națională în vigoare, clinica noastră medicală adoptă proceduri stricte în ceea ce privește colectarea datelor personale. Aceste proceduri sunt concepute pentru a proteja confidențialitatea și integritatea informațiilor personale ale pacienților, angajaților și altor părți interesate, încă de la momentul colectării acestora.

6.1 Consimțământul

Consimțământul reprezintă o bază juridică esențială pentru prelucrarea datelor personale în cadrul activităților noastre medicale. Este crucial să obținem consimțământul explicit și informat al subiecților datelor înainte de colectarea și prelucrarea datelor lor personale, în special când este vorba de datele sensibile legate de sănătate.

Obținerea Consimțământului:

- **Claritatea și Specificitatea:** Consimțământul trebuie să fie obținut printr-o declarație sau printr-o acțiune afirmativă clară care indică acordul subiectului datelor privind prelucrarea datelor personale. Termenii și condițiile trebuie să fie exprimați într-o manieră clară și accesibilă, fără a utiliza limbaj juridic complicat.
- **Informarea:** Subiecții datelor sunt informați în mod explicit despre identitatea controlorului de date (clinica), scopul prelucrării, tipurile de date colectate, dreptul de retragere a consimțământului în orice moment și orice alte informații relevante pentru a asigura o decizie informată.
- **Date Sensibile:** Având în vedere natura sensibilă a datelor personale legate de sănătate, clinica aplică o atenție sporită în asigurarea că consimțământul este specific și informat, acoperind scopurile exacte pentru care datele sunt prelucrate.

Documentarea Consimțământului:

- **Evidența Consimțământurilor:** Clinica păstrează o evidență clară a consimțământurilor obținute, inclusiv informații despre momentul obținerii consimțământului, metoda utilizată pentru colectare și detalii despre informațiile furnizate subiecților datelor în acel moment.
- **Revizuire și Actualizare:** Consimțământul este revizuit periodic pentru a se asigura că rămâne relevant și actualizat în raport cu scopurile prelucrării. Subiecții datelor sunt

informați despre orice modificări semnificative care ar putea afecta baza juridică a prelucrării datelor personale.

Retragerea Consimțământului:

- **Ușurința Retragerii:** Clinica asigură că subiecții datelor pot să își retragă consimțământul la fel de ușor pe cât l-au oferit. Mecanismele de retragere a consimțământului sunt accesibile și simplu de utilizat, fără a impune subiecților datelor sarcini nejustificate.

6.2 Colectarea Datelor de la Minori

În contextul serviciilor medicale, colectarea datelor de la minori necesită o atenție specială, dat fiind că minorii sunt considerați subiecți vulnerabili în cadrul GDPR. Clinica noastră medicală adoptă proceduri specifice pentru a asigura protecția adecvată a datelor personale ale minorilor.

Obținerea Consimțământului Părinților sau Tutorilor Legali:

- **Vârsta Consimțământului:** Conform legislației locale și a GDPR, pentru serviciile oferite direct minorilor, clinica trebuie să obțină consimțământul părinților sau al tutorilor legali pentru subiecții cu vârsta sub un anumit prag (de exemplu, 16 ani, sau vârsta specifică stabilită de legislația națională).
- **Verificarea Vârstei și a Consimțământului:** Clinica implementează măsuri adecvate pentru a verifica vârsta subiectului datelor și pentru a confirma că consimțământul a fost oferit sau autorizat de către deținătorul responsabilității părintești asupra minorului.

Informarea și Comunicarea Adaptată:

- **Comunicare Clară și Accesibilă:** Toate informațiile legate de prelucrarea datelor personale ale minorilor sunt furnizate într-un limbaj simplu și clar, adaptat vârstei și capacității de înțelegere a minorului, pentru a asigura că atât minorii, cât și părinții sau tutorii lor înțeleg scopul și implicațiile prelucrării.
- **Drepturi Specifice Minorilor:** Clinica recunoaște și promovează drepturile specifice ale minorilor în ceea ce privește protecția datelor, inclusiv dreptul de acces, rectificare, ștergere și opoziție, asigurând mecanisme adecvate pentru exercitarea acestor drepturi de către părinți sau tutori.

Utilizarea Datelor în Interesul Cel Mai Bun al Minorului:

- **Interesul Superior al Copilului:** Toate deciziile legate de prelucrarea datelor personale ale minorilor sunt luate cu considerarea primordială a intereselor superioare ale copilului, conform principiilor stabilite în Convenția cu privire la Drepturile Copilului.
- **Limitarea Scopului și Minimizarea Datelor:** Clinica se asigură că datele personale ale minorilor sunt colectate și prelucrate exclusiv pentru scopuri legate direct de furnizarea de servicii medicale și sunt limitate la ceea ce este strict necesar pentru realizarea acestor scopuri.

Prin aplicarea acestor proceduri specifice, clinica noastră medicală își demonstrează angajamentul față de protejarea drepturilor și bunăstarea minorilor în contextul prelucrării datelor personale, respectând în același timp cerințele legale și etice. Aceste măsuri contribuie la crearea unui mediu sigur și încrezător pentru minori și familiile lor, în care confidențialitatea și integritatea datelor personale sunt protejate cu cea mai mare grijă.

6.3 Categorii Speciale de Date

În calitate de clinică medicală, suntem conștienți de sensibilitatea crescută a datelor personale legate de sănătate pe care le prelucrăm. Aceste date sunt clasificate ca „categorii speciale de date personale" sub GDPR și sunt supuse unor reguli stricte pentru a asigura protecția maximă a intimității și a drepturilor subiecților datelor.

Politica Noastră de Prelucrare a Datelor de Sănătate:

- **Baza Legală:** Prelucrăm datele de sănătate doar atunci când este strict necesar pentru furnizarea de servicii medicale și în baza unei baze legale solide, cum ar fi consimțământul explicit al pacientului, necesitatea pentru diagnosticul medical, furnizarea de îngrijire sau tratament medical, sau gestionarea serviciilor de sănătate.
- **Confidențialitatea și Securitatea:** Implementăm cele mai înalte standarde de confidențialitate și securitate pentru a proteja datele de sănătate ale pacienților noștri. Aceasta include criptarea datelor, accesul securizat bazat pe roluri și monitorizarea constantă a sistemelor noastre de IT pentru a preveni orice acces neautorizat sau scurgeri de date.
- **Minimizarea Datelor:** Colectăm și prelucrăm doar datele de sănătate strict necesare pentru scopurile specifice pentru care sunt prelucrate. Orice date care nu sunt esențiale pentru furnizarea serviciilor medicale sunt excluse din colectare și prelucrare.
- **Conservarea Datelor:** Stabilim perioade clare de reținere pentru datele de sănătate, ținând cont de cerințele legale și de necesitatea pentru îngrijirea continuă a pacientului. După aceste perioade, datele sunt fie șterse în mod sigur, fie anonimizate pentru utilizare în cercetare medicală sau statistici, dacă pacientul a consimțit explicit pentru acest scop.

