Політика обробки та захисту персональних даних стоматологічної клініки ЗУБРИЦЬКИХ

1. Загальні положення

1.1. Діюча політика обробки персональних даних в (далі - Політика) складена на підставі Закону України «Про захист персональних даних» №2297-17 від 01.06.2010 року і являється основним внутрішнім регулятивним документом клініки ЗУБРИЦЬКИХ (далі – Клініка або Оператор) та визначає організаційні та технічні заходи, які забезпечують захист персональних даних (далі – ПД) від несанкціонованого доступу до інформації, неправомірного використання або втрати під час обробки.
1.2. Політика розроблена в цілях реалізації вимог законодавства пов'язаних із захистом і обробкою персональних даних і спрямована на захист основоположних прав і свобод людини і громадянина при обробці його ПД в Клініці в тому числі захисту прав на невтручання в приватне життя, особисте, сімейне і забезпечення захисту збереження лікарської таємниці.
1.3. Положення політики поширюється на відносини щодо обробки та захисту ПД отриманих Клінікою як до так і після затвердження Політики за виключенням випадків, коли з причин правового, організаційного і іншого характеру положення Політики не можуть бути розповсюджені на відносини при обробці і захисту ПД, отриманих до її затвердження.
1.4. Обробка ПД в Клініці здійснюється у зв'язку з виконанням функцій передбачених установчими документами та визначені:

- Конституція України №254к/96-ВР від 28.06.1996 року;
- Закон України «Основи законодавства України про охорону здоров'я» №2801-12 від 19.11.1992 року;
- Закон України «Про захист персональних даних» №2297-17 від 01.06.2010 року;

Крім того, обробка ПД в Клініці здійснюється під час трудових та інших відносин в яких Клініка виступає в якості роботодавця (глава 3 Кодексу законів про працю України) та в зв'язку з реалізацією Клінікою своїх прав та обов'язків як юридичної особи.
1.5. Клініка має право вносити зміни в діючу Політику. При внесенні змін вказується дата останнього оновлення редакції. Нова редакція Політики вступає в силу з моменту її розміщення на сайті, якщо інше не передбачено новою редакцією Політики.
1.6. Діюча редакція зберігається в місці знаходження Клініки за адресою: 79008, вул. Лесі Українки, 35/10, м. Львів, електронна версія Політики – на сайті за адресою: www.zubrytskyh.com

2. Визначення термінів

Персональні дані (ПД) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;
Обробка персональних даних – будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем;
Згода суб'єкта персональних даних – добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. У сфері електронної комерції згода суб'єкта персональних даних може бути надана під час реєстрації в інформаційно-телекомунікаційній системі суб'єкта електронної комерції шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки, за умови, що така система не створює можливостей для обробки персональних даних до моменту поставлення відмітки;
Третя особа – будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого Верховної Ради України з прав людини, якій володільцем чи розпорядником персональних даних здійснюється передача персональних даних;
Оператор – державний орган, муніципальний орган, юридична чи фізична особа, яка самостійно або спільно з іншими особами організують і (або) здійснюють обробку персональних даних, а також визначають цілі обробки персональних даних, склад персональних даних, що підлягають обробці, дії (операції), що здійснюються з персональними даними;
Поширення персональних даних – будь-які дії, спрямовані на розкриття персональних даних невизначеному колу осіб (передача персональних даних) або на ознайомлення з персональними даними необмеженого кола осіб, в тому числі оприлюднення персональних даних в засобах масової інформації, розміщення в інформаційно-телекомунікаційних мережах або надання доступу до персональних даних будь-яким іншим способом;
Надання персональних даних – дії, спрямовані на розкриття персональних даних певній особі або певного кола осіб;
Знищення персональних даних – будь-які дії, в результаті яких персональні дані знищуються безповоротно з неможливістю подальшого відновлення змісту персональних даних в інформаційній системі персональних даних і (або) внаслідок яких знищуються матеріальні носії персональних даних;
Знеособлення персональних даних – дії, в результаті яких неможливо

