Положение по обеспечению безопасности персональных данных.

О мерах, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 г. №152 ФЗ «О персональных данных», Федеральным законом от 27.07.2006 г. №149 ФЗ «Об информации, информационных технологиях и о защите информации», и принятыми с соответствии с ними нормативными правовыми актами.

В соответствии с главой 4, главой 5 Федерального закона от 27.07.2006 г. №152 ФЗ «О персональных данных», статьями 9, 11, 12, 13, 14, 15, 16, 17 Федерального закона от 27.07.2006 г. №149 ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 01.11. 2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и постановлением Правительства Российской федерации от 21 марта 2012 г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ними нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.

Правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований

1. Настоящие Правила обработки персональных данных устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований (далее - Правила).

Обработка персональных данных выполняется с использованием средств автоматизации или без использования таких средств с персональными данными в учреждении, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных субъектов, персональные данные которых обрабатываются в учреждении.

2. ГУЗ «Детская поликлиника № 5» в соответствии с Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных» является оператором, осуществляющим обработку персональных данных, а также определяющим цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (далее - оператор персональных данных).

3. Правила разработаны в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее - Федеральный закон).

3.1. Установить всю информацию, касающуюся фактов обращения за медицинской помощью, о состоянии здоровья, диагнозе и иных сведений, полученных при обследовании и лечении и составляющих врачебную тайну, а также любую другую документированную информацию, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу или пользователю - как информацию ограниченного доступа (п.3 ст. 6 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации», ст. 13 Федерального закона от 21 ноября 2011 года №323-ФЗ «Об основах охраны здоровья граждан в российской федерации»)

4. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных:

а) осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных;

б) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых учреждением мер, направленных на обеспечение выполнения обязанностей оператора персональных данных, предусмотренных Федеральным законом;

в) ознакомление сотрудников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, с требованиями по защите персональных данных.

5. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором персональных данных, оператор персональных данных в срок, не превышающий 3 рабочих дня с даты выявления неправомерной обработки персональных данных, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных.

В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор персональных данных в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении неправомерной обработки персональных данных или об уничтожении персональных данных оператор персональных данных обязан уведомить субъекта персональных данных или его представителя.

6. В случае достижения цели обработки персональных данных оператор персональных данных обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 30 рабочих дней с даты достижения цели обработки персональных данных.

7. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор персональных данных обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 3 рабочих дней с даты получения указанного отзыва. Об уничтожении персональных данных, оператор персональных данных в течении3 рабочих дней обязан уведомить субъекта персональных данных.

8. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных в пунктах 5-7 Правил, оператор персональных данных осуществляет блокирование таких персональных данных, обеспечивает уничтожение персональных данных в срок до 6 месяцев, если иной срок не установлен действующим законодательством Российской Федерации.

9. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели хранения персональных данных, если срок хранения персональных данных не установлен Федеральным законом.

Обрабатываемые персональные данные подлежат уничтожению по достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом.

10. Обработка персональных данных в информационных системах учреждения (далее - информационные системы персональных данных) осуществляется в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

11. Обеспечение безопасности персональных данных в информационных системах персональных данных достигается путем:

а) определения угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

б) применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

в) применения прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

г) оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационных систем персональных данных;

д) учета машинных носителей персональных данных;

е) обнаружения фактов несанкционированного доступа к персональным данным и принятием мер по прекращению несанкционированного доступа;

ж) восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

з) установления правил доступа (пароль, логин и др.) к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечения регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных.

12. Сотрудники, имеющие доступ к информационным системам персональных данных, обязаны:

а) принимать меры, исключающие несанкционированный доступ к используемым программно-техническим средствам;

б) вести учет электронных носителей информации, содержащих персональные данные, и осуществлять их хранение в металлических шкафах или сейфах;

в) производить запись персональных данных (отдельных файлов, баз данных) на электронные носители только в случаях, регламентированных порядком работы с персональными данными;

г) соблюдать установленный порядок и правила доступа в информационные системы, не допускать передачу персональных кодов и паролей к информационным системам персональных данных;

д) принимать все необходимые меры к надежной сохранности кодов и паролей доступа к информационным системам персональных данных;

е) работать с информационными системами персональных данных в объеме своих полномочий, не допускать их превышения;

ж) обладать навыками работы с антивирусными программами в объеме, необходимом для выполнения функциональных обязанностей и требований по защите информации.

13. При работе сотрудников на персональном компьютере, в том числе для доступа к информационным системам персональных данных, запрещается:

а) записывать значения кодов и паролей доступа к информационным системам персональных данных;

б) передавать коды и пароли доступа к информационным системам персональных данных другим лицам;

в) пользоваться в работе кодами и паролями других пользователей доступах информационным системам персональных данных;

г) производить подбор кодов и паролей доступа к информационным системам персональных данных других пользователей;

д) записывать на электронные носители с персональными данными посторонние программы и данные;

е) копировать информацию с персональными данными на неучтенные электронные носители информации;

ж) выносить электронные носители с персональными данными за пределы территории учреждения без согласования с непосредственным начальником;

з) покидать рабочее место с включенным персональным компьютером без применения аппаратных или программных средств блокирования доступа к персональному компьютеру;

и) приносить, самостоятельно устанавливать и эксплуатировать на персональном компьютере любые программные продукты, не принятые к эксплуатации;

к) открывать, разбирать, ремонтировать персональные компьютеры, вносить изменения в конструкцию, подключать нештатные блоки и устройства;

л) передавать информацию, содержащую персональные данные, подлежащие защите, по открытым каналам связи (факсимильная связь, электронная почта и иное), а также использовать сведения, содержащие персональные данные, подлежащие защите, в открытой переписке и при ведении переговоров по телефону.