Informarea Pacienților:

- **Transparență:** Oferim pacienților noștri informații clare și accesibile despre prelucrarea datelor lor de sănătate la momentul colectării. Aceasta include scopul prelucrării, baza legală, drepturile lor în legătură cu datele personale și modalitățile de exercitare a acestor drepturi.
- **Dreptul de Acces și Control:** Asigurăm că pacienții au acces ușor la datele lor de sănătate și pot solicita rectificarea sau ștergerea datelor inexacte sau perimate. De asemenea, recunoaștem dreptul pacienților de a se opune prelucrării datelor lor de sănătate în anumite circumstanțe și de a solicita limitarea prelucrării sau portabilitatea datelor.

Prin aceste măsuri, ne asumăm responsabilitatea de a proteja datele personale sensibile ale pacienților noștri, respectând în același timp drepturile și libertățile lor. Ne angajăm să menținem un nivel înalt de confidențialitate și integritate în toate practicile noastre de prelucrare a datelor,

asigurându-ne că serviciile medicale pe care le furnizăm sunt efectuate într-un cadru sigur și protejat pentru toți pacienții noștri.

7. Utilizarea și Prelucrarea Datelor

La clinica noastră, utilizarea și prelucrarea datelor personale sunt efectuate cu cea mai mare atenție și respect pentru confidențialitatea și intimitatea pacienților și angajaților noștri. Înțelegem responsabilitatea semnificativă pe care o avem în gestionarea acestor date, în special când sunt implicate date sensibile legate de sănătate.

7.1 Legalitatea Prelucrării

Prelucrăm datele personale doar atunci când avem o bază legală solidă pentru a face acest lucru. Aceste baze legale includ consimțământul pacientului, necesitatea pentru executarea unui contract (de exemplu, contracte de muncă pentru angajații noștri), obligațiile legale (cum ar fi raportările obligatorii către autoritățile de sănătate publică), protejarea intereselor vitale ale pacienților sau ale altor persoane, realizarea unui interes legitim al clinicii sau al unei terțe părți, și executarea sarcinilor în interes public sau în exercitarea autorității oficiale.

Implementarea Legalității Prelucrării:

- **Consimțământul:** Obținem consimțământul explicit al pacienților înainte de a prelucra datele lor personale pentru orice scopuri care nu sunt direct legate de furnizarea serviciilor medicale sau de îndeplinirea unui contract. Pacienții au dreptul de a-și retrage consimțământul în orice moment.
- **Contractual:** Prelucrarea datelor este adesea necesară pentru îndeplinirea obligațiilor contractuale, cum ar fi furnizarea de servicii medicale la cererea pacienților sau îndeplinirea obligațiilor față de angajați.
- **Obligații Legale:** Respectăm toate obligațiile legale de raportare și de altă natură, ceea ce poate necesita prelucrarea și divulgarea anumitor date personale către autorități.
- **Interese Vitale:** În situații de urgență, putem prelucra datele personale pentru a proteja interesele vitale ale pacienților sau ale altor persoane.
- **Interes Legitim:** În anumite cazuri, prelucrăm date personale sub baza unui interes legitim, care poate include activități administrative, de securitate internă sau de marketing, asigurându-ne că interesele și drepturile fundamentale ale subiecților datelor nu sunt suprimate.

Asigurarea Conformității:

- **Evaluarea Impactului asupra Protecției Datelor (EIPD):** Pentru activitățile de prelucrare care prezintă riscuri înalte pentru drepturile și libertățile subiecților datelor, efectuăm EIPD-uri pentru a identifica și a atenua riscurile.
- **Politici și Proceduri:** Avem politici și proceduri bine stabilite pentru toate aspectele prelucrării datelor personale, asigurându-ne că toate activitățile noastre de prelucrare respectă legile aplicabile privind protecția datelor.

- **Formare și Conștientizare:** Oferim formare regulată angajaților noștri pentru a asigura o înțelegere profundă a responsabilităților lor în ceea ce privește protecția datelor și pentru a promova o cultură a confidențialității în întreaga noastră organizație.

Prin respectarea strictă a acestor principii și proceduri, ne asigurăm că utilizarea și prelucrarea datelor personale în clinica noastră se face într-un mod responsabil și conform cu cele mai înalte standarde de confidențialitate și integritate, protejând drepturile și libertățile pacienților și angajaților noștri.

7.2 Partajarea și Transferul Datelor

Conștienți de importanța și sensibilitatea datelor personale cu care lucrăm, abordăm cu seriozitate partajarea și transferul acestor date, asigurându-ne că respectăm legislația aplicabilă în materie de protecție a datelor, inclusiv GDPR. Acest lucru este deosebit de relevant în contextul furnizării de servicii medicale, unde colaborarea și schimbul de informații pot fi esențiale pentru îngrijirea pacientului.

Politici și Proceduri pentru Partajarea Datelor:

- **Bazele Legale:** Ne asigurăm că orice partajare sau transfer de date personale se bazează pe o bază legală solidă, precum consimțământul pacientului, necesitatea pentru îndeplinirea unui contract, obligațiile legale sau interesul legitim.
- **Acorduri de Prelucrare a Datelor:** Încheiem acorduri stricte de prelucrare a datelor cu toți partenerii și terții părți care pot avea acces la datele personale ale pacienților sau angajaților, asigurându-ne că aceste părți respectă standarde echivalente de protecție și confidențialitate.
- **Transferuri Internaționale:** În cazul transferurilor de date personale în afara Spațiului Economic European (SEE), luăm măsuri suplimentare pentru a asigura protecția datelor, cum ar fi utilizarea clauzelor contractuale standard aprobate de Comisia Europeană sau asigurarea că destinatarii datelor se conformează cadrelor de protecție a datelor recunoscute internațional, precum Scutul de Confidențialitate UE-SUA.

