УТВЕРЖДАЮ
Главный врач
ОГБУЗ «Клиническая больница №1»
_____ Крюковский С.Б.
«16» 01 2017 г.

ПОЛИТИКА
в отношении обработки персональных данных в областном государственном бюджетном учреждении здравоохранения «Клиническая больница №1»

1. Общие положения

1.1 Политика в отношении обработки персональных данных в ОГБУЗ «Клиническая больница №1» (далее – Политика) разработана в соответствии с действующим законодательством Российской Федерации в области персональных данных и целями, задачами, принципами обеспечения безопасности персональных данных в ОГБУЗ «Клиническая больница №1».

1.2 Целью Политики является обеспечение безопасности объектов защиты ОГБУЗ «Клиническая больница №1» от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

1.3 Политика устанавливает ответственность руководства, а также определяет подход организации к управлению информационной безопасностью.

1.4 В Политике определены требования к сотрудникам учреждения, степень их ответственности, структура и необходимый уровень защищенности информационных систем персональных данных и объектов информатизации, статус и должностные

обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ОГБУЗ «Клиническая больница №1».

1.5 Требования Политики распространяются на всех сотрудников ОГБУЗ «Клиническая больница №1» (штатных, временных и т.п.), а также всех прочих лиц (подрядчики, разработчики информационных систем, ремонтные организации и т.п.).

1.6 Настоящая Политика определяет принципы, порядок и условия обработки персональных данных пациентов и работников учреждения, с целью обеспечения 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, а также устанавливает ответственность должностных лиц учреждения, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

2. Основания и цели обработки персональных данных

2.1 ОГБУЗ «Клиническая больница №1» осуществляет обработку персональных данных в соответствии с Конституцией Российской Федерации, Основами законодательства Российской Федерации об охране здоровья граждан (утвержденными ВС РФ 22 июля 1993 года № 5487-1), Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», ст. ст. 85-90 Трудового кодекса Российской Федерации, «Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119, «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным Постановлением Правительства РФ от 15 сентября 2008 года № 687, Лицензией № ФС-67-01-000859 от 11 февраля 2016 г, Уставом.

2.2 Обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, определения профессиональной пригодности, оказания медицинских и медико-социальных услуг.

2.3 В ОГБУЗ «Клиническая больница №1» обрабатываются следующие категории персональных данных:

- специальная категория персональных данных пациентов, касающаяся состояния здоровья, защиты законных прав и интересов граждан при оказании им медико-профилактических услуг, установления медицинского диагноза, оказания медицинских и медико-социальных услуг;
- персональные данные сотрудников, позволяющих идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением специальной категории персональных данных в целях осуществления и выполнения, возложенных законодательством Российской Федерации, на оператора функций, полномочий и обязанностей по выполнению трудового законодательства, осуществления бухгалтерской и кадровой деятельности.

3. Принципы и условия обработки персональных данных

3.1 Обработка персональных данных ОГБУЗ «Клиническая больница №1» осуществляется на основе принципов:

- законности и справедливости целей и способов обработки персональных данных;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения, созданных для несовместимых между собой целей баз данных, содержащих персональные данные;
- хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки;
- уничтожения по достижении целей обработки персональных данных.

3.2 Обработка персональных данных пациентов осуществляется с письменного согласия субъекта персональных данных на обработку его персональных данных, а также

если обработка персональных данных необходима для исполнения договора, стороной которого является субъект персональных данных.

3.3 Если получение согласия субъекта персональных данных невозможно, то обработка персональных данных осуществляется, только если она необходима для защиты жизни и здоровья или иных жизненно важных интересов субъекта персональных данных.

3.4 Обработка персональных данных сотрудников осуществляется в соответствии с заключенным трудовым договором.

3.5 Доступ к обрабатываемым персональным данным, предоставляется только тем сотрудникам учреждения, которым он необходим в связи с исполнением ими своих должностных обязанностей и с соблюдением принципов персональной ответственности.

3.6 Прекращение неавтоматизированной обработки персональных данных пациентов и уничтожение документов, содержащих персональные данные, осуществляется по истечению сроков хранения первичных медицинских документов пациента, которые составляют от одного года до двадцати пяти лет с момента оказания последней медицинской услуги.

3.7 Прекращение автоматизированной обработки персональных данных пациентов в информационных подсистемах персональных данных осуществляется:

- по письменному требованию пациента, немедленно, после завершения производства расчетов за оказанные медицинские и медико-социальные услуги;
- по истечению сроков хранения первичных медицинских документов пациента и составляют от одного года до двадцати пяти лет.

3.8 Прекращение автоматизированной и неавтоматизированной обработки персональных данных работников, осуществляется в следующих случаях:

- прекращение договорных отношений с работниками и физическими лицами;
- ликвидация учреждения.

3.9 Уничтожение документов, содержащих персональные данные работников, осуществляется по истечению сроков их хранения, которые регламентируются

Федеральным законом от 21.11.1996 г. № 129-ФЗ «О бухгалтерском учете», Налоговым кодексом Российской Федерации от 31.07.1998 г. № 146-ФЗ и Перечнем типовых архивных документов, образующихся в научно-технической и производственной деятельности организаций, с указанием сроков хранения, утвержденным Министерством культуры и массовых коммуникаций Российской Федерации 31 июля 2007 года № 1182.