визначити без використання додаткової інформації приналежність персональних даних конкретному суб'єкту персональних даних;
Автоматизована обробка персональних даних – обробка персональних даних за допомогою засобів обчислювальної техніки;
Інформаційна система персональних даних – сукупність персональних даних, що містяться в базі даних, інформаційних технологій і технічних засобів і забезпечують обробку персональних даних;
Пацієнт – фізична особа, яка звернулась за медичною допомогою та/або якій надається така допомога;
Медична діяльність – професійна діяльність з надання медичної (стоматологічної) допомоги;
Лікуючий лікар – лікар закладу охорони здоров'я або лікар який провадить господарську діяльність з медичної практики, на якого покладено функції з організації та безпосереднього надання пацієнту медичної допомоги в період обстеження за ним і його лікування.

3. Принципи забезпечення безпеки персональних даних

3.1. Основним завданням забезпечення безпеки ПД при їх обробці в Клініці являється запобігання несанкціонованого доступу до них третіх осіб, попередження
навмисних програмно-технічних та інших впливів з метою незаконного заволодіння ПД, знищення або видалення їх в процесі обробки.
3.2. Для забезпечення безпеки ПД Клініка керується такими принципами:

законність: захист ПД ґрунтується на положеннях нормативно-правових актів та методичних документах уповноважених державних органів в області обробки і захисту ПД;

системність: обробка ПД в Клініці здійснюється з урахуванням всіх взаємопов'язаних, взаємодіючих і змінюваних у часі елементів, умов і чинників, які є значущими для розуміння і вирішення проблеми забезпечення безпеки ПД;

комплексність: захист ПД будується з використанням функціональних можливостей інформаційних технологій, реалізованих в інформаційних системах Клініки та інших наявних в Клініці систем і засобів захисту;

безперервність: захист ПД забезпечується на всіх етапах їх обробки і у всіх режимах функціонування систем обробки ПД, в тому числі при проведенні
ремонтних і регламентних робіт;

своєчасність: заходи, що забезпечують належний рівень безпеки ПД, приймаються до початку їх обробки;

наступність і безперервність вдосконалення: модернізація і нарощування заходів і засобів захисту ПД здійснюється на підставі результатів аналізу, практики обробки ПД в Клініці з урахуванням виявлення нових способів і засобів реалізації загроз безпеки ПД, вітчизняного і зарубіжного досвіду в сфері захисту інформації;

персональна відповідальність: забезпечення безпеки ПД покладається на Працівників в межах їх обов'язків, пов'язаних з обробкою і захистом ПД;

мінімізація прав доступу: доступ до ПД надається Працівникам тільки в обсязі, необхідному для виконання їх посадових обов'язків;

гнучкість: забезпечення виконання функцій захисту ПД при зміні характеристик функціонування інформаційних систем персональних даних Клініки, а також обсягу і складу оброблених ПД;

спеціалізація і професіоналізм: реалізація заходів щодо забезпечення безпеки ПД здійснюються Працівниками, які мають необхідні для цього кваліфікацію і досвід;

нагляд і прозорість: заходи щодо забезпечення безпеки ПД повинні бути сплановані так, щоб результати їх застосування могли бути оцінені особами, які здійснюють контроль;

безперервність контролю і оцінка: встановлюються процедури постійного контролю використання систем обробки та захисту ПД, а результати контролю регулярно аналізуються.

3.3. В Клініці не проводиться обробка ПД, несумісна з цілями їх збору. якщо інше не передбачено законодавством, після закінчення обробки ПД в Клініці, в тому числі при досягненні цілей їх обробки або втрати необхідності в досягненні цих цілей, оброблені Клінікою ПН знищуються або знеособлюються.

3.4. При обробці ПД забезпечується їх точність, достатність, а при необхідності – і актуальність по відношенню до цілей обробки. Клініка вживає необхідних заходів щодо видалення або уточнення неповних або неточних ПД.

4. Обробка персональних даних

4.1. Отримання ПД

4.1.1. Всі ПД слід отримувати від самого суб'єкта. Якщо ПД суб'єкта можна отримати тільки у третьої сторони, то суб'єкт повинен бути повідомлений про це або від нього повинна бути отримана згода на отримання неохідних ПД.

