Утверждена Приказом главного врача
ГБУЗ АО «АГКП №1»
_____Фоминой А.С.
от «28» ноября 2016 г. № 505

ПОЛИТИКА
информационной безопасности обработки персональных данных в ГБУЗ Архангельской области «Архангельская городская клиническая поликлиника №1»

1. Общие положения

1.1. Настоящая Политика информационной безопасности обработки персональных данных (далее – Политика) разработана в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ) и определяет порядок обработки персональных данных и меры по обеспечению безопасности персональных данных в ГБУЗ Архангельской области «Архангельская городская клиническая поликлиника №1» (далее – Учреждение) с целью обеспечения защиты прав и свобод гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную, семейную и врачебную тайну.

1.2. В настоящей Политике используются следующие термины и определения:

– персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъект персональных данных);

– субъект персональных данных – сотрудник Учреждения или пациент Учреждения;

– обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

– автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

– распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

– предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

– блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

– уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

– обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

– информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

– трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

– общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

1.3. Действие политики распространяется на все персональные данные субъектов, обрабатываемые в ГБУЗ Архангельской области «Архангельская городская клиническая поликлиника №1» с использованием средств автоматизации, а также без использования таких средств.

1.4. Настоящая Политика является общедоступной и должна иметь неограниченный доступ всех субъектов персональных данных.

2. Принципы и условия обработки персональных данных.

2.1. Целями сбора, накопления, обработки и систематизации персональных данных является:

2.1.1. Осуществление кадровой работы в Учреждении в соответствии с требованиями трудового законодательства Российской Федерации;

2.1.2. Оказание медицинских услуг пациентам в соответствии с Федеральным законом от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

2.2. Обработка персональных данных в Учреждении осуществляется на основе следующих принципов:

– законной и справедливой основы;

– ограничения обработки персональных данных достижением конкретных, заранее определенных и законных целей;

– недопущения обработки персональных данных, несовместимой с целями их обработки;

– недопущение объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

– обработки только тех персональных данных, которые отвечают целям их обработки;

– соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки;

– недопущения обработки избыточных персональных данных по отношению к заявленным целям их обработки;

– обеспечения точности, достаточности и актуальности персональных данных по отношению к целям обработки персональных данных.

2.3. Учреждение осуществляет обработку персональных данных только с письменного согласия работников и пациентов – субъектов персональных данных на обработку их персональных данных.

2.4. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

3. Обрабатываемые персональные данные.

3.1. Учреждение осуществляет обработку персональных данных работников Учреждения с письменного согласия в случаях, установленных ст. 11 Закона №152-ФЗ.

3.2. Обработка специальных категорий персональных данных, касающихся состояния здоровья, ведется на пациентов при оказании медицинской услуги. Обработка ведется с письменного согласия пациента в соответствии со ст. 6, 9, 10 Закона № 152-ФЗ, ч. 3 ст. 13 Закона № 323-ФЗ.

3.3. В целях информационного обеспечения в Учреждении создаются общедоступные источники персональных данных, в том числе справочники, адресные и телефонные книги. В общедоступные источники персональных данных с согласия работника могут включаться его фамилия, имя, отчество, дата и место рождения, должность, номера контактных телефонов, адреса электронной почты и иные персональные данные, сообщаемые субъектом персональных данных.

4. Условия обработки персональных данных, их хранения и передачи третьим лицам.

4.1. Обработка персональных данных.

4.1.1. Работники Учреждения, допущенные к обработке персональных данных на основании правовых актов Учреждения и должностных регламентов, осуществляют обработку персональных данных после ознакомления с нормативными актами Учреждения, регламентирующими порядок и процедуры работы с персональными данными.

4.1.2. Доступ к персональным данным работников имеют:

– руководители структурных подразделений (к данным работников своего подразделения)

– специалисты отдела кадров и бухгалтерии – к тем данным, которые необходимы им для выполнения конкретных функций.

4.2. Хранение персональных данных.

4.2.1. Персональные данные хранятся в электронном виде в составе информационных систем персональных данных (далее – ИСПДн), в составе архивных копий баз данных ИСПДн и на бумажных носителях.

4.2.2. При обработке и хранении персональных данных соблюдаются организационные и технические меры, обеспечивающие их сохранность и исключающие несанкционированный доступ к ним, к которым относятся:

– назначение работника Учреждения, ответственного за организацию обработки персональных данных, и за обеспечение безопасности персональных данных при их обработке в ИСПДн;

– ограничение физического доступа к местам хранения персональных данных в бумажном виде и носителях информации в электронном виде;

– соблюдение правил обработки персональных данных в ИСПДн;

– применение сертифицированных средств защиты информации.

4.3. Передача персональных данных.

4.3.1. Для достижения целей обработки персональных данных субъектов, Учреждение может передавать персональные данные третьим лицам:

1) Персональные данные работников Учреждения

В соответствии с требованиями Трудового Кодекса РФ (Федеральный закон от 30.12.2001 г. № 197-ФЗ) только с письменного согласия работника (ст. 88);

- в Федеральную инспекцию по труду (ст. 357 ТК РФ);

- в органы государственного контроля и надзора за соблюдением законов о труде (ст. 357, 366-369 ТК РФ);

- в Пенсионный фонд (ФЗ-27 от 01.04.1996 г.);

- в Фонд социального страхования (ФЗ-125 от 24.07.1998 г.);

- в налоговые органы (ст. 24 налогового кодекса РФ);

- в рамках договора (контракта), предусматривающего обеспечение конфиденциальности и безопасности полученных сведений (банки (ст. 136 ТК РФ), страховые компании, организации, осуществляющие сопровождение ИСПДн).