Partajarea Datelor cu Furnizori de Servicii Medicale și Alți Specialiști:

- **Îngrijire Coordonată:** Pentru a oferi cea mai bună îngrijire posibilă, este adesea necesar să partajăm datele personale ale pacienților cu alți furnizori de servicii medicale, cum ar fi laboratoare, specialiști sau spitale. Acest lucru se face numai cu consimțământul explicit al pacientului sau atunci când este necesar pentru interesul vital al pacientului.
- **Securitatea Datelor în Partajare:** Implementăm protocoale stricte pentru transferul securizat al datelor, inclusiv criptarea datelor în tranzit, pentru a preveni accesul neautorizat sau pierderea informațiilor.

Informarea Pacienților:

- **Transparență:** Pacienții sunt informați despre partajarea datelor lor personale, inclusiv identitatea destinatarilor, scopurile partajării și orice transferuri internaționale de date.

Aceasta permite pacienților să înțeleagă cum și de ce sunt utilizate datele lor personale, consolidând încrederea în practicile noastre.

Prin respectarea acestor principii și proceduri detaliate, ne angajăm să protejăm confidențialitatea și securitatea datelor personale în toate activitățile noastre de partajare și transfer. Înțelegem că aceste date nu sunt doar informații; ele reprezintă încrederea pe care pacienții și angajații noștri o plasează în noi, iar protejarea acestei încrederi este o responsabilitate pe care o luăm cu cea mai mare seriozitate.

7.3 Acorduri de Prelucrare a Datelor

Pentru a asigura conformitatea cu GDPR și legislația locală în domeniul protecției datelor, clinica noastră medicală stabilește acorduri de prelucrare a datelor cu toți terții părți care prelucrează date personale în numele nostru. Aceste acorduri sunt esențiale pentru a menține controlul asupra modului în care sunt gestionate datele personale și pentru a asigura că toate părțile implicate respectă standardele stricte de protecție a datelor.

Elemente Cheie ale Acordurilor de Prelucrare a Datelor:

- **Obiectul și Durata Prelucrării:** Acordul detaliază natura și scopul specific al prelucrării, durata prelucrării și tipurile de date personale și categoriile de subiecți ai datelor implicați.
- **Obligațiile și Drepturile Controlorului:** Se clarifică faptul că controlorul de date (clinica) păstrează controlul asupra datelor personale și stabilește obligațiile procesatorului de date conform instrucțiunilor primite de la controlor.
- **Măsuri de Securitate:** Procesatorul de date este obligat să implementeze măsuri tehnice și organizatorice adecvate pentru a asigura un nivel de securitate corespunzător riscului, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, distrugerii sau deteriorării accidentale a datelor.
- **Sub-procesatorii:** Acordul specifică condițiile în care procesatorul de date poate angaja alți sub-procesatori și impune aceleași obligații de protecție a datelor sub-procesatorilor.
- **Drepturile Subiecților Datelor:** Asigură că procesatorul de date va asista controlorul în îndeplinirea obligațiilor sale de a răspunde la solicitările de exercitare a drepturilor subiecților datelor conform GDPR.
- **Notificarea Încălcărilor de Securitate:** Include obligația procesatorului de date de a notifica controlorul de date fără întârzieri nejustificate în cazul unei încălcări a securității datelor personale.
- **Terminarea Prelucrării:** Detaliază procedurile pentru returnarea sau ștergerea datelor personale la încheierea serviciilor de prelucrare, conform alegerii controlorului de date.

Implementarea Acordurilor de Prelucrare a Datelor:

- **Evaluare și Selecție Riguroasă a Procesatorilor:** Selectăm cu atenție procesatorii de date care pot demonstra conformitatea cu GDPR și capacitatea de a implementa măsuri de securitate adecvate.

- **Monitorizare Continuă:** Supraveghem în mod activ performanța procesatorilor de date în ceea ce privește gestionarea și protecția datelor personale pentru a asigura respectarea continuă a acordurilor stabilite.
- **Formare și Conștientizare:** Organizăm sesiuni de formare pentru personalul nostru implicat în gestionarea contractelor cu procesatorii de date pentru a asigura o înțelegere profundă a importanței și necesității acordurilor de prelucrare a datelor.

Prin stabilirea și menținerea acordurilor stricte de prelucrare a datelor, clinica noastră medicală își reafirmă angajamentul față de protejarea datelor personale și asigurarea conformității cu reglementările de protecție a datelor, protejând astfel intimitatea și drepturile subiecților datelor în toate aspectele operațiunilor noastre.

8. Măsuri de Securitate a Datelor

Clinica noastră medicală tratează securitatea datelor cu cea mai mare seriozitate, recunoscând importanța protejării datelor personale și sensibile ale pacienților și angajaților noștri. Implementăm o serie de măsuri tehnice și organizatorice pentru a asigura confidențialitatea, integritatea și disponibilitatea datelor personale pe care le gestionăm.

8.1 Măsuri Tehnice de Securitate

Criptarea Datelor:

- **Criptarea în Repaus și în Tranzit:** Toate datele personale sensibile, inclusiv înregistrările medicale și informațiile financiare, sunt criptate atât când sunt stocate în sistemele noastre, cât și când sunt transmise electronic către sau de la terți părți autorizați. Utilizăm standarde de criptare puternice recunoscute în industrie pentru a preveni accesul neautorizat sau interceptarea datelor.

Controlul Accesului:

- **Gestionarea Accesului:** Implementăm politici stricte de control al accesului pentru a asigura că numai personalul autorizat are acces la datele personale, bazat pe necesitățile lor specifice de îndeplinire a sarcinilor. Accesul la date este controlat prin utilizarea de parole puternice, autentificare multi-factor și drepturi de acces bazate pe roluri.
- **Jurnalizarea și Monitorizarea Accesului:** Monitorizăm și înregistrăm accesul la sistemele de prelucrare a datelor pentru a detecta și a investiga orice activitate suspectă sau neautorizată, permitându-ne să răspundem rapid la potențialele încălcări ale securității datelor.

Securitatea Rețelei:

- **Firewall-uri și Sisteme de Detectare a Intruziunilor:** Utilizăm firewall-uri avansate și sisteme de detectare și prevenire a intruziunilor pentru a proteja rețelele noastre împotriva accesului neautorizat și a atacurilor cibernetice.

- **Securitatea Aplicațiilor:** Toate aplicațiile utilizate pentru prelucrarea datelor personale sunt supuse unor teste riguroase de securitate și actualizări regulate pentru a remedia orice vulnerabilități de securitate cunoscute.

