

УТВЕРЖДАЮ

Главный врач

БУЗ ВО «Вологодская городская
поликлиника №3»



 Н.В. Соколов

М.П.

«»



2014 г.

ПОЛОЖЕНИЕ

о защите персональных данных пациентов БУЗ ВО «Вологодская городская поликлиника
№3»

1. Общие положения

1.1. Настоящее Положение о защите персональных данных пациентов (далее – Положение) БУЗ ВО «Вологодская городская поликлиника №3» (далее – Учреждение) разработано с целью обеспечения требований защиты прав граждан при обработке их персональных данных.

1.2. Положение разработано в соответствии с Конституцией РФ, Основами законодательства РФ об охране здоровья граждан, Федеральным законом РФ "Об информации, информационных технологиях и о защите информации" № 149-ФЗ от 27.07.2006 г., Федеральным законом РФ "О персональных данных" № 152-ФЗ от 27.07.2006 г., Указом Президента РФ «Об утверждении перечня сведений конфиденциального характера» № 188 от 06.03.1997 г., Постановлением Правительства РФ «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» № 781 от 17.11.2007 г. и другими нормативными правовыми актами.

1.3. Положение определяет порядок обработки персональных данных в Учреждении и гарантии конфиденциальности сведений, предоставляемых гражданами (пациентами) в Учреждение.

1.4. Персональные данные являются конфиденциальной информацией.

1.5. Положение вступает в силу с момента его утверждения главным врачом Учреждения и действует бессрочно. Изменения и дополнения в Положение вносятся приказом по Учреждению.

1.6. Положение является обязательным для исполнения всеми работниками Учреждения, имеющими доступ к персональным данным пациентов. Вышеуказанные работники должны быть ознакомлены с Положением под роспись.

2. Основные понятия и состав персональных данных

2.1. Для целей настоящего Положения используются следующие основные понятия:

- **Персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных);

- **Обработка персональных данных** - сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных;

- **Конфиденциальность персональных данных** - обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным, требование не допускать их распространения без согласия гражданина или иного законного основания;

- **Распространение персональных данных** - действия, направленные на передачу персональных данных определенному кругу лиц (передача

персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

- **Использование персональных данных** - действия (операции) с персональными данными, совершаемые должностным лицом в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении граждан либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

- **Блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

- **Уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

- **Обезличивание персональных данных** - действия, в результате которых невозможно определить принадлежность персональных данных конкретному гражданину;

- **Общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия гражданина или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2.2. В состав персональных данных пациентов входят:

- фамилия, имя, отчество;
- дата рождения;
- полис ОМС (серия, номер, дата начала действия, дата окончания действия, наименование учреждения выдавшего полис);
- статус представителя пациента (фамилия, имя, отчество);
- гражданство;
- реквизиты документа удостоверяющего личность;
- место проживания и место регистрации;
- социальный статус пациента;
- место работы, учебы;
- даты начала и окончания лечения;
- коды: вида медицинской помощи, профиля отделения, койки/специалиста, диагноза заболевания;
- количество койко-дней;
- исход заболевания;
- СНИЛС пациента;
- снимок внутренних органов;
- пол;
- исход заболевания;
- данные больничного листа и льготного рецепта,

- иная информация, которую граждане добровольно сообщают о себе в целях оказания им медицинской помощи, если ее обработка не запрещена законом.

2.3. Материалы медицинской карты, истории болезни пациентов относятся к конфиденциальной информации ограниченного доступа.

3. Обработка персональных данных

3.1. Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

3.2. Обработка персональных данных осуществляется на основе соблюдения принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Учреждения;
- 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 информационных систем персональных данных;
- уничтожения персональных данных после достижения целей обработки или в случае утраты необходимости в их достижении;
- личной ответственности сотрудников Учреждения за сохранность и конфиденциальность персональных данных, а также носителей этой информации;
- наличия четкой разрешительной системы доступа сотрудников Учреждения к документам и базам данных, содержащим персональные данные.

