«Утверждаю»
Генеральный директор
ООО «Центр клинической постурологии»
Стецюра О. А.
_____10.01.2024
Подпись Дата

Приложение №1
к приказу № ВНТ–2024/0001 от 10.01.2024 года

Положение о порядке действий при утечке ПДн

1. Общие положения

1.1. Оказание медицинских услуг предполагает обработку и хранение персональных данных пациентов (клиентов, потребителей медицинских услуг) в автоматизированных информационных системах ООО «Центр клинической постурологии» (далее по тексту Клиника)
1.2. В соответствии с действующим законодательством (федеральный закон от 27.06.2006 года №152-ФЗ «О персональных данных»), ст. 1, 2, Клиника выполняет комплекс технических и организационных мероприятий для обеспечения безопасности обрабатываемых и хранимых персональных данных наших пациентов.
1.3. Клиника является высокотехнологичной организацией, применяющей в своей работе передовые IT-технологии. Поэтому одна из приоритетных задач в работе Клиники - соблюдение действующего законодательства Российской Федерации в области информационной безопасности, а также требований федеральных законов № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации» и № 152-ФЗ от 27.07.2006 «О персональных данных», основной целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.
1.4. Оператор ПД - ООО «Центр клинической постурологии» (регистрационный номер 77-23-152712, Приказ № 304 от 15.09.2023)

2. Цель обработки персональных данных

Целью сбора, обработки, хранения, а также других действий с персональными данными пациентов, посетителе и сотрудников Клиники является исполнением обязательств Клинки перед пациентами по договору с ними, перед посетителями и перед сотрудниками Клиники во исполнении федеральных законов № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации» и № 152-ФЗ от 27.07.2006 «О персональных данных»

3. Принципы обработки персональных данных

3.1. При обработке персональных данных пациентов, посетителей Клиники, Клиника придерживается следующих принципов:
- соблюдение законности получения, обработки, хранения, а также других действий с персональными данными во исполнении действующего законодательства Российской Федерации, срок хранения персональных данных составляет 25 (двадцать пять) лет;
- строгое выполнение требований по обеспечению безопасности персональных данных и сведений, составляющих врачебную тайну при их обработке и хранении персональных данных;
- обработка персональных данных исключительно с целью исполнения своих обязательств по договору оказания платных медицинских услуг и во исполнение федерального закона от 27.06.2006 года №152-ФЗ «О персональных данных»;

3.2. Соблюдение прав субъекта персональных данных на доступ к его персональным данным.

4. Обоснование необходимости электронной безопасности

Использование компьютерного оборудования для обработки персональных данных пациентов (далее по тексту ПДН) – чрезвычайно необходимая мера в современных российских реалиях. С целью защиты ПДН от несекционного использования третьими лицами.
4.1. В состав обрабатываемых в Клинике персональных данных пациентов могут входить:
- фамилия, имя, отчество;
- дата рождения, пол;
- паспортные данные (для заполнения договора на оказание платных медицинских услуг);
- адрес проживания;

- номер телефона;
- другая информация, необходимая для правильного проведения и интерпретации медицинских исследований (необходима в некоторых случаях для установки правильных пограничных значений результатов);
- результаты выполненных медицинских исследований.

4.2. Клиника не обрабатывает персональные данные, касающиеся состояния здоровья клиента, за исключением случаев, когда их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов.

5. Законодательство

5.1. Первичная правовая база по организации безопасности и защиты персональной информации в медицинских учреждениях, выполнение с этой целью всех защитных мероприятий основываются на законе № 152-ФЗ, принятом 27.07.2006. «О персональных данных»

Общие юридические основания о врачебной тайне прописаны в «Основах... об охране здоровья...». В этом документе содержатся основополагающие требования по защите персональных данных.