Managementul Incidentelor de Securitate:

- **Planuri de Răspuns la Incidente:** Avem în loc planuri de răspuns la incidente de securitate pentru a asigura o reacție rapidă și eficientă la orice încălcare a datelor. Acest lucru include notificarea imediată a persoanelor afectate și a autorităților competente, conform cerințelor GDPR.

Formare și Conștientizare în Securitate:

- **Programe de Formare pentru Angajați:** Organizăm sesiuni de formare și conștientizare regulată pentru toți angajații, pentru a-i educa despre riscurile de securitate, bunele practici în materie de securitate a datelor și procedurile de raportare a incidentelor.

Prin implementarea acestor măsuri tehnice detaliate, clinica noastră medicală își demonstrează angajamentul neclintit față de protecția datelor personale și sensibile ale tuturor subiecților noștri de date. Ne angajăm să menținem și să îmbunătățim continuu securitatea informațiilor pentru a răspunde la evoluția amenințărilor de securitate și la cerințele legislative.

8.2 Măsuri Organizatorice de Securitate

Pe lângă măsurile tehnice stricte, clinica noastră medicală implementează și o serie de măsuri organizatorice esențiale pentru a asigura securitatea datelor personale. Aceste măsuri sunt concepute pentru a crea un cadru solid și o cultură a securității în toată organizația, implicând fiecare membru al echipei în protecția datelor.

Politici și Proceduri de Securitate:

- **Dezvoltarea și Implementarea Politicilor:** Avem politici și proceduri detaliate de securitate a datelor, care sunt revizuite și actualizate periodic pentru a reflecta cele mai bune practici și evoluțiile legislative. Aceste politici acoperă aspecte precum gestionarea accesului, clasificarea datelor, securitatea fizică și electronică, precum și gestionarea incidentelor de securitate.
- **Distribuirea Politicilor:** Toți angajații primesc copii ale politicilor de securitate și sunt obligați să confirme că le-au citit și înțeles. Politicile sunt accesibile în permanență pentru consultare.

Formare și Conștientizare:

- **Programe Regulate de Formare:** Organizăm sesiuni regulate de formare în securitatea datelor pentru a asigura că toți angajații sunt conștienți de responsabilitățile lor și de cele mai bune practici pentru protecția datelor. Aceste sesiuni includ instruire privind identificarea și raportarea incidentelor de securitate, gestionarea corectă a datelor personale și înțelegerea amenințărilor la adresa securității.

- **Campanii de Conștientizare:** Desfășurăm campanii de conștientizare pentru a menține securitatea datelor ca o prioritate constantă în cadrul clinicii.

Evaluarea Riscurilor și Gestionarea Incidentelor:

- **Evaluări Periodice ale Riscurilor:** Conducem evaluări ale riscurilor de securitate pentru a identifica și a aborda vulnerabilitățile și amenințările potențiale la adresa securității datelor noastre.
- **Planuri de Răspuns la Incidente:** Avem planuri detaliate de răspuns la incidente, care includ protocoale pentru notificarea autorităților și a subiecților datelor afectați în cazul unei încălcări a securității.

Roluri și Responsabilități:

- **Desemnarea Responsabililor cu Securitatea Datelor:** Identificăm clar rolurile și responsabilitățile legate de securitatea datelor în cadrul organizației, inclusiv desemnarea unui Ofițer de Protecție a Datelor (OPD) care supraveghează conformitatea cu reglementările de protecție a datelor și politici interne.

Verificări și Audituri:

- **Audituri Interne și Externe:** Realizăm audituri periodice ale măsurilor noastre de securitate pentru a verifica conformitatea cu politicile interne și cerințele legale. Aceste audituri sunt efectuate atât de echipe interne, cât și de experți externi independenți.

Prin aceste măsuri organizatorice, ne asigurăm că securitatea datelor este integrată în toate aspectele activităților noastre, de la nivelul conducerii până la fiecare angajat. Creăm astfel un mediu în care toți membrii organizației sunt împuterniciți și responsabilizați să protejeze datele personale, consolidând încrederea pacienților și partenerilor noștri în capacitatea noastră de a gestiona în mod sigur și responsabil informațiile sensibile.

8.3 Managementul Incidentelor de Securitate

Conștientizarea și gestionarea rapidă și eficientă a incidentelor de securitate sunt esențiale pentru protejarea datelor personale și a informațiilor sensibile ale pacienților și angajaților noștri. La clinica noastră, am dezvoltat un cadru detaliat pentru identificarea, raportarea, gestionarea și remedierea incidentelor de securitate.

Identificarea Incidentelor:

- **Sisteme de Monitorizare:** Folosim tehnologii avansate de monitorizare a securității pentru a detecta activități suspecte sau neautorizate care ar putea indica o încălcare a securității datelor.
- **Formare și Conștientizare:** Angajații sunt instruiți să recunoască și să raporteze incidentele de securitate, indiferent de gravitatea aparentă a acestora.

Procedura de Raportare:

- **Canale de Raportare:** Stabilim canale clare și accesibile prin care angajații și părțile terțe pot raporta incidentele de securitate, inclusiv un sistem de raportare anonim, dacă este necesar.
- **Răspuns Rapid:** Toate rapoartele de incidente primesc o atenție imediată de la echipa noastră de securitate, care începe evaluarea și răspunsul în cel mai scurt timp posibil.

Gestionarea Incidentelor:

- **Echipa de Răspuns la Incidente:** Avem o echipă dedicată de răspuns la incidente, formată din membrii cu experiență în securitatea informațiilor, IT și conformitate, care coordonează răspunsul la incidente, de la identificare la rezoluție.
- **Evaluarea Impactului:** Evaluăm impactul potențial al fiecărui incident asupra datelor personale și asupra operațiunilor clinicii, pentru a determina acțiunile corespunzătoare de remediere.
- **Comunicarea Incidentelor:** Comunicăm în mod transparent și eficient cu toate părțile implicate, inclusiv cu subiecții datelor afectați și autoritățile de reglementare, conform cerințelor GDPR și ale altor legi aplicabile.

Recuperarea și Remedierea:

- **Planuri de Continuitate a Afacerii:** Implementăm planuri de continuitate a afacerii și de recuperare după dezastre pentru a minimiza întreruperile operaționale și pentru a asigura restabilirea rapidă a serviciilor și a accesului la date.
- **Îmbunătățiri Post-Incident:** Analizăm fiecare incident pentru a identifica și a implementa îmbunătățiri ale măsurilor noastre de securitate, pentru a preveni reapariția incidentelor similare.

