Для служебного пользования
Экз. №1

УТВЕРЖДАЮ
Глав.врач БУЗ ВО «Вологодская городская поликлиника№5»
_____М.Ю. Бритвин
«04» февраля 2015г.

ПОЛОЖЕНИЕ
об обработке и защите персональных данных работников в БУЗ ВО «Вологодская городская поликлиника №5»

г. Вологда
2015 г.

1. Общие положения

1.1. Целью данного Положения является защита персональных данных работников от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Настоящее Положение разработано на основании статей Конституции РФ, Трудового Кодекса РФ, Кодекса об административных правонарушениях РФ, Гражданского Кодекса РФ, Уголовного Кодекса РФ, а также Федерального закона «Об информации, информатизации и защите информации»

1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

1.4. Настоящее Положение утверждается и вводится в действие приказом главного врача и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным.

2. Понятие и состав персональных данных

2.1.1. Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающиеся конкретного работника. Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

2.1.2. В состав персональных данных работника входят:

- анкетные и биографические данные;
- наименование структурного подразделения;
- занимаемая должность;
- сведения о текущем должностном окладе;
- паспортные данные;
- адрес прописки;
- ИНН;
- номер страхового свидетельства;
- данные об образовании;
- данные о детях;
- данные о семейном положении;
- содержание трудового договора;
- содержание декларации, подаваемой в налоговую инспекцию;
- 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;
- копии отчетов, направляемые в органы статистики.

2.2.1. Персональные данные клиента/пациента – информация, необходимая организации в связи с медицинским обслуживанием и касающиеся конкретного клиента/пациента. Под информацией о клиентах/пациентах понимаются сведения о фактах, событиях и обстоятельствах жизни клиента/пациента, позволяющие идентифицировать его личность.

2.1.2. В состав персональных данных клиента/пациента входят:

- анкетные и биографические данные;

- место работы;
- занимаемая должность;
- паспортные данные;
- адрес прописки;
- ИНН;
- номер страхового свидетельства;
- данные о детях;
- данные о семейном положении;
- копии отчетов, направляемые в органы статистики.

2.3. Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

3. Обработка персональных данных

3.1. Под обработкой персональных данных работника/клиента/пациента понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных работника/клиента/пациента.

3.2. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования;

В целях обеспечения прав и свобод человека и гражданина организация и ее представители при обработке персональных данных клиента/пациента обязаны соблюдать следующие общие требования:

3.2.1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

Обработка персональных данных клиента/пациента может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, оказания клиенту/пациенту медицинской помощи, обеспечения личной безопасности клиента/пациента, контроля количества и качества оказываемых медицинских услуг.

3.2.2. При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами;

При определении объема и содержания обрабатываемых персональных данных пациента организация должна руководствоваться Конституцией Российской Федерации и иными федеральными законами.

3.2.3. Получение персональных данных работника может осуществляться как путем представления их самим работником, так и путем получения их из иных источников.

Получение персональных данных клиента/пациента может осуществляться как путем представления их самим клиентом/пациентом, так и путем получения их из иных источников.

3.2.4. Персональные данные следует получать у самого работника. Если персональные данные работника возможно получить только у третьей стороны, то работник должен

быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

Персональные данные следует получать у самого клиента/пациента. Если персональные данные клиента/пациента возможно получить только у третьей стороны, то клиент/пациент должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Организация должна сообщить клиенту/пациенту о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа клиента/пациента дать письменное согласие на их получение.

3.2.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений данные о частной жизни работника (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны работодателем только с его письменного согласия;

Организация не имеет права получать и обрабатывать персональные данные клиента/пациента о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений данные о частной жизни клиента/пациента (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны организацией только с его письменного согласия.

3.2.6. Работодатель не имеет право получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом;

Организация не имеет право получать и обрабатывать персональные данные клиента/пациента о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.3. К обработке, передаче и хранению персональных данных работника могут иметь доступ сотрудники:

- бухгалтерии;
- сотрудники службы управления персоналом;
- сотрудники компьютерных отделов.

К обработке, передаче и хранению персональных данных клиента/пациента могут иметь доступ сотрудники:

- регистратуры;
- медработники;
- сотрудники компьютерных отделов.

3.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

3.4.1. 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.

3.5. Передача персональных данных работника/клиента/пациента возможна только с согласия работника/клиента/пациента или в случаях, прямо предусмотренных законодательством.

3.5.1. При передаче персональных данных работника/клиента/пациента организация должна соблюдать следующие требования:

- не сообщать персональные данные работника/клиента/пациента третьей стороне без письменного согласия работника/клиента/пациента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника/клиента/пациента, а также в случаях, установленных федеральным законом;

- не сообщать персональные данные работника/клиента/пациента в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные работника/клиента/пациента, 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 работника/клиента/пациента, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работника/клиента/пациента в порядке, установленном федеральными законами;

- разрешать доступ к персональным данным работников/клиентов/пациентов только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные работника/клиента/пациента, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций; а представителям клиентов/пациентов – только с письменного согласия субъекта ПДн, если другое не предусмотрено законодательством РФ, и ограничивать эту информацию только теми персональными данными клиента/пациента, которые необходимы для выполнения указанными представителями их функций.

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

3.5.3. При передаче персональных данных работника/клиента/пациента потребителям (в том числе и в коммерческих целях) за пределы организации, представитель не должен сообщать эти данные третьей стороне без письменного согласия работника/клиента/пациента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника/клиента/пациента или в случаях, установленных федеральным законом.

3.6. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника/клиента/пациента распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

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

3.8. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

3.9. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения. Работодатель учитывает личные качества работника, его добросовестный и эффективный труд.