Федеральным законом РФ от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Основные нормативы, которыми руководствуются медучреждения при создании системы защиты ПДн:

- ФЗ № 149 об информации, информ технологиях и способах защиты этой информации;
- Указ Президента № 188, в котором перечислены сведения, отнесенные к конфиденциальным;
- Основы законодательства РФ – статьи 31 и 61, описывающие права пациентов, в том числе связанные с обработкой ПДн с применением автоматизированных средств;
- ФЗ № 5487 об охране здоровья граждан на территории РФ;
- Приказ № 29н Минздрава РФ о медицинских формах учета и отчетности.

5.2. Правовые документы по обработке ПДн медперсонала

Кроме вышеперечисленных документов, в мед. организациях применяются нормативные акты по организационному обеспечению защиты ПДн медперсонала. К этим документам относятся:

- ТК РФ – гл. 14;
- Постановление Госкомстата РФ № 1 от 05.01.2004 г., касающееся утверждения и оформления унифицированных форм учета документов по оформлению трудовых отношений, оплате труда.

5.3. Сроки обработки данных установлены приказом «О введении в действие положения о медицинском архиве лечебного учреждения».

Клиника берет на себя ответственность за правильную и безопасную работу с персональными данными и непосредственно отвечает за сбор информации у пациентов и посетителей.

6. Специфика обработки персональных данных в медучреждениях

6.1. Оператор ПДн учитывает при обработке персональных данных в медицинских учреждениях, –роль этической составляющей. Клиника хранит данные о здоровье каждого пациента и не допускает огласки такой информации. Многие болезни считаются социально табуированными и не подлежат разглашению по базовым правилам медицинской этики.

6.2. Анализ персональных данных пациентов основывается на принципе, согласно которому здоровье пациента является чрезвычайно конфиденциальной категорией информации. Какое-либо своевольное изъятие данных категорически воспрещается.

6.3. Исключение делается только в ситуации чрезвычайных обстоятельств. Например, речь может идти о защите самой жизни или здоровья пациента либо третьих лиц. Также возможность изымать персональные данные без согласия фигуранта допускается в случае полной физической

невозможности заручиться таким разрешением (пациент недееспособен, недоступен для заверения своей воли, либо речь идет об уже умершем человеке). В любом случае к работе с персональной информацией допускаются исключительно медработники, имеющие соответствующую квалификацию и аттестованные по правилам Минздрава.

6.4. Первым техническим моментом организации обработки ПДн пациентов и персонала медучреждений является выполнение требований статьи 31 «Основы законодательства об охране здоровья». Пациент должен быть обязательно проинформирован о состоянии здоровья его организма (общий анамнез, симптомы заболеваний, предлагаемая терапия, все возможные риски, побочные эффекты, дополнительные финансовые траты, сроки проведения процедур, коррекция рабочего времени по недееспособности и т. д.). Причем эта информация должна быть подана в форме, доступной для понимания пациента. Это также касается лиц с ограниченными физическими возможностями. Это полностью пересекается со 143-й статьей закона о персональных данных – требованием, определяющим право на доступ к ПД как пациента, так и медперсонала.

7. Обязанности оператора ПДн

7.1. Клиника при сборе ПД по требованию может предоставить каждому пациенту следующую информацию (если такое требование им предъявляется), которая касается ПДн:

- подтверждение факта их обработки, ее цели;
- способы, применяемые оператором во время обработки ПДн;
- сведения о лицах, получивших доступ к этой информации и имеющих право на доступ к ней;
- список ПДн, необходимых для обработки в медучреждении, источник таких данных;
- срок, на протяжении которого эта информация будет обрабатываться, включая сроки ее хранения;
- данные о последствиях юридического характера для субъекта во время обработки ПДн;
- предоставление разъяснений о последствиях отказа пациента от предоставления своих ПДн, если это будет установлено как обязанность субъекта соответствующим федеральным законом.

7.2. При получении ПДн не от их субъекта оператор перед началом их обработки должен ознакомить пациента со следующей информацией:

- название (ФИО), адрес оператора, его представителя, предоставившего ПДн;
- цели их обработки, правовые аспекты таких действий;
- кому могут быть доступны ПДн (кто может пользоваться этими данными);
- права, установленные законом в отношении субъекта персональных данных.