3.10 Передача персональных данных третьим лицам:

- передача информации, содержащей персональные данные пациентов, осуществляется в организации и учреждения, с которыми заключены договора на оказание медицинских услуг и ведущих расчеты (отчетность) за оказанные медицинские и медико-социальные услуги, с согласия субъекта персональных данных;
- передача информации содержащей персональные данные сотрудников осуществляется в соответствии с Федеральным законом от 21.11.1996 г. № 129-ФЗ «О бухгалтерском учете», Налоговым кодексом Российской Федерации от 31.07.1998 г. № 146-ФЗ, Трудовым Кодексом Российской Федерации от 30.12.2001 № 197-ФЗ.

3.11 Передача информации, содержащей персональные данные, третьим лицам осуществляется с использованием автоматизированных информационных систем по закрытым средствами криптографической защиты каналам связи и методом физической доставки адресату в распечатанном виде.

4. Обеспечение безопасности персональных данных

4.1 Важнейшим условием реализации целей деятельности ОГБУЗ «Клиническая больница №1» является обеспечение необходимого и достаточного уровня безопасности информационных систем персональных данных, соблюдения конфиденциальности, целостности и доступности обрабатываемых персональных данных и сохранности носителей сведений, содержащих персональные данные на всех этапах работы с ними.

4.2 В ОГБУЗ «Клиническая больница №1» создаются условия и режим защиты информации, отнесенной к персональным данным, позволяющие обеспечить защиту обрабатываемых персональных данных.

4.3 В ОГБУЗ «Клиническая больница №1» в соответствии с действующим законодательством Российской Федерации разрабатывается и вводится в действие

комплекс организационно-распорядительных, функциональных и планирующих документов, регламентирующих и обеспечивающих безопасность обрабатываемых персональных данных:

- Концепция и политика информационной безопасности;
- Положение по обработке и защите персональных данных;
- Положение о внутриобъектовом, охранном и пропускном режиме;
- Положение по организации режима защиты помещений;
- Положение по разграничению доступа к персональным данным;
- Положение по резервированию и восстановлению баз персональных данных;
- Положения об архивах;
- Инструкции по ведению медицинских архивов, архивов материалов лучевой диагностики, архивов управленческой документации;

4.4 Разрабатывается перечень персональных данных, подлежащих защите. Выделяются информационные системы персональных данных и проводится их классификация.

4.5 Для формирования обоснованных требований к обеспечению безопасности обрабатываемых персональных данных и проектирования системы защиты персональных данных разрабатываются частные модели угроз безопасности для каждой информационной системы персональных данных.

4.6 Определяется перечень помещений, предназначенных для обработки и хранения персональных данных, перечень средств вычислительной техники, на которых разрешается обрабатывать персональные данные.

4.7 Вводится режим безопасности обработки и обращения с персональными данными, а также режим защиты помещений, в которых осуществляется обработка и хранение носителей персональных данных;

4.8 Назначаются ответственный за организацию и обеспечение безопасности персональных данных, администраторы информационных систем персональных данных и администратор безопасности информационных систем персональных данных, им определяются обязанности и разрабатываются инструкции по обеспечению безопасности информации;

4.9 Определяется круг лиц, имеющих право обработки персональных данных, разрабатываются инструкции пользователям по защите персональных данных, антивирусной защите, действиям в кризисных ситуациях;

4.10 Определяются требования к персоналу, степень их ответственности, за обеспечение безопасности персональных данных.

4.11 Проводится ознакомление работников, осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации по обеспечению безопасности персональных данных и требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных. Проводится периодическое обучение указанных работников правилам обработки персональных данных.

4.12 Предпринимаются необходимые и достаточные технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий:

4.13 Вводится система разграничения доступа;

4.14 Устанавливается защита от несанкционированного доступа к автоматизированным рабочим местам, информационным сетям и базам персональных данных;

4.15 Устанавливается защита от вредоносного программно-математического воздействия;

4.16 Осуществляется регулярное резервное копирование информации и баз данных;

4.17 Передача информации по сети общего пользования «Интернет» осуществляется с использованием средств криптографической защиты информации;

4.18 Организовывается система контроля за порядком обработки персональных данных и обеспечения их безопасности. Планируются проверки соответствия системы защиты персональных данных, аудит уровня защищенности персональных данных в информационных системах персональных данных, функционирования средств защиты информации, выявления изменений в режиме обработки и защиты персональных данных.

5. Права

5.1 Права ОГБУЗ «Клиническая больница №1»:

- предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);
- отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством;
- использовать персональные данные субъекта без его согласия в случаях, предусмотренных законодательством.

5.2 Права субъекта персональных данных:

- требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- требовать перечень своих персональных данных, обрабатываемых учреждением и источник их получения;
- получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения;
- требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

6. Заключительные положения

6.1 Настоящая Политика является общедоступной и подлежит размещению на официальном сайте или иным образом обеспечивается неограниченный доступ к данной Политике.

6.2 Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года.

6.3 Контроль исполнения требований настоящей Политики осуществляется ответственным за обеспечение безопасности персональных данных ОГБУЗ «Клиническая больница №1».

6.4 Ответственность должностных лиц ОГБУЗ «Клиническая больница №1», имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами ОГБУЗ «Клиническая больница №1».