4. Доступ к персональным данным

4.1.1. Внутренний доступ (доступ внутри организации).

4.1.1.1. Право доступа к персональным данным сотрудника имеют:

-1 главный врач;

-2 руководители структурных подразделений по направлению деятельности (доступ к личным данным только сотрудников своего подразделения);

- при переводе из одного структурного подразделения в другое, доступ к персональным данным сотрудника может иметь руководитель нового подразделения;

- сам работник, носитель данных.

- другие сотрудники организации при выполнении ими своих служебных обязанностей.

4.1.1.2. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом главного врача.

4.1.2. Внешний доступ.

4.1.2.1. К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:

-3 налоговые инспекции;

-4 правоохранительные органы;

-5 органы статистики;

-6 страховые агентства;

-7 военкоматы;

-8 органы социального страхования;

-9 пенсионные фонды;

-10 подразделения муниципальных органов управления;

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

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

4.1.2.4. 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.

Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия. (УК РФ).

4.2.1. Внутренний доступ (доступ внутри организации).

4.2.1.1. Право доступа к персональным данным клиента/пациента имеют:

- сотрудники регистратуры;
- лечащие врачи;
- другие сотрудники организации при выполнении ими своих служебных обязанностей;
- сам клиент/пациент, носитель данных.

4.2.1.2. Перечень лиц, имеющих доступ к персональным данным клиентов/пациентов, определяется приказом главного врача организации.

4.2.2. Внешний доступ.

4.2.2.1. К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования.

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

4.2.2.3. Организации, в которые клиент/пациент может осуществлять перечисления денежных средств (страховые компании, кредитные учреждения), могут получить доступ к персональным данным клиента/пациента только в случае его письменного разрешения.

4.2.2.4. Другие организации.

Сведения о клиенте/пациенте могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления клиента/пациента.

Персональные данные клиента/пациента могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого клиента/пациента.

5. Защита персональных данных

5.1. 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.

5.2. 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.

5.3. 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 деятельности организации.

5.4. Защита персональных данных работника/клиента/пациента от неправомерного их использования или утраты должна быть обеспечена организацией за счет ее средств в порядке, установленном федеральным законом.

5.5. «Внутренняя защита».

5.5.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации.

5.5.2. Для обеспечения внутренней защиты персональных данных работников/клиентов/пациентов необходимо соблюдать ряд мер:

-1 ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;

-2 строгое избирательное и обоснованное распределение документов и информации между работниками;

-3 рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;

-4 знание работником требований нормативно - методических документов по защите информации и сохранении тайны;

-5 наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

-6 определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

-7 организация порядка уничтожения информации;

-8 своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;

- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

- не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только главному врачу, работникам отдела персонала и в исключительных случаях, по письменному разрешению главного врача, - руководителю структурного подразделения (например, при подготовке материалов для аттестации работника).

5.5.3. Защита персональных данных сотрудника/клиента/пациента на электронных носителях.

Все папки, содержащие персональные данные сотрудника, должны быть защищены паролем, который сообщается руководителю службы управления персоналом и руководителю службы информационных технологий.

Все папки, содержащие персональные данные клиента/пациента, должны быть защищены паролем, который сообщается врачам и руководителю службы информационных технологий

5.6. «Внешняя защита».

5.6.1. Для защиты конфиденциальной информации 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.

5.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности компании, 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.

5.6.3. Для обеспечения внешней защиты персональных данных сотрудников/клиентов/пациентов необходимо соблюдать ряд мер:

-1 порядок приема, учета и контроля деятельности посетителей;

-2 пропускной режим организации;

-3 учет и порядок выдачи удостоверений;

-4 технические средства охраны, сигнализации;

-5 порядок охраны территории, зданий, помещений, транспортных средств;

-6 требования к защите информации при интервьюировании и собеседованиях.

5.7. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников/клиентов/пациентов.

5.8. По возможности персональные данные обезличиваются.

5.9. Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники, клиенты/пациенты и их представители могут вырабатывать совместные меры защиты персональных данных работников.

6. Права и обязанности субъекта персональных данных

5.9. Закрепление прав субъекта ПДн, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

5.10. Субъекты ПДн и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

5.11. В целях защиты персональных данных, хранящихся в организации, субъект ПДн имеет право:

- требовать исключения или исправления неверных или неполных персональных данных.

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

- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;

- определять своих представителей для защиты своих персональных данных;

- на сохранение и защиту своей личной и семейной тайны.

6.4. Обязательства субъекта ПДн:

6.4.1. Работник обязан:

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ.

- своевременно сообщать работодателю об изменении своих персональных данных

6.4.2. Клиент/пациент обязан:

- передавать организации или ее представителю комплекс достоверных персональных данных, необходимых для оказания медицинских услуг.

- своевременно сообщать организации об изменении своих персональных данных

6.5. Работники ставят работодателя в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.

Клиенты/пациенты ставят организацию в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в медицинской карте на основании представленных документов.

6.6. В целях защиты частной жизни, личной и семейной тайны субъекты ПДн не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

7.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

7.2. 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.

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

7.4. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

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

7.5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

7.5.2. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

7.5.3. В соответствии с Гражданским Кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

7.5.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

7.6. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

С положением ознакомлены:

Глав.врач БУЗ ВО «Вологодская городская поликлиника №5»	М.Ю. Бритвин
Заместитель глав.врача по мед.части	Ю.А. Фазылова
Медстатистик	Е.Н. Сахарнова
Главный бухгалтер	З.А. Бибиксаров
Юрисконсульт	М.В. Перепелиц
Специалист отдела кадров	Н.С. Шлаева