Получения персональных данных

3.3. Все персональные данные пациента следует получать у него самого или в случае его недееспособности у его законного представителя после

оформления ими письменного согласия (Приложение 1). Письменное согласие включает в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных (его законного представителя), номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес Учреждения, получающего согласие пациента;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие пациента;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Учреждением способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

3.4. Согласие на обработку персональных данных не требуется если:

- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является пациент;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов пациента, если получение его согласия невозможно.

3.5. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе следующую информацию:

- подтверждение факта обработки персональных данных Учреждением, а также цель такой обработки;
- способы обработки персональных данных, применяемые Учреждением;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

3.6. Если персональные данные субъекта возможно получить только у третьей стороны, то Учреждение должно получить письменное согласие пациента на эту операцию и уведомить его о факте получения данных, предоставив следующую информацию:

- наименование и адрес третьей стороны;

- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» права субъекта персональных данных.

3.7. Учреждение не имеет права получать и обрабатывать персональные данные пациента о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, частной жизни, за исключением случаев, предусмотренных законом. В частности, Учреждение вправе обрабатывать указанные персональные данные пациента только с его письменного согласия.

Хранение персональных данных

3.8. Персональные данные пациента хранятся в его медицинской карте, истории болезни. Медицинская карта, история болезни пациента ведется лечащим врачом.

К медицинской карте, истории болезни пациента приобщаются:

- письменное согласие на обработку персональных данных;
- договор на оказание услуг;
- иные документы по согласованию с пациентом.

Документы, приобщенные к медицинской карте, истории болезни пациента, брошюруются, страницы нумеруются, к медицинской карте, истории болезни прилагается опись.

3.9. Персональные данные пациентов также хранятся в электронном виде в информационных системах персональных данных.

Доступ к электронным базам данных, содержащим персональные данные пациентов, обеспечивается двухступенчатой системой паролей: на уровне локальной компьютерной сети и на уровне баз данных.

Пароли устанавливаются администратором ИСПДн Учреждения и сообщаются индивидуально медицинским работникам, имеющим доступ к персональным данным пациентов. Изменение паролей администратором ИСПДн осуществляется не реже 1 раза в 3 месяца.

3.10. Медицинские карты, истории болезни пациентов, журналы и книги учета хранятся в рабочее и нерабочее время в металлических запирающихся шкафах. Сотрудникам Учреждения не разрешается при выходе из помещения оставлять какие-либо документы, содержащие персональные данные, на рабочем столе или оставлять шкафы незапертыми.

На рабочем столе медицинского работника должен всегда находиться только тот массив документов, с которым в настоящий момент он работает, касающийся только того пациента, прием которого проводится. Другие документы, медицинские карты, истории болезни, карточки, журналы должны находиться в запертом шкафу.

В конце рабочего дня медицинские карты, истории болезней и другие документы, содержащие персональные данные, должны быть заперты в металлические шкафы, сейфы или сданы на хранение ответственным лицам.

Доступ к персональным данным работников Учреждения

3.11. Право доступа к персональным данным пациента при их хранении, обработке и передаче имеют:

- главный врач Учреждения;
- лечащий врач пациента, в ведение которого передан соответствующий массив документов, содержащих персональные данные;
- другие сотрудники Учреждения, согласно утвержденному главным врачом Положению о разграничении прав доступа пользователей информационных систем к обрабатываемым персональным данным.

Доступ к персональным данным третьих лиц

3.12. Персональные данные пациента могут быть предоставлены третьим лицам только с его письменного согласия, которое должно содержать:

- Фамилию, имя, отчество, адрес пациента, реквизиты основного документа, удостоверяющего его личность;
- Наименование и адрес Учреждения, получившего согласие на передачу;
- Наименование и адрес принимающей стороны (юридического, физического лица);
- Цель передачи персональных данных;
- Перечень персональных данных, на передачу которых дает согласие пациент;
- Срок в течении которого действует согласие, а также порядок его отзыва.