2) Персональные данные пациентов

- при поступлении запросов от уполномоченных государственных органов, в рамках действующего законодательства (пункт 3, части 4, ст. 13 Федерального закона от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в РФ»);

- персональные данные без письменного согласия пациента – субъекта персональных данных передаются в случаях, установленных п. 7.7. ст. VII Постановления главного санитарного врача РФ от 11.01.2011 г. № 1;

- в территориальных фонд ОМС, если помощь оказывается по программе обязательного медицинского страхования в соответствии со ст. 38, 39, 43, 44, 48 Федерального закона от 29.11.2010 г. № 326-ФЗ «Об обязательном медицинском страховании» и единый донорский центр региона по защищенной модемной линии.

5. Обеспечение безопасности персональных данных

Обеспечение безопасности персональных данных в Учреждении достигается следующими мерами:

5.1. Назначение работника Учреждения, ответственного за организацию обработки персональных данных, и за обеспечение безопасности персональных данных при их обработке в ИСПДн;

5.2. Определение угроз безопасности персональных данных, разработка на их основе частной модели угроз безопасности персональных данных и разработка системы защиты персональных данных для соответствующего класса ИСПДн;

5.3. Назначение администраторов безопасности ИСПДн;

5.4. Реализация разрешительной системы доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты информации;

5.5. Применение сертифицированных средств защиты информации;

5.6. Осуществление антивирусного контроля;

5.7. Парольная защита доступа к ИСПДн;

5.8. Резервное копирование;

5.9. Обеспечение восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5.10. Ведение электронного журнала регистрации действий пользователей ИСПДн;

5.11. Разработка и утверждение локальных актов Учреждения, регламентирующих порядок обработки персональных данных, разработка инструкций;

5.12. Обучение работников Учреждения, допущенных к обработке персональных данных, и использующих средства защиты информации, правилам работы с ними;

5.13. Проведение периодических проверок состояния защищенности ИСПДн.

6. Права субъекта персональных данных

6.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, за исключением случаев, когда право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральным законодательством.

6.2. Субъект персональных данных имеет право на получение следующей информации:

– правовые основания и цели обработки персональных данных;

– применяемые способы обработки персональных данных;

– подтверждение факта обработки персональных данных;

– сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора (контракта) или на основании федерального законодательства;

– обрабатываемые персональные данные, относящиеся к субъекту персональных данных, источник их получения;

– иных сведений, предусмотренных Законом № 152-ФЗ.

6.3. Получение данной информации осуществляется на основании письменного запроса субъекта персональных данных в Учреждение.

6.4. Ответ, содержащий запрашиваемую информацию либо мотивированных отказ в ее предоставлении направляется субъекту по адресу, указанному в запросе, в течение 30 дней.

6.5. Порядок обработки запросов субъектов персональных данных по выполнению их законных прав осуществляется в соответствии с локальными актами Учреждения.

7. Обязанности

7.1. Работники Учреждения обязуются осуществлять обработку персональных данных только с согласия субъектов персональных данных, за исключением случаев, предусмотренных Законом № 152-ФЗ.

7.2. При сборе персональных данных Учреждение обязуется по запросу субъекта персональных данных предоставлять последнему информацию, касающуюся обработки его персональных данных, в соответствии с положениями настоящей Политики. В случае, если предоставление персональных данных субъектов персональных данных является обязательным в соответствии с федеральным законодательством, Учреждение обязуется разъяснять субъекту персональных данных юридические последствия отказа от предоставления персональных данных.

7.3. Учреждение при обработке персональных данных обязуется принимать необходимые правовые, организационные и технические меры 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.

7.4. Учреждение обязуется отвечать на запросы субъектов персональных данных, их законных представителей, а также уполномоченного органа по защите прав субъектов персональных данных в части обрабатываемых персональных данных в соответствии с требованиями законодательства.

7.5. В случае предоставления субъектом персональных данных либо его представителем сведений, подтверждающих факты каких-либо нарушений в процессе обработки персональных данных, Учреждение обязуется устранить данные нарушения в течение семи рабочих дней и уведомить субъекта персональных данных о внесенных изменениях и принятых мерах.

8. Ответственность за нарушение норм, регулирующих обработку персональных данных.

8.1. Разглашение персональных данных работника ГБУЗ АО «АГКП №1», то есть передача посторонним лицам, не имеющим к ним доступа; публичное раскрытие; утрата документов и иных носителей, содержащих персональные данные работника; иные нарушения обязанностей по их защите, обработке и хранению, установленным настоящим Положением, а также иными локальными нормативными актами ГБУЗ АО «АГКП №1», лицом, ответственным за получение, обработку и защиту персональных данных работника, - влекут наложение на него дисциплинарного взыскания (выговора, увольнения по пп. "в" п. 6 ч. 1 ст. 81 ТК РФ).

8.2. В случае причинения ущерба ГБУЗ АО «АГКП №1» работник, имеющий доступ к персональным данным сотрудников и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в соответствии с п. 7 ч. 1 ст. 243 ТК РФ.

8.3. Административная ответственность за нарушение положений законодательства Российской Федерации в области персональных данных предусмотрена статьями 5.39, 13.11, 13.12, 13.13, 13.14, 19.7 КоАП РФ.

8.4. Уголовная ответственность за нарушение положений законодательства Российской Федерации в области персональных данных предусмотрена статьями 137, 140, 272 Уголовного Кодекса Российской Федерации.

9. Изменение Политики.

В целях обеспечения эффективности осуществления мероприятий по обработке персональных данных, настоящая Политика подлежит пересмотру и актуализации не реже одного раза в три года с момента ее опубликования.

Политика подлежит внеплановому пересмотру в случае существенных изменений законодательства в области защиты персональных данных.