4.1.2. Оператор повинен повідомити суб'єкта про цілі обробки ПД, способи отримання ПД, необхідний перелік ПД, перелік дій з ПД, в разі необхідності визначити терміни протягом якого діє надана згода і порядок її відкликання, а також повідомляє про наслідки відмови суб’єкта дати письмову згоду на

їх отримання.
4.1.3. Документи, що містять ПД створюються шляхом:
а) копіювання оригіналів документів (паспорт, документ про освіту, свідоцтво ІПН, пенсійне свідоцтво та ін.);
б) внесення відомостей в облікові форми;
в) отримання оригіналів необхідних документів (трудова книжка, медичний висновок,
характеристика і ін.).
Порядок доступу суб'єкта ПД до його ПД, оброблюваних Клінікою, визначається у відповідності до законодавства та визначається внутрішніми регулятивними документами Клініки.

4.2. Обробка ПД

4.2.1. Обробка персональних даних здійснюється:

за згодою суб'єкта персональних даних на обробку його персональних даних;

у випадках, коли обробка персональних даних необхідна для здійснення і виконання покладених законодавством України функцій, повноважень і обов'язків;

у випадках, коли здійснюється обробка персональних даних, доступ необмеженого кола осіб до яких надано суб'єктом персональних даних або на його прохання (далі - персональні дані, зроблені загальнодоступними суб'єктом персональних даних).

Доступ Працівників до оброблюваних ПД здійснюється відповідно до їх посадових обов'язків і вимог згідно внутрішніх регулятивних документів Клініки.
Допущені до обробки ПД Працівники під розпис знайомляться з документами організації, що встановлюють порядок обробки ПД, включаючи документи, що встановлюють права і обов'язки конкретних Працівників.
Клінікою проводиться усунення виявлених порушень законодавства про обробці і захисту ПД.

4.2.2 Цілі обробки ПД:

Обробка ПД проводиться з ціллю реалізації прав, обов’язків та інтересів в сфері трудових правовідносин, як з боку Клініки так з боку суб’єктів ПД, також з метою підготовки відповідно до вимог законодавства статистичної, бухгалтерської, адміністративної звітності та іншої інформації. Клініка як володілець баз персональних даних Пацієнтів обробляє такі ПД виключно з метою надання медичних (стоматологічних) послуг. Обробка ПД проводиться також з метою реалізації прав, обов’язків та інтересів Клініки та інших учасників процесу під час господарської діяльності та цивільно-правових відносин. Обробка ПД здійснюється для конкретних і законних цілей, визначених за згодою суб’єкта ПД, передбачених законами України, у порядку, встановленому законодавством.

4.2.3. Категорії суб'єктів персональних даних

В Клініці обробляються ПД наступних суб'єктів:

фізичні особи, які перебувають в трудових відносинах;
фізичні особи, які є близькими родичами співробітників;
фізичні особи, що звільнилися;
фізичні особи, які є кандидатами на роботу;
фізичні особи, які перебувають в цивільно-правових відносинах;
фізичні особи, які звернулися за медичною допомогою.

4.2.4. ПД, оброблювані Клінікою:

дані отримані при здійсненні трудових відносин;
дані отримані для здійснення відбору кандидатів;
дані отримані при здійсненні цивільно-правових відносин;
дані отримані при наданні медичної допомоги.

Повний список ПД представлений в Переліку ПД, затвердженому головним лікарем Клініки.

Клініка не обробляє персональні дані про расове або етнічне походження, політичні, релігійні або світоглядні переконання, дані про статеве життя, членство в політичних партіях та професійних спілках, засудження до кримінального покарання.

4.2.5. Обробка персональних даних здійснюється:

з використанням засобів автоматизації;
без використання засобів автоматизації

4.3. Зберігання ПД

4.3.1. ПД суб'єктів можуть бути отримані, проходити подальшу обробку і передаватися на зберігання як на паперових носіях, так і в електронному вигляді.