3.13. Согласие пациента на передачу персональных данных третьим лицам не требуется в следующих случаях:

- передача персональных данных осуществляется в целях исполнения договора, одной из сторон которого является пациент;
- передача персональных данных осуществляется для статистических или иных научных целей при условии их обязательного обезличивания;
- передача персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов пациента, если получение его согласия невозможно.

3.14. При передаче персональных данных пациента третьим лицам Учреждение должно выполнить следующие условия:

- уведомить лиц, получающих персональные данные 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;

- предупредить принимающую сторону об ответственности за незаконное использование полученной конфиденциальной информации в соответствии с федеральными законами.

3.15. Передача документов (иных материальных носителей), содержащих персональные данные пациентов, осуществляется при наличии:

- соглашения о неразглашении конфиденциальной информации либо в договоре с третьим лицом пунктов о неразглашении конфиденциальной информации, в том числе, предусматривающих защиту персональных данных граждан;
- письма-запроса от третьего лица, которое должно включать в себя указание на основания получения доступа к запрашиваемой информации, содержащей персональные данные, её перечень, цель использования, Ф.И.О. и должность лица, которому поручается получить данную информацию.

Доступ пациента к своим персональным данным

3.16. Доступ пациента к своим персональным данным предоставляется при обращении либо при получении запроса пациента.

3.17. Запрос должен содержать фамилию, имя, отчество, адрес, номер основного документа, удостоверяющего личность пациента или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя.

3.18. Пациент имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Учреждением, а также цель такой обработки;
- способы обработки персональных данных, применяемые Учреждением;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для пациента может повлечь за собой обработка его персональных данных.

3.19. Учреждение обязано сообщить пациенту информацию о наличии его персональных данных, а также предоставить возможность ознакомления

с ними в течение десяти рабочих дней с момента обращения или получения запроса.

Сведения о наличии персональных данных должны быть предоставлены пациенту в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

3.20. Право пациента на доступ к своим персональным данным ограничивается в случае, если предоставление персональных данных нарушает конституционные права и свободы других лиц.

Уточнение, блокирование и уничтожение персональных данных

3.21. Блокирование информации, содержащей персональные данные пациента, производится в случае:

- если персональные данные являются неполными, устаревшими, недостоверными;
- если сведения являются незаконно полученными или не являются необходимыми для заявленной цели обработки.

3.22. В случае подтверждения факта недостоверности персональных данных Учреждение на основании документов, представленных пациентом, уполномоченным органом по защите прав субъектов персональных данных или полученных в ходе самостоятельной проверки, обязан уточнить персональные данные и снять их блокирование.

3.23. В случае выявления неправомерных действий с персональными данными Учреждение обязано устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий трех рабочих дней с момента выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные.

Об устранении допущенных нарушений или об уничтожении персональных данных Учреждение обязано уведомить пациента, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

3.24. Учреждение обязано уничтожить персональные данные пациента в случае:

- достижения цели обработки персональных данных;
- отзыва пациентом согласия на обработку своих персональных данных.

3.25. Уничтожение персональных данных должно быть осуществлено по истечении периода времени, необходимого для проведения взаиморасчетов по оказанной ранее пациенту медицинской помощи.

Учреждение должно направить уведомление об уничтожении персональных данных пациенту, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также в указанный орган.

4. Организация защиты персональных данных

4.1. 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.

4.2. 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.

4.3. 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 управленческой и производственной деятельности Учреждения.

4.4. Защита персональных данных от неправомерного их использования или утраты обеспечивается Учреждением за счет собственных средств в порядке, установленном федеральными законами.

4.5. Общую организацию защиты персональных данных осуществляет ведущий инженер по защите информации.

4.6. Ведущий инженер по защите информации обеспечивает:

- ознакомление сотрудников, допущенных к работе с информацией, содержащей персональные данные пациентов, под роспись с настоящим Положением.

При наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных, с данными актами также производится ознакомление сотрудников под роспись.

- истребование с сотрудников письменного обязательства о соблюдении режима конфиденциальности персональных данных и соблюдении правил их обработки (Приложение 2).
- общий контроль за соблюдением сотрудниками Учреждения мер по защите персональных данных.

4.7. Организацию и контроль за защитой персональных данных в структурных подразделениях Учреждения, сотрудники которых имеют доступ к персональным данным, осуществляют их непосредственные руководители.

4.8. Защите подлежит:

- информация о персональных данных;
- документы, содержащие персональные данные;
- персональные данные, содержащиеся на электронных носителях.

Внутренняя защита

4.9. 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 Учреждения.

4.10. Для обеспечения внутренней защиты персональных данных 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 конфиденциальными документами и базами данных;
- 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 конфиденциальными документами.

4.11. Защита сведений, хранящихся в электронных базах данных Учреждения, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, обеспечивается системой защиты персональных данных.

Внешняя защита

4.12. 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.

4.13. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Учреждения, 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 Учреждении.

4.14. Для обеспечения внешней защиты персональных данных необходимо соблюдать ряд мер:

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

4.15. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных.

4.16. По возможности персональные данные обезличиваются.

4.17. Кроме мер защиты персональных данных, установленных законодательством, Учреждение, сотрудники и их представители могут вырабатывать совместные меры защиты персональных данных.

5. Ответственность за разглашение персональных данных и нарушение норм, регулирующих получение, обработку и защиту персональных данных

5.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных пациента, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.

5.2. Разглашение персональных данных пациента (передача их посторонним лицам, в том числе, работникам Учреждения, не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные работника, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативными актами (приказами, распоряжениями) Учреждения, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарного взыскания – замечания, выговора, увольнения.

5.3. Сотрудники, имеющие доступ к персональным данным пациента и совершившие указанный дисциплинарный проступок, несут полную материальную ответственность в случае причинения его действиями ущерба Учреждению.

5.4. Сотрудники, имеющие доступ к персональным данным пациента, виновные в незаконном разглашении или использовании персональных данных пациента без согласия пациента из корыстной или иной личной заинтересованности и причинившие крупный ущерб, несут уголовную ответственность в соответствии со ст. 183 Уголовного кодекса РФ.

СОГЛАСИЕ
на обработку персональных данных

Я, (или законный представитель субъекта персональных данных)

Ф.И.О. недееспособного лица _____
проживающий(его) по адресу: (по месту регистрации) _____

_____, паспорт
№ _____, выдан (дата, название выдавшего органа)

_____, в соответствии
и с требованиями статьи 9 федерального закона от 27.07.06 г. "О персональных
данных" № 152-ФЗ, подтверждаю свое согласие на обработку БУЗ ВО «Вологодская
городская поликлиника №3» (далее – Оператор), зарегистрированной по адресу: г.
Вологда, ул. Московская, 2а, моих персональных данных (данных недееспособного
лица), включающих: фамилию, имя, отчество, пол, дату рождения, адрес
проживания, контактный телефон, реквизиты полиса ОМС (ДМС), страховой номер
индивидуального лицевого счета в Пенсионном фонде России (СНИЛС), данные о
состоянии моего здоровья (здоровья недееспособного лица), заболеваниях, случаях
обращения за медицинской помощью, – в медико-профилактических целях, в целях
установления медицинского диагноза и оказания медицинских услуг при условии,
что их обработка осуществляется лицом, профессионально занимающимся
медицинской деятельностью и обязанным сохранять врачебную тайну.

В процессе оказания Оператором мне (недееспособному лицу) медицинской
помощи я предоставляю право медицинским работникам, передавать мои
персональные данные (данные недееспособного лица), содержащие сведения,
составляющие врачебную тайну, другим должностным лицам Оператора, в
интересах моего (недееспособного лица) обследования и лечения.