Managementul eficient al incidentelor de securitate este o componentă cheie a strategiei noastre de protecție a datelor. Prin abordarea proactivă și sistemul bine pus la punct de gestionare a incidentelor, ne asigurăm că suntem pregătiți să răspundem rapid și eficient la orice amenințări la adresa securității datelor, protejând astfel informațiile sensibile și menținând încrederea pacienților și a angajaților în clinică.

9. Training și Conștientizare

Recunoaștem importanța esențială a formării și conștientizării continue în ceea ce privește protecția datelor personale în rândul tuturor angajaților noștri. Educația continuă și înțelegerea profundă a responsabilităților legate de protecția datelor sunt fundamentale pentru asigurarea conformității cu GDPR și alte reglementări aplicabile, precum și pentru protejarea confidențialității și integrității informațiilor pe care le gestionăm.

9.1 Programe de Formare pentru Personal

Obiectivele Programului de Formare:

- **Conștientizarea Riscurilor de Securitate a Datelor:** Educăm angajații despre diferitele tipuri de riscuri și amenințări la adresa securității datelor pentru a-i împuternici să recunoască și să evite potențialele incidente de securitate.
- **Înțelegerea Obligațiilor Legale și de Conformitate:** Furnizăm instruire detaliată privind cerințele GDPR și ale legislației locale, subliniind responsabilitățile personale și ale organizației în ceea ce privește prelucrarea și protejarea datelor personale.
- **Promovarea Celor Mai Bune Practici:** Încurajăm adoptarea celor mai bune practici în manipularea datelor personale, de la colectare la stocare și eliminare, prin demonstrarea tehnicilor și proceselor adecvate.

Implementarea Programului de Formare:

- **Sesiuni Regulate de Formare:** Organizăm sesiuni de formare la intervale regulate pentru a asigura că toți angajații sunt la curent cu ultimele dezvoltări în domeniul protecției datelor și securității informațiilor. Aceste sesiuni includ atât instruire la angajare pentru noii veniți, cât și sesiuni de reîmprospătare pentru personalul existent.
- **Materiale de Învățare Diverse:** Folosim o gamă largă de materiale de învățare, inclusiv prezentări, broșuri, studii de caz și teste, pentru a asigura o înțelegere cuprinzătoare și pentru a menține angajamentul angajaților.
- **Evaluări și Feedback:** Evaluăm eficacitatea programelor noastre de formare prin teste și feedback direct de la angajați, ajustând materialele și metodele de predare conform necesităților identificate.

Beneficiile Formării și Conștientizării:

- **Prevenirea Încălcărilor de Securitate:** Prin educarea angajaților despre cum să recunoască și să gestioneze în mod eficient riscurile de securitate, putem reduce semnificativ probabilitatea incidentelor de securitate și a încălcărilor de date.
- **Creșterea Încrederii și Transparenței:** Un personal bine informat transmite încredere pacienților și partenerilor, demonstrând angajamentul nostru față de gestionarea responsabilă și etică a datelor personale.
- **Conformitate Continuă:** Asigurăm că clinica rămâne în conformitate cu cerințele legale în continuă schimbare, adaptându-ne la noi reglementări și standarde în domeniul protecției datelor.

Prin angajamentul nostru către formare și conștientizare, consolidăm cultura protecției datelor în întreaga noastră organizație, asigurând că fiecare membru al echipei contribuie activ la securitatea și confidențialitatea datelor pe care le gestionăm.

9.2 Inițiative de Conștientizare Continuă

Pe lângă programele structurate de formare, clinica noastră implementează inițiative de conștientizare continuă pentru a menține securitatea datelor și protecția datelor personale ca o prioritate constantă în mintea tuturor angajaților. Aceste inițiative sunt esențiale pentru a construi și menține o cultură a protecției datelor în întreaga organizație.

Campanii de Conștientizare:

- **Campanii Periodice:** Desfășurăm campanii de conștientizare regulat, folosind postere, e-mailuri informative și prezentări la întâlnirile de echipă pentru a sublinia aspecte importante ale securității și protecției datelor. Aceste campanii sunt proiectate să reamintească personalului despre practicile corecte și să-i informeze despre noile amenințări sau schimbări legislative.
- **Ziua Protecției Datelor:** Celebrăm Ziua Europeană a Protecției Datelor și alte evenimente relevante pentru a promova importanța și valoarea protecției datelor în cadrul organizației noastre.

Materiale Educaționale Accesibile:

- **Resurse Online:** Oferim acces la materiale educaționale, ghiduri și tutoriale online, care pot fi accesate de către angajați în orice moment pentru auto-învățare sau pentru a clarifica orice îndoieli referitoare la manipularea datelor personale.
- **Newsletter-e:** Trimitem periodic buletine informative care conțin sfaturi de securitate, rezumate ale incidentelor de securitate relevante la nivel global și lecții învățate, pentru a ține echipa informată și vigilentă.

Dialog Deschis și Feedback:

- **Sesiuni de Întrebări și Răspunsuri:** Organizăm sesiuni regulare de întrebări și răspunsuri, unde angajații pot adresa întrebări legate de securitatea datelor și protecția datelor personale, facilitând astfel un dialog deschis și constructiv.
- **Feedback și Sugestii:** Încurajăm angajații să ofere feedback și să sugereze îmbunătățiri ale politicilor și procedurilor de securitate a datelor, recunoscând rolul activ pe care fiecare îl joacă în protejarea datelor.

Prin aceste inițiative de conștientizare continuă, ne asigurăm că fiecare membru al echipei este informat, responsabil și angajat în protejarea datelor personale și a confidențialității. Această abordare holistică întărește mecanismele noastre de apărare împotriva amenințărilor la adresa securității datelor și promovează o cultură organizațională în care protecția datelor este văzută ca o responsabilitate comună.

9.3 Evaluarea și Îmbunătățirea Continuă a Programelor de Formare și Conștientizare

Pentru a asigura eficacitatea și relevanța continuă a programelor noastre de formare și conștientizare în domeniul protecției datelor, clinica noastră medicală se angajează într-un proces de evaluare și îmbunătățire constantă. Acest proces ne permite să adaptăm și să rafinăm inițiativele noastre de educație pe măsură ce apar noi provocări în domeniul securității datelor și pe măsură ce organizația noastră evoluează.

Evaluarea Programelor de Formare:

- **Feedback de la Participanți:** După fiecare sesiune de formare, solicităm feedback de la participanți pentru a evalua claritatea materialului prezentat, eficacitatea metodelor de predare și gradul de angajament al cursanților. Acest feedback este esențial pentru ajustarea și îmbunătățirea continuă a programelor noastre.

