

УТВЕРЖДЕНО

Приказом главного врача
ГУ «Республиканская
туберкулезная больница
«Новоелья»
от 12 апреля 2022 № 23

ПОЛИТИКА в отношении обработки персональных данных

1. Политика в отношении обработки персональных данных (далее – Политика) в Государственном учреждении «Республиканская туберкулезная больница «Новоелья»» (далее – больница) определяет основные требования, цели, условия и способы обработки персональных данных, перечни субъектов и обрабатываемых персональных данных, права субъектов персональных данных, а также реализуемые в больнице требования к защите, передаче, хранению и конфиденциальности персональных данных.

2. Положения Политики служат основой для разработки локальных правовых актов, регламентирующих в больнице вопросы обработки персональных данных работников и других субъектов персональных данных.

3. Политика обработки персональных данных определяется в соответствии со следующими нормативными правовыми актами:

Конституция Республики Беларусь;

Трудовой кодекс Республики Беларусь;

Кодекс Республики Беларусь об административных правонарушениях;

Процессуально-исполнительный кодекс Республики Беларусь об административных правонарушениях;

закон Республики Беларусь от 07.05.2021 № 99-3 «О защите персональных данных»;

закон Республики Беларусь от 21.07.2008 № 418-3 «О регистре населения»;

закон Республики Беларусь от 10.11.2008 № 455-3 «Об информации, информатизации и защите информации»;

закон Республики Беларусь от 18.06.1993 № 2435-XII «О здравоохранении»;

закон Республики Беларусь от 28.05.2021 № 114-3 «Об изменении законов по вопросам трудовых отношений»;

решение Конституционного Суда Республики Беларусь от 29.04.2021 № P1261/2021 «О соответствии Конституции Республики Беларусь Закона Республики Беларусь «О защите персональных данных»;

постановление Совета Министров Республики Беларусь от 10.04.2019 № 228 «Об особенностях внесения отдельных персональных данных и их актуализации в регистре населения»;

постановление Министерства внутренних дел Республики Беларусь от 27.09.2012 № 341 «Об установлении порядка обезличивания персональных данных, содержащихся в регистре населения»;

постановление Министерства здравоохранения Республики Беларусь от 07.06.2021 № 74 «О формах и порядке дачи и отзыва согласия на внесение и обработку персональных данных пациента» (вместе с Инструкцией о формах и порядке дачи и отзыва согласия на внесение и обработку персональных данных, информации, составляющей врачебную тайну, отказа от их внесения и обработки и порядке информирования о праве на отказ от внесения информации, составляющей врачебную тайну, в централизованную информационную систему здравоохранения);

постановление Министерства здравоохранения Республики Беларусь от 28.05.2021 № 64 «Об утверждении Инструкции о порядке обезличивания персональных данных лиц, которым оказывается медицинская помощь»;

постановление Правления Национального банка Республики Беларусь от 31.12.2019 № 552 «Об утверждении стандартов проведения, расчетов; Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28.01.1981;

Хартии Европейского союза об основных правах от 12.12.2007;

иные акты законодательства и международные договоры Республики Беларусь.

В случае, если законодательным актом, устанавливающим правовой режим охраняемой законом тайны, предусматриваются особенности обработки персональных данных, входящих в состав охраняемой законом тайны, применяются положения этого законодательного акта.

Если международным договором Республики Беларусь установлены иные правила, чем те, которые содержатся в законодательстве, то применяются правила международного договора.

4. Больница, являясь оператором персональных данных, осуществляет обработку персональных данных работников больницы, их родственников, кандидатов на рабочие места, контрагентов – физических лиц, пациентов, доноров, и других субъектов персональных данных, обратившихся в больницу.

5. Под персональными данными понимается любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая в связи с трудовыми и иными отношениями с больницей.

6. Обработка персональных данных осуществляется с учетом необходимости обеспечения защиты прав и свобод работников больницы и других субъектов персональных данных, в том числе защиты права на неприкосновенность частной жизни, личную и семейную тайну, в соответствии со следующими требованиями:

обработка персональных данных осуществляется в соответствии с законодательством; обработка персональных данных должна быть соразмерна заявленным целям их обработки и обеспечивать на всех этапах такой обработки справедливое соотношение интересов всех заинтересованных лиц;

обработка персональных данных осуществляется с согласия субъекта персональных данных, за исключением случаев, предусмотренных законодательными актами;

обработка персональных данных ограничивается достижением конкретных, заранее заявленных законных целей. Не допускается обработка персональных данных, не совместимая с первоначально заявленными целями их обработки;

содержание и объем обрабатываемых персональных данных соответствуют заявленным целям их обработки. Обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям их обработки;

обработка персональных данных носит прозрачный характер. Субъекту персональных данных может предоставляться соответствующая информация, касающаяся обработки его персональных данных;

принимаются меры по обеспечению достоверности обрабатываемых персональных данных, при необходимости обновляются;

персональные данные хранятся в форме, позволяющей идентифицировать субъекта персональных данных, не дольше, чем этого требуют заявленные цели обработки персональных данных.