4.3.2. ПД, зафіксовані на паперових носіях, зберігаються й замикаються в спеціально обладнаних для цієї цілі в шафах, або замикаються в приміщеннях з обмеженим правом доступу.

4.3.3. ПД суб'єктів, оброблювані з використанням засобів автоматизації в різних цілях, зберігаються в різних папках (вкладках).

4.3.4. Не допускається зберігання і розміщення документів, що містять ПД, у відкритих електронних каталогах (файлообмінниках) в ІСПД.

4.3.5. Зберігання ПД в формі, що дозволяє визначити суб'єкта ПД, здійснюється не довше, ніж цього вимагають цілі їх обробки, і вони підлягають знищенню після досягнення цілей обробки або в разі втрати необхідності в їх досягненні.

4.4. Знищення ПД

4.4.1. Знищення документів (носіїв), що містять ПД проводиться шляхом спалення, дроблення (подрібнення), хімічного розкладання, перетворення в безформну масу або порошок. Для знищення паперових документів допускається застосування шредера.

4.4.2. ПД на електронних носіях знищуються шляхом стирання або форматування носія.

4.5. Передача ПД

4.5.1. Клініка передає ПД третім особам в наступних випадках:

суб'єкт ПД висловив свою згоду на такі дії, що підтверджується у письмовій формі;

у визначених чинним законодавством України випадках на момент отримання відповідного запиту про доступ до ПД з боку третьої особи у письмовій формі відповідно до вимог закону;

поширення (передача) ПД без згоди суб'єкта персональних даних або уповноваженої ним особи дозволяються у випадках, визначеним законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини;

виконання вимог встановленого режиму захисту ПД забезпечує сторона, що поширює ці дані;

сторона, якій передаються ПД, повинна попередньо вжити заходів щодо забезпечення вимог закону.

4.5.2. Перелік осіб, яким передаються ПД

Треті особи, яким передаються ПД:

Пенсійний фонд України для обліку (на законних підставах);

Податкові органи України (на законних підставах);

Фонд соціального страхування (на законних підставах);

Страхові медичні організації добровільного медичного страхування (на законних підставах);

банки для нарахування заробітної плати (на підставі договору);

судові і правоохоронні органи у випадках, встановлених законодавством;

бюро кредитних історій (за згодою суб'єкта);

юридичні фірми, що працюють в рамках законодавства України, при невиконанні зобов'язань за договором позики (за згодою суб'єкта).

5. Захист персональних даних

5.1. Відповідно до вимог нормативних документів Клінікою створена система захисту персональних даних (далі-СЗПД), що складається з підсистем правового, організаційного та технічного захисту.

5.2. Підсистема правового захисту є комплексом правових, організаційно-розпорядчих і нормативних документів, що забезпечують створення, функціонування і вдосконалення СЗПД.

5.3. Підсистема організаційної захисту включає в себе організацію структури управління СЗПД, дозвільної системи, захисту інформації при роботі з співробітниками, партнерами і сторонніми особами, захисту інформації під час публікацій і рекламної діяльності, аналітичної роботи.

5.4. Підсистема технічного захисту включає в себе комплекс технічних, програмних, програмно-апаратних засобів, що забезпечують захист ПД.