8. Права пациентов и посетителей

8.1. Обеспечение безопасности ПДн пациентов и посетителей регламентируется не только техническими средствами. Любые данные, подпадающие под определение врачебной тайны, могут быть оглашены только с согласия пациента. Исключения описаны в статье 61 «Основ... об охране здоровья». Это требование полностью дублирует шестая статья ФЗ «О персональных данных». ПД должны передаваться только по защищенным каналам связи, которые позволяют уберечь эту информацию от утечки

8.2. Пациенты и посетители имеют право в отношении своих ПДн требовать их блокирования, уточнения, уничтожения, если эта информация является неполной, неактуальной, неверной, полученной незаконным путем, не нужна для заявленных целей обработки.

8.3. Пациент и посетитель имеют право на защиту своих прав, предусмотренных законодательством в отношении обработки, передачи, хранения персональных данных.

8.4. По запросу доступ к ПДн может быть предоставлен законному представителю пациента (ГК РФ ст. 26) – родителям, усыновителям, попечителям.
8.5. Законный представитель имеет право выполнять от имени носителя ПДн любые действия, а также определять лиц, которым будет разглашаться информация, являющаяся врачебной тайной пациента. Лицо, которое имеет право получить такие данные, не имеет никаких прав вступать в гражданские правоотношения от лица пациента.
8.6. В случае необходимости предоставления носителю ПДн срочной медпомощи, его согласие на обработку этой информации не требуется (в случае техногенных катастроф, стихийных бедствий, при реальной угрозе его жизни и здоровью).

9. Техническая часть

9.1. Необходимая оргтехника подбирается и поставляется в соответствии с рекомендациями контролирующих органов. Сбор данных, проводимый согласно законодательно установленным методикам, должен быть защищен на всех этапах. Спецификой работы медучреждений является сравнительно большая база по сравнению с муниципальными органами специализированных терминалов, связанных с хранением данных, передачей через Интернет, по локальным сетям различных типов.
9.2. Список разрешенных программных средств регулярно обновляет Минздрав и локальные отделы кибербезопасности. Размещение информсистем, приобретение, установка, работа специального оборудования, а также охрана таких помещений должны строиться на обеспечении полной сохранности носителей, на которых размещены ПДн, средств защиты такой информации. Организация работы с ПДн должна предусматривать все необходимые меры, исключающие возможность несанкционированного проникновения или нахождения в таких помещениях посторонних лиц.
9.3. Оператор обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных (ст. 19 Федерального закона № 152-ФЗ, Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»).

10. Уведомление в Роскомнадзор и внутреннее расследование

10.1. Обнаружив факт неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, оператор обязан в течение 24 часов сообщить в Роскомнадзор о произошедшем инциденте и о его предполагаемых причинах, о вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с Роскомнадзором по вопросам, связанным с выявленным инцидентом (п. 3.1 ст. 21 Федерального закона № 152-ФЗ).
10.2. Сообщение можно передать через Портал персональных данных, на котором Роскомнадзор организовал соответствующий сервис в разделе «Инциденты (утечки)» на странице «Уведомление о факте неправомерной или случайной передачи (предоставления,

распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных.

10.3. В оценке угроз и определении необходимых действий обеспечению защищенности ПДн помогут п. 6-16 Требований, утв. Постановлением Правительства РФ от 01.11.2012 г. № 1119 и Приказ ФСТЭК России от 18.02.2013 № 21.

10.4. Клиника обеспечивает третий уровень защищенности ПДн (при обработке, в том числе, биометрических персональных данных). С пациентов Клиника берет согласие на обработки и передачу биометрических данных.