7. Содержание и объем персональных данных каждой категории субъектов определяется необходимостью достижения конкретных целей их обработки, а также необходимостью

больницы реализовать свои права и обязанности, а также права и обязанности соответствующего субъекта.

Перечень обрабатываемых персональных данных определяется в соответствии с законодательством и локальными правовыми актами с учетом целей обработки персональных данных, составляется начальником отдела автоматизированных систем управления и утверждается главным врачом.

Персональные данные обрабатываются исключительно для достижения одной или нескольких указанных законных целей. Если персональные данные были собраны и обрабатываются для достижения определенной цели, для использования этих данных в других целях необходимо поставить в известность об этом субъекта персональных данных и, в случае необходимости, получить новое согласие на обработку.

Персональные данные могут обрабатываться в иных целях, если это необходимо в связи с обеспечением соблюдения законодательства.

8. Согласие субъекта персональных данных на обработку персональных данных не требуется:

для целей ведения административного и (или) уголовного процесса, осуществления оперативно-розыскной деятельности; для осуществления правосудия, исполнения судебных постановлений и иных исполнительных документов;

в целях осуществления контроля (надзора) в соответствии с законодательными актами; при реализации норм законодательства в области национальной безопасности, о борьбе с коррупцией, о предотвращении легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения;

при реализации норм законодательства о выборах, референдуме, об отзыве депутата Палаты представителей, члена Совета Республики Национального собрания Республики Беларусь, депутата местного Совета депутатов;

для ведения индивидуального (персонифицированного) учета сведений о застрахованных лицах для целей государственного социального страхования, в том числе профессионального пенсионного страхования; при оформлении трудовых отношений, а также в процессе трудовой деятельности субъекта персональных данных в случаях, предусмотренных законодательством;

для осуществления нотариальной деятельности; при рассмотрении вопросов, связанных с гражданством Республики Беларусь, предоставлением статуса беженца, дополнительной защиты, убежища и временной защиты в Республике Беларусь;

в целях назначения и выплаты пенсий, пособий;

для организации и проведения государственных статистических наблюдений, формирования официальной статистической информации;

в научных или иных исследовательских целях при условии обязательного обезличивания персональных данных;

при осуществлении учета, расчета и начисления платы за жилищно-коммунальные услуги, платы за пользование жилым помещением и возмещения расходов на электроэнергию, платы за другие услуги и возмещения налогов, а также при предоставлении льгот и взыскании задолженности по плате за жилищно-коммунальные услуги, плате за пользование жилым помещением и возмещению расходов на электроэнергию;

при получении персональных данных оператором на основании договора, заключенного (заключаемого) с субъектом персональных данных, в целях совершения действий, установленных этим договором;

при обработке персональных данных, когда они указаны в документе, адресованном оператору и подписанном субъектом персональных данных, в соответствии с содержанием такого документа;

в целях осуществления законной профессиональной деятельности журналиста и (или) деятельности средства массовой информации, организации, осуществляющей издательскую деятельность, направленных на защиту общественного интереса, представляющего собой потребность общества в обнаружении и раскрытии информации об угрозах национальной безопасности, общественному порядку, здоровью населения и окружающей среде, информации, влияющей на выполнение своих обязанностей государственными должностными лицами, занимающими ответственное положение, общественными деятелями, за исключением случаев, предусмотренных гражданским процессуальным, хозяйственным процессуальным, уголовно-процессуальным законодательством, законодательством, определяющим порядок административного процесса;

для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно;

в отношении распространенных ранее персональных данных до момента заявления субъектом персональных данных требований о прекращении обработки распространенных персональных данных, а также об их удалении при отсутствии иных оснований для обработки персональных данных, предусмотренных законодательными актами;

в случаях, когда обработка персональных данных является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами;

в случаях, когда законодательными актами прямо предусматривается обработка персональных данных без согласия субъекта персональных данных.

9. Обработка специальных персональных данных без согласия субъекта персональных данных запрещается, за исключением следующих случаев:

если специальные персональные данные сделаны общедоступными персональными данными самим субъектом персональных данных;

при оформлении трудовых отношений, а также в процессе трудовой деятельности субъекта персональных данных в случаях, предусмотренных законодательством;

в целях организации оказания медицинской помощи при условии, что такие персональные данные обрабатываются медицинским, фармацевтическим или иным работником здравоохранения, на которого возложены обязанности по обеспечению защиты персональных данных и в соответствии с законодательством распространяется обязанность сохранять врачебную тайну;

для осуществления правосудия, исполнения судебных постановлений и иных исполнительных документов, совершения исполнительной надписи; в случаях, предусмотренных законодательством в области национальной безопасности, о борьбе с коррупцией, о борьбе с терроризмом и противодействии экстремизму, о гражданстве;

для организации и проведения государственных статистических наблюдений, формирования официальной статистической информации;

для осуществления административных процедур; при документировании населения;

для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно;

в случаях, когда обработка специальных персональных данных является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами;

в случаях, когда законодательными актами прямо предусматривается обработка специальных персональных данных без согласия субъекта персональных данных.