14. Порядок использования носителей информации:

а) Под использованием носителей информации понимается их подключение к инфраструктуре с целью обработки, приема/передачи информации между рабочей станцией и носителями информации.

б) Допускается использование только учтенных носителей информации, которые поставлены на бухгалтерский учет и подвергаются регулярной ревизии и контролю.

15. Порядок учета, хранения и обращения со съемными носителями конфиденциальной информации (персональных данных), твердыми копиями и их утилизации:

а) Все находящиеся на хранении и в обращении съемные носители с конфиденциальной информацией (персональными данными) подлежат учёту.

б) Каждый съемный носитель с записанными на нем конфиденциальной информацией ('персональными данными) должен иметь этикетку, на которой указывается его уникальный учетный номер.

в) Хранение съемных носителей информации разрешено исключительно в запираемых шкафах, сейфах, исключающее возможность неправомерного доступа к ним.

16. Утвердить категории персональных данных:

16.1 Для пациентов учреждения - Ф.И.О., пол, дата рождения, адрес места жительства, реквизиты документа, удостоверяющего личность, реквизиты полиса медицинского страхования, сведения о наличии льгот, СНИЛС, сведения о случаях обращения за медицинской помощью, данные о состоянии здоровья.

16.2 Для сотрудников учреждения - Ф.И.О., пол, дата и место рождения, адрес места жительства, реквизиты документа, удостоверяющего личность, реквизиты полиса медицинского страхования, СНИЛС, ИНН, сведения о наличии льгот, данные кадрового учёта, сведения о заработной плате.

17. Сроки хранения документов с персональными данными

Вид документа	**Срок хранения**
Сведения, справки о совокупном доходе работников за год и уплате налогов. Документы о начисленных и перечисленных суммах налогов, об освобождении от них, о предоставленных льготах, отсрочках по уплате налогов.	5 лет
Лицевые счета работников	75 лет
Личные дела: - руководителя организации, членов руководящих, исполнительных, контрольных органов организации, а также работников, имеющих государственные и иные звания, премии, награды, ученые степени - остальных работников	Постоянно
Трудовые договоры, трудовые соглашения, не вошедшие в состав личных дел, личные карточки работников (включая временных)	75 лет
Документы лиц, не принятых на работу	1 год
Перечень лиц, имеющих право подписи первичных документов	До замены новыми
Положения, инструкции о правах и обязанностях должностных лиц (должностные инструкции) типовые	Постоянно
Положения, инструкции о правах и обязанностях должностных лиц (должностные инструкции)	75 лет
Коллективные договоры	Не менее 10 лет
Табели (графики), журналы учета рабочего времени	5 лет
Документы о премировании	5 лет

Штатные расписания и изменения к ним по месту разработки и/или утверждения	Не менее 10 лет
Личные карточки работников (в том числе временных)	75 лет
Медицинская карта пациента, получающего медицинскую помощь в амбулаторных условиях	25 лет

19. Сотрудники, виновные в разглашении или утрате информации, содержащей персональные данные, несут ответственность в соответствии с законодательством Российской Федерации.

20. Контроль над исполнением сотрудниками требований настоящих Правил возлагается на руководителей структурных подразделений учреждения и назначенного приказом главного врача ответственного лица за организацию обработки персональных данных.

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора

1. Настоящими Правилами определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.
2. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных организовывается проведение плановых и внеплановых проверок условий обработки персональных данных на предмет соответствия Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных», принятым в соответствии с ним нормативным правовым актам и локальным актам ГУЗ «Детская поликлиника № 5» (далее - проверки).
3. Проверки проводятся в учреждении на основании ежегодного плана или на основании поступившего в учреждение письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки).
4. В плане по каждой проверке устанавливается объект внутреннего контроля, проверяемый период, срок проведения проверки, ответственные исполнители.
5. Проверки проводятся комиссией, создаваемой приказом главного врача.
6. Основанием для проведения внеплановой проверки является поступившее в учреждение письменное обращение субъекта персональных данных или его представителя о нарушении правил обработки персональных данных.
7. Проведение внеплановой проверки организуется в течение 3 рабочих дней с момента поступления обращения.
8. Срок проведения проверки не может превышать месяц со дня принятия решения о ее проведении.
9. Члены комиссии, получившие доступ к персональным данным субъектов персональных данных в ходе проведения проверки, обеспечивают конфиденциальность персональных данных субъектов персональных данных, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных.
10. По существу поставленных в обращении (жалобе) вопросов комиссия в течение 5 рабочих дней со дня окончания проверки дает письменный ответ заявителю.