- **Teste de Cunoștințe:** Implementăm teste de cunoștințe sau quiz-uri la sfârșitul sesiunilor de formare pentru a măsura asimilarea informațiilor și pentru a identifica orice lacune în înțelegerea subiectelor prezentate.
- **Analiza Incidentelor de Securitate:** Revizuim și analizăm periodic incidentele de securitate pentru a determina dacă acestea ar fi putut fi prevenite prin formare sau conștientizare îmbunătățite. Învățămintele extrase sunt integrate în programele viitoare de formare.

Îmbunătățirea Continuă:

- **Actualizarea Continuă a Conținutului:** Ne asigurăm că materialele de formare și campaniile de conștientizare sunt actualizate regulat pentru a reflecta cele mai recente evoluții în domeniul securității și protecției datelor, inclusiv noi amenințări, tehnologii și reglementări legale.
- **Diversificarea Metodelor de Livrare:** Experimentăm cu diverse forme și metode de livrare, cum ar fi e-learning, webinarii, ateliere interactive și jocuri educaționale, pentru a mări angajamentul și retenția informațiilor.
- **Formare Specifică Rolului:** Dezvoltăm module de formare personalizate care să se adreseze cerințelor specifice de securitate și protecție a datelor pentru diferite roluri și departamente în cadrul clinicii, asigurându-ne că fiecare angajat primește instruirea cea mai relevantă pentru funcțiile și responsabilitățile sale.

Urmărirea Efectelor Formării și Conștientizării:

- **Monitorizarea Comportamentelor de Securitate:** Observăm și monitorizăm comportamentele legate de securitate în rândul personalului pentru a evalua impactul inițiativelor noastre de conștientizare pe termen lung.
- **Raportarea și Analiza Trendurilor:** Analizăm tendințele în raportarea incidentelor și solicitările de informații despre protecția datelor pentru a identifica domenii care pot beneficia de formare suplimentară sau campanii de conștientizare.

Prin acest proces de evaluare și îmbunătățire continuă, ne asigurăm că eforturile noastre de formare și conștientizare rămân eficiente, relevante și adaptate la nevoile în continuă schimbare ale clinicii și ale personalului nostru. Acest angajament ne ajută să construim și să menținem o cultură a protecției datelor, împuternicind fiecare membru al echipei să contribuie la securitatea și confidențialitatea datelor personale pe care le gestionăm.

10. Gestionarea Furnizorilor si a Procesatorilor Terti de Date

În calitate de clinică medicală, colaborăm frecvent cu furnizori externi și procesatori de date terți care pot avea acces la datele personale pe care le gestionăm. Recunoaștem importanța esențială a asigurării că toți partenerii noștri respectă aceleași standarde înalte de protecție a datelor ca și noi. Prin urmare, avem implementate proceduri stricte pentru gestionarea relațiilor cu acești parteneri, pentru a proteja confidențialitatea și securitatea datelor personale ale pacienților și angajaților noștri.

10.1 Due Diligence a Furnizorilor și Procesatorilor Terci

Evaluarea Inițială:

- **Verificarea Credențialelor:** Înainte de a angaja orice furnizor sau procesator terț, efectuăm o evaluare amănunțită a credențialelor acestora, inclusiv a istoricului lor de conformitate cu legile de protecție a datelor și a măsurilor de securitate pe care le au în vigoare.
- **Evaluarea Riscurilor:** Evaluăm riscurile potențiale asociate cu partajarea datelor personale cu fiecare potențial partener, asigurându-ne că pot gestiona datele într-un mod sigur și conform.

Acorduri de Prelucrare a Datelor:

- **Clauze Contractuale Stricte:** Stabilim acorduri de prelucrare a datelor care includ clauze contractuale stricte, obligând furnizorii și procesatorii terți să respecte legislația privind protecția datelor și să implementeze măsuri adecvate de securitate a datelor.
- **Audituri și Evaluări Periodice:** Includem dreptul de a efectua audituri și evaluări periodice ale măsurilor de securitate și conformitate ale partenerilor noștri, pentru a asigura menținerea standardelor de protecție a datelor.

Gestionarea Relațiilor:

- **Comunicare Clară a Așteptărilor:** Clarificăm așteptările noastre în materie de protecție a datelor la începutul oricărei relații cu furnizori și procesatori terți, inclusiv necesitatea notificării prompte în cazul oricăror incidente de securitate.
- **Instruire și Conștientizare:** Încurajăm sau cerem partenerilor noștri să asigure că angajații lor care vor avea acces la datele noastre personale primesc formare adecvată în protecția și securitatea datelor.

Monitorizare și Revizuire Continuă:

- **Monitorizarea Performanței:** Supraveghem îndeaproape performanța furnizorilor și procesatorilor terți în ceea ce privește gestionarea datelor personale, pentru a identifica și aborda rapid orice probleme sau deficiențe.
- **Actualizarea și Renegocierea Acordurilor:** Revizuim și, dacă este necesar, renegociem acordurile de prelucrare a datelor la intervale regulate sau când apar schimbări în operațiunile partenerului care ar putea afecta securitatea datelor personale.

Prin implementarea acestor măsuri de due diligence și gestionare atentă a relațiilor cu furnizorii și procesatorii terți, ne asigurăm că partenerii noștri tratează datele personale cu aceeași grijă și seriozitate ca și noi. Aceasta ne ajută să protejăm confidențialitatea și integritatea datelor personale ale pacienților și angajaților noștri, consolidând încrederea în practicile noastre de protecție a datelor.

10.2 Contracte și Acorduri

Pentru a asigura conformitatea și protecția datelor personale gestionate de clinica noastră medicală, toate relațiile noastre cu furnizorii și procesatorii de date terți sunt guvernate de

contracte și acorduri detaliate. Aceste documente sunt concepute pentru a stabili în mod clar responsabilitățile și obligațiile fiecărei părți în ceea ce privește prelucrarea datelor personale, asigurând un nivel înalt de securitate și conformitate cu reglementările de protecție a datelor, inclusiv GDPR.