Обработка специальных персональных данных проводится после принятия комплекса мер, направленных на предупреждение рисков, которые могут возникнуть при обработке таких персональных данных для прав и свобод субъектов персональных данных.

10. Трансграничная передача персональных данных запрещается, если на территории иностранного государства не обеспечивается надлежащий уровень защиты прав субъектов персональных данных, за исключением случаев, когда:

дано согласие субъекта персональных данных при условии, что субъект персональных данных проинформирован о рисках, возникающих в связи с отсутствием надлежащего уровня их защиты;

персональные данные получены на основании договора, заключенного (заключаемого) с субъектом персональных данных, в целях совершения действий, установленных этим договором;

персональные данные могут быть получены любым лицом посредством направления запроса в случаях и порядке, предусмотренных законодательством;

такая передача необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно;

обработка персональных данных осуществляется в рамках исполнения международных договоров Республики Беларусь;

получено соответствующее разрешение уполномоченного органа по защите прав субъектов персональных данных.

11. Больница при осуществлении обработки персональных данных:

принимает меры, необходимые и достаточные для обеспечения выполнения требований законодательства и локальных правовых актов в области персональных данных;

принимает 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;

назначает лиц, ответственных за осуществление внутреннего контроля за обработкой персональных данных;

издает локальные правовые акты, определяющие политику и вопросы обработки и защиты персональных данных в больнице;

ознакомливает работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства и локальных правовых актов в области обработки персональных данных, в том числе требованиями к защите персональных данных, и обучает указанных работников;

публикует или иным образом обеспечивает неограниченный доступ к настоящей Политике;

сообщает в установленном порядке субъектам персональных данных или их представителям информацию о наличии персональных данных, относящихся к соответствующим субъектам, предоставляет возможность ознакомления с этими персональными данными при обращении и (или) поступлении запросов указанных субъектов персональных данных или их представителей, если иное не установлено законодательством;

прекращает обработку и уничтожает персональные данные в случаях, предусмотренных законодательством в области персональных данных;

совершает иные действия, предусмотренные законодательством в области персональных данных.

12. Источником информации обо всех персональных данных является непосредственно субъект персональных данных.

Если иное не установлено актами законодательства, больница вправе получать персональные данные субъекта персональных данных от третьих лиц при наличии письменного согласия субъекта на получение его персональных данных от третьих лиц.

13. Персональные данные в больнице обрабатываются следующими способами:

с использованием средств автоматизации (совершение действий (операций) с такими данными с помощью объектов вычислительной техники в компьютерной сети);

без использования средств автоматизации, если при этом обеспечиваются поиск персональных данных и (или) доступ к ним по определенным критериям (картотеки, списки, базы данных, журналы и др.).

14. Персональные данные обрабатываются с согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством в области персональных данных.

Согласие субъекта персональных данных представляет собой свободное, однозначное, информированное выражение его воли, посредством которого он разрешает обработку своих персональных данных.

Согласие субъекта персональных данных может быть получено в письменной форме, в виде электронного документа или в иной электронной форме.

В случае смерти субъекта персональных данных, объявления его умершим согласие на обработку его персональных данных дают один из наследников, близких родственников, усыновителей (удочерителей), усыновленных (удочеренных) либо супруг (супруга) субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

В случае признания субъекта персональных данных недееспособным или ограниченно дееспособным, а также до достижения им возраста шестнадцати лет, за исключением вступления в брак до достижения возраста шестнадцати лет, согласие на обработку его персональных данных дает один из его законных представителей. Законодательными актами может быть предусмотрен иной возраст несовершеннолетнего, до достижения которого согласие на обработку его персональных данных дает один из его законных представителей.

Лица в случае дачи согласия на обработку персональных данных вместо субъекта персональных данных пользуются правами субъекта персональных данных, предусмотренными законодательными актами.

15. До получения согласия субъекта персональных данных больница должна разъяснить субъекту персональных данных его права, связанные с обработкой персональных данных, механизм реализации таких прав, а также последствия дачи согласия субъекта персональных данных или отказа в даче такого согласия. Если цели обработки персональных данных не требуют обработки информации, эта информация не обрабатывается оператором при получении согласия субъекта персональных данных.

16. Обработка персональных данных, в том числе содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такая обработка осуществляется при непосредственном участии человека.