10.5. Для обеспечения необходимого уровня защищенности в Клинике организованы (п. 14 Требований, утв. Постановлением Правительства РФ от 01.11.2012 г. № 1119):

- режим обеспечения безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечена сохранность носителей персональных данных;
- утвержден документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- используются средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.
- установлены сертифицированные средства защиты информации, включая антивирусное ПО (п. 12 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Приказом ФСТЭК России от 18.02.2013 № 21.
- назначено должностное лицо, ответственное за обеспечение безопасности персональных данных в информационной системе.

10.6. Исполняя пункт 10.5 настоящего Положения, Клиника может воспользоваться услугами сторонних квалифицированных организаций и специалистов. Согласно п. 5 ст. 6 Федерального закона № 152-ФЗ в случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет именно оператор

- **Если оператор ПДн предпринял необходимые усилия по защите ПДн, но их оказалось недостаточно, состава нарушения в его действиях не будет. В таком случае указывается в уведомлении причины, повлекшие нарушение прав субъектов персональных данных, которые оператор не мог контролировать.**
- Характеризуя персональные данные, пострадавшие в ходе инцидента, приводится в уведомлении информация о содержании скомпрометированной базы данных (категории субъектов персональных данных (например, работники, клиенты, контрагенты и др.), примерное количество записей, перечень категорий персональных данных (например, ФИО, дата рождения, данные документа, удостоверяющего личность, сведения об образовании и др.), актуальность базы данных, а также период, в течение которого собраны данные.
- При оценке роли оператора на первый план выходит вопрос соотношения нанесенного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом «О персональных данных» (пп. 5 п. 1 ст. 18.1 Федерального закона № 152-ФЗ).
- В уведомлении указываются принятые меры по устранению последствий инцидента. Они должны соответствовать требованиям ст. 18.1 и 19 Федерального закона № 152-ФЗ. В частности,

следует убедиться, что система защиты ПДн соответствует требованиям, восстановить ее функциональность; заняться восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

- Уведомив об инциденте в течение 24 часов с момента его выявления, нужно не забыть в течение 72 часов также проинформировать Роскомнадзор о результатах внутреннего расследования происшествия, а также предоставить сведения о виновниках (при наличии). Это можно сделать с помощью того же сервиса на портале персональных данных. В этом втором уведомлении нужно указать итоговую информацию о результатах внутреннего расследования, в том числе:
- о причинах, повлекших неправомерное распространение персональных данных;
- о нанесенном правам субъекта персональных данных вреде;
- об информационной системе, к которой был осуществлен несанкционированный доступ;
- о лицах, чьи действия стали причиной инцидента (ФИО и должность сотрудника оператора или ФИО, наименование, IP-адрес, предполагаемое местонахождение стороннего виновника, если эту информацию удалось установить);
- о дополнительных мерах, принятых по результатам внутреннего расследования (по устранению доступа, недопущению подобных инцидентов в будущем и иные);
- о решении оператора с указанием его реквизитов о проведении внутренней проверки.

10.7. Если системы оператора подверглись хакерской атаке, он, помимо вышеописанного взаимодействия с Роскомнадзором, обязан передать сведения о взломе, повлекшем неправомерную передачу (предоставление, распространение, доступ) персональных данных, в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (т. н. ГосСОПКА) (п. 12 ст. 19 Федерального закона № 152-ФЗ). Эта обязанность для большинства операторов персональных данных новая – она появилась с 01.09.2022.

10.8. О самой системе ГосСОПКА можно прочесть в ст. 5 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

10.9. Оператором системы является Национальный координационный центр по компьютерным инцидентам (НКЦКИ).

10.10. В настоящее время применяется Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

10.11. Оператору персональных данных, не являющемуся субъектом критической информационной инфраструктуры, достаточно в течение 24 часов с момента обнаружения компьютерного инцидента передать информацию о нем посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на его официальном сайте в разделе «Сообщить об инциденте».

11. Заключительные положения

Иные права и обязанности Клиники в связи с ПДн определяются законодательством Российской Федерации в области персональных данных. Сотрудники Клиники, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско- правовую или уголовную ответственность в порядке, установленном федеральными законами.