Elementele Cheie ale Contractelor și Acordurilor:

- **Scopul și Durata Prelucrării:** Contractele specifică în mod clar scopurile pentru care datele personale pot fi prelucrate de către furnizorii sau procesatorii terți, limitând prelucrarea la acele scopuri și stabilind durata prelucrării.
- **Descrierea Tipurilor de Date Personale:** Detaliem tipurile de date personale care vor fi prelucrate și categoriile de subiecți ai datelor implicati, asigurându-ne că partenerii noștri înțeleg natura datelor cu care vor lucra.
- **Obligații de Securitate:** Impunem obligații stricte de securitate, cerând furnizorilor și procesatorilor să implementeze măsuri tehnice și organizatorice adecvate pentru a proteja datele personale împotriva accesului neautorizat, pierderii sau distrugerii accidentale.
- **Sub-procesare:** Contractele restricționează posibilitatea partenerilor noștri de a angaja sub-procesatori fără consimțământul nostru prealabil scris și impun transmiterea obligațiilor de securitate și de protecție a datelor către orice sub-procesatori.
- **Drepturi ale Subiecților Datelor:** Asigurăm că acordurile prevăd mecanisme prin care furnizorii și procesatorii terți să asiste clinica în răspunsul la solicitările subiecților datelor pentru exercitarea drepturilor lor conform GDPR.
- **Notificarea Încălcărilor de Securitate:** Stabilim obligația partenerilor de a notifica clinica fără întârzieri nejustificate în cazul unei încălcări de securitate a datelor, permițându-ne să luăm măsuri adecvate de răspuns.
- **Audituri și Inspecții:** Contractele permit clinicii să efectueze audituri și inspecții ale măsurilor de securitate și de protecție a datelor implementate de către parteneri, asigurând conformitatea continuă cu acordurile stabilite.

Implementarea și Monitorizarea Acordurilor:

- **Proces Riguros de Verificare:** Înainte de semnarea oricărui contract, efectuăm o verificare aprofundată a practicilor de securitate și de protecție a datelor ale partenerului, inclusiv o evaluare a conformității acestora cu GDPR și alte legi relevante.
- **Instruire Continuă:** Oferim instruire regulată echipei noastre care gestionează relațiile cu furnizorii și procesatorii terți, asigurându-ne că sunt la curent cu cele mai bune practici în negocierea și monitorizarea contractelor.
- **Monitorizare Continuă:** Supraveghem în mod activ conformitatea partenerilor cu termenii contractuali pe parcursul întregii relații, intervenind rapid pentru a adresa orice abateri sau probleme identificate.

Prin aceste practici riguroase de contractare și monitorizare, ne asigurăm că toți partenerii și procesatorii de date terți cu care colaborăm împărtășesc angajamentul nostru față de protecția și securitatea datelor personale, contribuind astfel la menținerea unui standard înalt de confidențialitate și integritate a datelor în toate operațiunile noastre.

11. Data Protection Impact Assessment (DPIA)

Conștienți de importanța evaluării impactului asupra protecției datelor (DPIA) în identificarea și minimizarea riscurilor de protecție a datelor asociate cu prelucrarea datelor personale, clinica noastră medicală implementează DPIA-uri ca parte integrantă a procesului nostru de management al riscurilor. Acest proces este crucial în planificarea și implementarea oricăror noi proiecte sau tehnologii care implică prelucrarea datelor personale, asigurând conformitatea cu GDPR și protejarea drepturilor și libertăților fundamentale ale subiecților datelor.

11.1 Când este Necesar DPIA

Situații care Necesită DPIA:

- **Prezentarea de Riscuri Ridicate:** DPIA este necesară atunci când o formă de prelucrare, în special folosind noi tehnologii, și având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, este susceptibilă să prezinte un risc ridicat pentru drepturile și libertățile subiecților datelor. Acest lucru include prelucrarea pe scară largă a datelor sensibile sau a datelor personale referitoare la condamnări penale și infracțiuni.
- **Evaluare Sistematică și Extinsă:** DPIA este indicată pentru orice evaluare sistematică și extinsă a aspectelor personale ale subiecților datelor, care se bazează pe prelucrarea automată, inclusiv profilarea, și care formează baza pentru decizii care produc efecte juridice sau afectează în mod semnificativ subiecții datelor.
- **Supravegherea pe Scară Largă:** Orice supraveghere sistematică și pe scară largă a unei zone accesibile publicului necesită efectuarea unei DPIA.

Procedura DPIA:

- **Descrierea Procesului de Prelucrare:** Începem cu o descriere detaliată a prelucrării planificate, identificându-ne scopul și mijloacele prelucrării.
- **Evaluarea Necesității și Proporționalității:** Evaluăm necesitatea și proporționalitatea prelucrării în raport cu scopul pentru care sunt prelucrate datele personale.
- **Evaluarea Riscurilor:** Identificăm și evaluăm riscurile pentru drepturile și libertățile subiecților datelor, luând în considerare natura, domeniul de aplicare, contextul și scopurile prelucrării.
- **Măsuri pentru Atenuarea Riscurilor:** Stabilim măsuri pentru a atenua riscurile identificate, asigurând protecția drepturilor și libertăților subiecților datelor.
- **Consultare:** Dacă este necesar, consultăm Autoritatea de Protecție a Datelor (APD) înainte de prelucrare, mai ales atunci când DPIA indică faptul că prelucrarea ar rezulta într-un risc ridicat în absența măsurilor de atenuare.

Prin aplicarea DPIA-urilor în mod sistematic și riguros, clinica noastră medicală demonstrează angajamentul său față de gestionarea responsabilă și transparentă a datelor personale, prioritizând protecția datelor și conformitatea cu GDPR în toate aspectele activităților noastre de prelucrare. Această abordare ne ajută să identificăm și să minimizăm orice riscuri potențiale pentru confidențialitatea și securitatea datelor înainte de a afecta subiecții datelor.

11.2 Procesul DPIA

Pentru a asigura o implementare eficientă și cuprinzătoare a evaluărilor impactului asupra protecției datelor (DPIA), clinica noastră medicală urmează un proces structurat, care include mai multe etape cheie. Acest proces ne permite să evaluăm și să atenuăm riscurile asociate cu prelucrarea datelor personale înainte de inițierea oricăror activități noi sau semnificative de prelucrare.

Identificarea Nevoii de DPIA:

- **Revizuire Preliminară:** Evaluăm orice proiecte noi sau modificările semnificative ale proceselor existente pentru a determina dacă implică prelucrarea datelor personale într-un mod care ar putea prezenta riscuri ridicate pentru drepturile și libertățile individuale.
- **Consultare Internă:** Consultăm departamentele relevante în cadrul clinicii, inclusiv IT, juridic și operațiuni, pentru a înțelege domeniul de aplicare și detaliile prelucrării propuse.

