«УТВЕРЖДАЮ»
ВрИО Главного врача
ГБУЗ КК «ПК ГРД»

А. А. Сивак
«24» июля 2013 г.

ПОЛОЖЕНИЕ О ЗАЩИТЕ

ПЕРСОНАЛЬНЫХ ДАННЫХ В ГБУЗ КК «ПК ГРД»

1. Общие положения

1.1. Цель данного Положения - защита в государственном бюджетном учреждении здравоохранения Камчатского края «Петропавловск-Камчатский городской родильный дом» – лечебно-профилактическом учреждении охраны материнства и детства (далее ГБУЗ КК «ПК ГРД») персональных данных от несанкционированного доступа.

1.2. Сбор, хранение, использование и распространение информации о частной жизни лица без письменного его согласия не допускаются. Персональные данные требуют безопасной обработки.

1.3. Режим безопасной обработки персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

1.4. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому сотруднику возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

1.5. Должностные лица, в обязанность которых входит ведение персональных данных пациента, обязаны обеспечить каждому пациенту возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

1.6. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной

принадлежности запрещено и карается в соответствии с законодательством.

1.7. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

1.8. Неправомерность деятельности органов государственной власти и организаций по сбору персональных данных может быть установлена в судебном порядке по требованию субъектов, действующих на основании статей 14 и 15 Федерального закона и законодательства о персональных данных.

1.9. Настоящее положение является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным сотрудника или пациента.

2. Понятие и состав персональных данных.

2.1. Персональные данные – информация о физических лицах (далее – субъекты), необходимая ГБУЗ КК «ПК ГРД» в связи с исполнением трудовых, медицинских и прочих договорных отношений и касающаяся конкретного гражданина.

2.2. Состав Персональных данных сотрудника:

- образование;
- сведения о трудовом и общем стаже;
- сведения о доходах и вознаграждениях;
- паспортные данные (фамилия, имя, отчество, дата рождения, прописка, серия и номер паспорта, где и кем выдан паспорт, сведения о ранее выданных паспортах);
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- специальность;
- занимаемая должность;
- адрес по регистрации;
- домашний или мобильный телефон;
- содержание трудового договора;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- номер ПФР;
- индивидуальный налоговый номер;

- копии отчетов, направляемые в органы статистики.

2.3.Состав персональных данных пациента:

- Фамилия;
- Имя;
- Отчество;
- Пол;
- Дата рождения;
- Паспортные данные (серия, номер, место и дата выдачи);
- Адрес места регистрации;
- Адрес места жительства;
- Контактные телефоны;
- Реквизиты полиса ОМС (ДМС);
- Страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС);
- Данные о состоянии здоровья, заболеваниях, случаях обращения – в медико-профилактических целях, в целях установления медицинского диагноза и оказания медицинских услуг;
- сведения о месте работы;
- занимаемая должность;

3. Обязанности ГБУЗ КК «ПК ГРД»

3.1. В целях обеспечения прав и свобод человека и гражданина ГБУЗ КК «ПК ГРД» и её представители при обработке персональных данных обязаны соблюдать следующие общие требования:

3.1.1. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов;

3.1.2. При определении объема и содержания обрабатываемых персональных данных ГБУЗ КК «ПК ГРД» должно руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами;

3.1.3. При принятии решений, затрагивающих интересы субъекта, ГБУЗ КК «ПК ГРД» не имеет права основываться на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения;

3.1.4. Защита персональных данных субъекта от неправомерного их использования или утраты должна быть обеспечена ГБУЗ КК «ПК ГРД» за счет его средств в порядке, установленном федеральным законом;

3.1.5. Сотрудники ГБУЗ КК «ПК ГРД», принимающие участие в обработке персональных данных субъекта, и их представители

должны быть ознакомлены под расписку с документами ГБУЗ КК «ПК ГРД», устанавливающими порядок обработки персональных субъекта, а также об их правах и обязанностях в этой области;

3.1.6. Субъекты не должны отказываться от своих прав на сохранение и защиту тайны.