Предоставляю Оператору право осуществлять все действия (операции) с
моими персональными данными (данными недееспособного лица), включая сбор,
систематизацию, накопление, хранение, обновление, изменение, использование,
обезличивание, блокирование, уничтожение. Оператор вправе обрабатывать мои
персональные данные (данные недееспособного лица), посредством внесения их в
электронную базу данных, включения в списки (реестры) и отчетные формы,
предусмотренные документами, регламентирующими предоставление отчетных
данных (документов) по ОМС (договором ДМС).

Оператор имеет право во исполнение своих обязательств по работе в
системе ОМС (по договору ДМС _____) на обмен (прием и передачу)
моими персональными данными (данными недееспособного лица) с АО «Страховая
компания «СОГАЗ-Мед», страховыми медицинскими организациями и
территориальным фондом ОМС с использованием машинных носителей или по
каналам связи, с соблюдением мер, обеспечивающих их защиту от
несанкционированного доступа, при условии, что их прием и обработка будет
осуществляется лицом, обязанным сохранять профессиональную тайну.

Срок хранения моих персональных данных (данных недееспособного лица),
соответствует сроку хранения первичных медицинских документов и составляет
двадцать пять лет (для стационара, пять лет – для поликлиники).

Передача моих персональных данных (данных недееспособного лица), иным лицам или иное их разглашение может осуществляться только с моего письменного согласия.

Настоящее согласие дано мной «____» _____ 20__ года и действует бессрочно.

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

В случае получения моего письменного заявления об отзыве настоящего согласия на обработку персональных данных, Оператор обязан прекратить их обработку в течение периода времени, необходимого для завершения взаиморасчетов по оплате оказанной мне (недееспособному лицу), до этого медицинской помощи.

Контактный телефон _____ и адрес по месту жительства _____

Подпись субъекта персональных данных (или его законного представителя)

Обязательство о соблюдении режима конфиденциальности персональных данных

Я, _____,
работая по должности (профессии) _____,

в БУЗ ВО «Вологодская городская поликлиника №3» обязуюсь:

1. Не разглашать, не раскрывать публично, а также соблюдать установленный Положением о защите персональных данных БУЗ ВО «Вологодская городская поликлиника №3» порядок передачи третьим лицам сведений, составляющих персональные данные, которые мне будут доверены или станут известны по работе.

Выполнять относящиеся ко мне требования Положения о защите персональных данных, приказов, распоряжений, инструкций и других локальных нормативных актов по обеспечению конфиденциальности персональных данных и соблюдению правил их обработки.

2. В случае попытки посторонних лиц получить от меня сведения, составляющие персональные данные, немедленно сообщить руководителю структурного подразделения и ведущему инженеру по защите персональных данных.

3. В случае моего увольнения, все носители, содержащие персональные данные (документы, копии документов, дискеты, диски, магнитные ленты, распечатки на принтерах, черновики, кино- и фотонегативы, позитивы и пр.), которые находились в моем распоряжении в связи с выполнением мною трудовых обязанностей во время работы у работодателя, передать руководителю структурного подразделения или другому сотруднику по указанию руководителя структурного подразделения.

4. Об утрате или недостатке документов или иных носителей, содержащих персональные данные (удостоверений, пропусков и т.п.); ключей от хранилищ, сейфов (металлических шкафов) и о других фактах, которые могут привести к разглашению персональных данных, а также о причинах и условиях возможной утечки сведений немедленно сообщить руководителю структурного подразделения и ведущему инженеру по защите персональных данных.

Я ознакомлен под роспись:

с Положением о защите персональных данных БУЗ ВО «Вологодская городская поликлиника №3» и инструкцией пользователя ИСПДн.

Мне известно, что нарушение мною обязанностей по защите персональных данных может повлечь дисциплинарную, гражданско-правовую, уголовную и иную ответственность в соответствии с законодательством РФ.

«___» _____ 20__ г.

(подпись)

(Ф.И.О. работника)