Documentarea Procesului de Prelucrare:

- **Descrierea Detaliată:** Documentăm detaliile prelucrării, inclusiv tipul datelor colectate, scopul prelucrării, baza legală, metodele de colectare și stocare, și orice transferuri de date planificate.
- **Evaluarea Riscurilor:** Identificăm și evaluăm riscurile potențiale pentru subiecții datelor, luând în considerare atât probabilitatea cât și severitatea impactului asupra drepturilor și libertăților acestora.

Consultarea Părților Interesate:

- **Angajarea Subiecților Datelor:** Acolo unde este posibil și adecvat, implicăm subiecții datelor sau reprezentanții acestora în procesul DPIA, pentru a obține feedback direct cu privire la percepțiile lor asupra riscurilor și a măsurilor de atenuare.
- **Consultarea cu Ofițerul de Protecție a Datelor (OPD):** OPD-ul este consultat pe parcursul întregii DPIA, oferind orientări cu privire la conformitatea cu GDPR și alte reglementări relevante.

Implementarea Măsurilor de Atenuare:

- **Plan de Atenuare:** Dezvoltăm și implementăm un plan detaliat de atenuare a riscurilor identificate, care poate include măsuri tehnice, organizatorice și de politică.
- **Integrarea Protecției Datelor de la Proiectare:** Asigurăm că măsurile de protecție a datelor sunt integrate de la început în designul proiectului sau procesului, conform principiului "privacy by design".

Monitorizarea și Revizuirea:

- **Monitorizarea Implementării:** Supraveghem implementarea planului de atenuare a riscurilor pentru a ne asigura că măsurile sunt efective și că riscurile rămân sub control.

- **Revizuirea Periodică:** DPIA-urile sunt revizuite periodic sau atunci când intervin schimbări semnificative în procesul de prelucrare, pentru a ne asigura că evaluarea riscurilor este încă relevantă și completă.

11.3 Documentarea și Raportarea DPIA

Documentarea și raportarea corectă și completă a evaluării impactului asupra protecției datelor (DPIA) sunt componente esențiale ale procesului DPIA, asigurând că toate etapele evaluării și rezultatele acesteia sunt înregistrate adecvat. Aceasta nu doar că demonstrează conformitatea cu GDPR, dar și facilitează revizuirea și monitorizarea continuă a riscurilor asociate cu prelucrarea datelor personale.

Conținutul Raportului DPIA:

- **Descrierea Prelucrării:** O descriere detaliată a operațiunii de prelucrare propuse, inclusiv scopul prelucrării și tipurile de date personale implicate.
- **Necesitatea și Proporționalitatea:** O analiză a necesității și proporționalității prelucrării în raport cu scopurile urmărite.
- **Evaluarea Riscurilor:** O evaluare a riscurilor pentru drepturile și libertățile subiecților datelor, inclusiv probabilitatea și severitatea potențialului impact negativ.
- **Măsuri de Atenuare:** Detalii despre măsurile propuse pentru atenuarea riscurilor identificate, inclusiv garanții, măsuri de securitate și mecanisme pentru a asigura protecția datelor personale.
- **Concluzii și Decizia de Prelucrare:** O sinteză a rezultatelor DPIA și a deciziei cu privire la continuarea prelucrării, luând în considerare riscurile și măsurile de atenuare.

Procedura de Documentare și Raportare:

- **Înregistrarea DPIA:** Toate DPIA-urile sunt documentate într-un registru centralizat, care facilitează accesul ușor și revizuirea documentelor de către personalul autorizat, inclusiv de către Ofițerul de Protecție a Datelor (OPD).
- **Consultare Internă și Externă:** Documentația DPIA include detalii despre orice consultări interne sau externe efectuate în cursul evaluării, precum și feedback-ul primit de la acestea.
- **Revizuire și Actualizare:** DPIA este revizuită periodic pentru a reflecta orice schimbări în natura, domeniul de aplicare sau contextul prelucrării sau pentru a integra noi informații despre riscuri și măsuri de atenuare.
- **Raportarea către Autoritatea de Supraveghere:** În cazul în care DPIA indică că prelucrarea ar putea rezulta într-un risc ridicat care nu poate fi atenuat în mod satisfăcător, clinica noastră are obligația de a consulta Autoritatea Națională de Supraveghere înainte de a începe prelucrarea.

12. Revizuirea și Monitorizarea Politicii

Pentru a asigura că practicile noastre de protecție a datelor rămân eficiente și conform cu legislația în continuă evoluție, clinica noastră medicală adoptă un program regulat de revizuire și monitorizare a politicii de protecție a datelor. Acest proces ne permite să identificăm și să

abordăm rapid orice lacune sau neconformități și să ne adaptăm practicile la noile provocări și reglementări.

Programul Regulat de Revizuire a Politicii

- **Revizuire Anuală:** Politica noastră de protecție a datelor este supusă unei revizuiri anuale pentru a asigura că reflectă corect practicile actuale de prelucrare a datelor și conformitatea cu reglementările aplicabile. Această revizuire este coordonată de Ofițerul nostru de Protecție a Datelor (OPD) și implică reprezentanți din diferite departamente relevante.
- **Feedback-ul Angajaților:** Încurajăm feedback-ul continuu de la angajații noștri în legătură cu politica și practicile de protecție a datelor, folosind aceste informații pentru a identifica zonele care necesită îmbunătățiri sau clarificări suplimentare.

Audituri de Conformitate

- **Audituri Interne:** Efectuăm audituri interne regulate ale conformității cu politica de protecție a datelor și cu reglementările GDPR. Aceste audituri sunt planificate și executate de OPD, având ca scop identificarea oricăror acțiuni de remediere necesare.
- **Audituri Externe:** Pe lângă auditurile interne, angajăm periodic auditori externi pentru a evalua conformitatea noastră cu GDPR și cu alte standarde relevante. Acest lucru ne oferă o perspectivă obiectivă asupra eficacității măsurilor noastre de protecție a datelor.

Actualizarea Procedurilor și Practicilor

- **Implementarea Modificărilor:** Pe baza rezultatelor revizuirilor și auditurilor, implementăm modificările necesare în procedurile și practicile noastre de protecție a datelor. Acest lucru poate include actualizarea politicilor, îmbunătățirea măsurilor de securitate sau redefinirea proceselor de colectare și prelucrare a datelor.
- **Comunicarea Modificărilor:** Orice modificare semnificativă a politicii de protecție a datelor este comunicată în mod clar tuturor angajaților și, dacă este cazul, pacienților și altor părți interesate. Asigurăm că toate părțile implicate înțeleg noile practici și sunt instruite corespunzător.