5.5. Основними заходами захисту ПД, використовуваними Клінікою, є:
5.5.1. Призначення особи відповідальної за обробку ПД, яка здійснює організацію обробки ПД, навчання та інструктаж, внутрішній контроль за дотриманням вимог до захисту ПД;
5.5.2. Визначення актуальних загроз безпеки ПД при їх обробці в ІСПД, і розробка заходів і заходів щодо захисту ПД;
5.5.3. Розробка політики щодо обробки персональних даних;
5.5.4. Встановлення правил доступу до ПД, оброблюваних в ІСПД, а також забезпечення реєстрації та обліку всіх дій, що здійснюються з ПД в ІСПД;
5.5.5. Встановлення індивідуальних паролів доступу співробітників в інформаційну систему в Відповідно до їх виробничими обов'язками;
5.5.6. Застосування пройшли в установленому порядку процедуру оцінки відповідності засобів захисту інформації, облік машинних носіїв ПД, забезпечення їх збереження;
5.5.7. Сертифіковане антивірусне програмне забезпечення з регулярно оновленими базами;
5.5.8. Сертифікований програмні засоби захисту інформації від несанкціонованого доступу;
5.5.9. Сертифіковані між мережеві екрани і засоби виявлення вторгнення;
5.5.10. Дотримання умов, що забезпечують збереження ПД і виключають несанкціонований доступ до них, оцінка ефективності прийнятих і реалізованих заходів щодо забезпечення безпеки ПД;
5.5.11. Встановлення правил доступу до оброблюваних ПД, забезпечення реєстрації та обліку дій, що здійснюються з ПД, а також виявлення фактів несанкціонованого доступу до персональних даних та вжиття заходів;
5.5.12. Відновлення ПД, модифікованих або знищених внаслідок несанкціонованого доступу до них;
5.5.13. Навчання працівників Клініки які безпосередньо здійснюють обробку персональних даних, положенням законодавства України про персональні дані, в тому числі вимогам до захисту персональних даних, документами, що визначають політику Клініки щодо обробки персональних даних, локальних актів з питань обробки персональних даних;
5.5.14. Здійснення внутрішнього контролю та аудиту

6. Основні права суб'єкта ПД і обов'язки Клініки

6.1. Основні права суб'єкта ПД

Особисті немайнові права на ПД, які має кожна фізична особа, є невід’ємними і непорушними.
Суб'єкт ПД має право на отримання інформації щодо обробки його персональних даних, в тому числі включає містить:

підтвердження факту обробки персональних даних Оператором;
правові підстави та мету обробки персональних даних;

цілі і застосовані оператором способи обробки персональних даних;

на доступ до своїх персональних даних;

найменування та місце знаходження Оператора, відомості про осіб (за винятком працівників оператора), які мають доступ до персональних даних або яким можуть бути розкриті персональні дані на підставі договору з Оператором або на підставі законодавства;

оброблювані персональні дані, які стосуються відповідному суб'єкту персональних даних, джерело їх отримання, якщо інший порядок подання таких
даних не передбачений законодавством;

терміни обробки персональних даних, в тому числі терміни їх зберігання;

знати механізм автоматичної обробки персональних даних;

на захист від автоматизованого рішення, яке має для нього правові наслідки;

інформацію про здійснену або про передбачувану транскордонної передачі даних;

найменування або прізвище, ім'я, по батькові та адреса особи, яка здійснює обробку персональних даних за дорученням оператора, якщо обробка доручена або буде доручена такій особі;

на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв’язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;

звертатися із скаргами на обробку своїх персональних даних до Уповноваженого або до суду;

інші відомості, передбачені цим Законом або іншими законами.

Суб'єкт ПД вправі вимагати від Оператора уточнення його персональних даних, їх блокування або знищення в разі, якщо персональні дані є неповною,
застарілими, неточними, незаконно отриманими або не є необхідними для заявленої мети обробки, а також вживати передбачених законом заходів для захисту своїх прав.

6.2. Обов'язки Клініки

Клініка зобов'язана:

при зборі ПД надати інформацію про обробку його ПД;

у випадках якщо ПД були отримані не від суб'єкта ПД повідомити суб'єкта;

при відмові в наданні ПД суб'єкту роз'яснюються наслідки такої відмови;

опублікувати або іншим чином забезпечити необмежений доступ до документа, визначає його політику щодо обробки ПД, до відомостей про реалізовані вимогах до захисту ПД;

приймати необхідні правові, організаційні та технічні заходи або забезпечувати їх прийняття для захисту ПД від неправомірного або випадкового доступу до ним, знищення, перекручення, блокування, копіювання, надання,поширення ПД, а також від інших неправомірних дій у відношенні ПД;

давати відповіді на запити і звернення суб'єктів ПД, їх представників і уповноваженого органу з захисту прав суб'єктів ПД.