4. Обязанности работников ГБУЗ КК «ПК ГРД»

4.1. Передавать ГБУЗ КК «ПК ГРД» или представителю ГБУЗ КК «ПК ГРД» комплекс достоверных документированных персональных данных, состав которых установлен Трудовым кодексом РФ;

4.2. Своевременно сообщать ГБУЗ КК «ПК ГРД» об изменении своих персональных данных.

4.3. Соблюдать все требования ГБУЗ КК «ПК ГРД» по защите персональных данных.

5. Права субъекта персональных данных

5.1. Требовать исключения или исправления неверных или неполных персональных данных;

5.2. На свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;

5.3. Персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;

5.4. Определять своих представителей для защиты своих персональных данных;

5.5. На сохранение и защиту своей личной, семейной и медицинской тайны.

6. Сбор, обработка и хранение персональных данных

6.1. Обработка персональных данных субъекта – получение, хранение, комбинирование, передача или любое другое использование персональных данных субъекта.

6.2. Порядок получения персональных данных.

6.2.1. Все персональные данные следует получать у субъекта персональных данных. Если персональные данные возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. ГБУЗ КК «ПК ГРД» должно сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере

подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

6.2.2. ГБУЗ КК «ПК ГРД» не имеет права получать и обрабатывать персональные данные субъекта о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации, ГБУЗ КК «ПК ГРД» вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия. В случаях, непосредственно связанных с вопросами медицинских отношений, в соответствии со статьей 24 Конституции Российской Федерации, ГБУЗ КК «ПК ГРД» вправе получать и обрабатывать данные о частной жизни пациента только с его письменного согласия.

6.3. Обработка, передача и хранение персональных данных субъекта.

К обработке, передаче и хранению персональных данных сотрудника в приделах своих полномочий

ГБУЗ КК «ПК ГРД» могут иметь доступ сотрудники:

- бухгалтерии;
- планово-экономического отдела;
- сотрудники отдела кадров;
- сотрудники юридического отдела;
- главный врач (в отсутствии - исполняющий обязанности главного врача);
- главная акушерка;
- сотрудник ответственный за ведение воинского учета сотрудников ГБУЗ КК «ПК ГРД»;
- программист.

К обработке, передаче и хранению персональных данных пациента ГБУЗ КК «ПК ГРД» могут иметь доступ сотрудники в приделах своих полномочий:

- главный врач (в отсутствии - исполняющий обязанности главного врача);
- заместитель главного врача по клинико-экспертной работе;
- заместитель главного врача по лечебной работе;
- сотрудники планово-экономического отдела;
- сотрудники женской консультации (включая сотрудников регистратуры и сотрудников дневного стационара);
- сотрудники гинекологического отделения;
- сотрудники акушерского отделения;

- сотрудники отделения новорожденных;
- сотрудники отделения патологии беременности;
- сотрудники отделения анестезиологии и реанимации;
- сотрудники палаты интенсивной терапии;
- сотрудники отдела профилактики;
- сотрудники клинико-диагностического отделения;
- сотрудники отдела статистики;
- архивариус;
- программист.

6.4. При передаче персональных данных субъекта ГБУЗ КК «ПК ГРД» должно соблюдать следующие требования:

- не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные субъекта о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать режим безопасности. Данное положение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами;
- разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные субъекта, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья сотрудника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения сотрудником трудовой функции;
- передавать персональные данные субъекта представителям субъектов в порядке, установленном законом, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функций.

6.5. Передача персональных данных от субъекта или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

6.6. При передаче персональных данных субъекта потребителям (в том числе и в коммерческих целях) за пределы ГБУЗ КК «ПК ГРД», ГБУЗ КК «ПК ГРД» не должно сообщать эти данные третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта или в случаях, установленных федеральным законом.

6.7. Все меры конфиденциальности при сборе, обработке и хранении персональных данных субъекта распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

6.8. Не допускается отвечать на вопросы, связанные с передачей персональной информации, по телефону или факсу.

6.9. По возможности персональные данные обезличиваются.

7. Доступ к персональным данным

7.1. Внутренний доступ (доступ внутри ГБУЗ КК «ПК ГРД»).

Право доступа к персональным данным работника имеют:

- Главный врач (в отсутствии - исполняющий обязанности главного врача);
- Сотрудники отдела кадров;
- Сотрудники бухгалтерии;
- Сотрудники юридического отдела;
- Программист;
- любой сотрудник, в отношении своих персональных данных.

Право доступа к персональным данным пациента имеют:

- главный врач (в отсутствии - исполняющий обязанности главного врача);
- заместитель главного врача по клинико-экспертной работе;
- заместитель главного врача по лечебной работе;
- сотрудники женской консультации (включая сотрудников регистратуры и сотрудников дневного стационара);
- сотрудники гинекологического отделения;
- сотрудники акушерского отделения;
- сотрудники отделения новорожденных;
- сотрудники отделения патологии беременности;
- сотрудники отделения анестезиологии и реанимации;
- сотрудники палаты интенсивной терапии;
- сотрудники отдела медицинской профилактики;

- сотрудники клинико-диагностического отделения;
- сотрудники юридического отдела;
- сотрудники отдела статистики (включая операторов эвм);
- программист;
- архивариус;
- любой пациент в отношении своих персональных данных.

7.2. Внешний доступ.

7.2.1. К числу массовых потребителей персональных данных вне ГБУЗ КК «ПК ГРД» можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- центры социальной помощи;
- правоохранительные органы;
- службы судебных приставов;
- органы статистики;
- страховые (агентства, организации, компании; территориальный фонд обязательного медицинского страхования);
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления;

7.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

7.2.3. Компании, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные Компании, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

7.2.4. Другие организации.

Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии нотариально заверенного заявления работника.

7.2.5. Субъект, его родственники и члены семей.

Персональные данные субъекта могут быть предоставлены самому субъекту или с его письменного разрешения его родственникам или членам его семьи.

8. Защита персональных данных

Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности ГБУЗ КК «ПК ГРД».

8.1. «Внутренняя защита».

Регламентация доступа персонала к документам и базам данных с персональными сведениями входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами ГБУЗ КК «ПК ГРД». Для защиты персональных данных субъектов необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно – методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с документами и базами данных с персональными сведениями;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;

- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с документами, содержащими персональные данные;
- не допускается выдача личных дел сотрудников на рабочие места руководителей отделений.

Личные дела могут выдаваться на рабочие места только главному врачу (в отсутствии – исполняющему обязанности главного врача), начальнику отдела кадров, специалисту отдела кадров, начальнику юридического отдела и в исключительных случаях, по письменному разрешению главного врача (в отсутствии – исполняющему обязанности главного врача), руководителю отделения.

8.1.1. Защита персональных данных работника на переносных электронных носителях.

- Все переносные электронные носители, содержащие персональные данные, должны быть защищены, с использованием сертифицированных ФСТЭК и ФСБ средств криптозащиты, ключ для шифровки и дешифровки сообщается начальнику отдела кадров и программисту;
- Все переносные электронные носители, содержащие персональные данные, допускается хранить только в сейфе, в отделе кадров.

8.1.2. Работа с персональными данными пациента на переносных электронных носителях (хранение, копирование, обработка).

- Все переносные электронные носители, содержащие персональные данные, должны быть защищены, с использованием сертифицированных ФСТЭК средств криптозащиты в соответствие с классом информационных систем К1, ключ для шифровки и дешифровки сообщается начальнику отдела, в котором происходит работа с персональными данными пациентов на переносных электронных носителях;
- Все переносные электронные носители, содержащие персональные данные, допускается хранить только в сейфе.

.

8.2. «Внешняя защита».

Для защиты персональных данных создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение,

внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности ГБУЗ КК «ПК ГРД», посетители, работники других организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе кадров.

8.2.1. Для защиты персональных данных сотрудников и пациентов необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

8.2.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

8.2.3. Все лица, связанные с получением, обработкой и защитой персональных данных сотрудника обязаны заключить «Соглашение о неразглашении персональных данных сотрудников ГБУЗ КК «ПК ГРД»».

9.Ответственность за разглашение персональных данных, связанной с персональными данными.

9.1. Персональная ответственность – одно из главных требований к ГБУЗ КК «ПК ГРД» функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

9.2. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

9.3. Каждый сотрудник ГБУЗ КК «ПК ГРД», получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

9.4. Лица, виновные в нарушении установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) несут дисциплинарную, административную, гражданско–правовую или уголовную ответственность в соответствии с федеральным законом.