Руководитель структурного подразделения, осуществляющего обработку персональных данных без использования средств автоматизации:

определяет места хранения персональных данных (материальных носителей); осуществляет контроль наличия в структурном подразделении условий, обеспечивающих сохранность персональных данных;

и исключаяющих несанкционированный к ним доступ;

информирует лиц, осуществляющих обработку персональных данных без использования средств автоматизации, о перечне обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки;

организует раздельное, то есть не допускающее смешение, хранение материальных носителей персональных данных (документов, дисков, дискет, USB флеш-накопителей, пр.), обработка которых осуществляется в различных целях.

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Уточнение персональных данных при их обработке без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

17. Больница вправе поручить обработку персональных данных от своего имени или в своих интересах уполномоченному лицу на основании заключаемого с этим лицом договора.

В договоре между оператором и уполномоченным лицом, акте законодательства либо решении государственного органа должны быть определены:

цели обработки персональных данных;

перечень действий, которые будут совершаться с персональными данными уполномоченным лицом;

обязанности по соблюдению конфиденциальности персональных данных; меры по обеспечению защиты персональных данных в соответствии со ст. 17 Закона Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных».

Уполномоченное лицо не обязано получать согласие субъекта персональных данных. Если для обработки персональных данных по поручению больницы необходимо получение согласия субъекта персональных данных, такое согласие получает больница.

18. Передача персональных данных третьим лицам допускается только в случаях, установленных законодательством, Политикой, локальными правовыми актами по вопросам обеспечения конфиденциальности и безопасности персональных данных.

Больница без согласия субъекта персональных данных не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено законодательством.

Передача персональных данных осуществляется ответственным за обработку персональных данных должностным лицом на основании письменного или устного поручения главного врача, заместителя главного врача или руководителя структурного подразделения.

Должностное лицо, предоставившее персональные данные третьим лицам, направляет письменное уведомление субъекту персональных данных о факте передачи его данных третьим лицам, за исключением случаев, определенных законодательством, в частности, если:

субъект персональных данных уведомлен об осуществлении обработки его персональных данных оператором, который получил соответствующие данные;

персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

персональные данные обрабатываются для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных.

Запрещается передача персональных данных по телефону, факсу, электронной почте, за исключением случаев, установленных законодательством и локальными правовыми актами.

Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах персональные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

Информация, содержащая персональные данные, должна передаваться способом, обеспечивающим защиту от неправомерного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий в отношении такой информации.

19. Лица, получающие персональные данные, должны предупреждаться о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и с соблюдением режима конфиденциальности. Больница вправе требовать от этих лиц подтверждения того, что это правило соблюдено.

20. В целях внутреннего информационного обеспечения могут создаваться справочные материалы, в которые с письменного согласия субъекта персональных данных, если иное не предусмотрено законодательством, могут включаться его фамилия, имя, отчество, место работы, должность, абонентский номер, адрес электронной почты, иные персональные данные, сообщаемые субъектом персональных данных.

21. Доступ к обрабатываемым персональным данным предоставляется только работникам больницы, служебные обязанности которых предполагают работу с персональными данными, должности, которых включены в перечень должностей структурных подразделений, имеющих допуск на обработку персональных данных, и только на период, необходимый для работы с соответствующими данными,

Если необходимо предоставить доступ к персональным данным работникам, не входящим в перечень лиц, имеющих доступ к персональным данным, им может быть предоставлен временный доступ к ограниченному кругу персональных данных по распоряжению главного врача или заместителя главного врача по организационно-методической работе. Работники, которым предоставлен временный допуск, должны быть ознакомлены под подпись со всеми локальными правовыми актами в области персональных данных, а также должны подписать обязательство о неразглашении персональных данных.

Работники, обрабатывающие персональные данные без использования средств автоматизации, информируются о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных законодательством и Политикой.

Работникам, не имеющим надлежащим образом оформленного допуска, доступ к персональным данным запрещается.

Лицо, получившее доступ к персональным данным, обязано не допускать предоставления, распространения, разглашения и использования без согласия субъекта персональных данных информации о нем, за исключением случаев предусмотренных законодательными актами.

При необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных персональные данные, подлежащие распространению или использованию, копируются способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных.

22. Субъекты персональных данных имеют право на:
отзыв согласия субъекта персональных данных;

получение информации, касающейся обработки персональных данных, и изменение персональных данных;

получение информации о предоставлении своих персональных данных третьим лицам;

требование прекращения обработки персональных данных и (или) их удаления;

обжалование действий (бездействия) и решений оператора, связанных с обработкой персональных данных.

23. Под защитой персональных данных понимается ряд правовых, организационных и технических мер, направленных на:

обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

соблюдение конфиденциальности информации;

реализацию права на доступ к информации.

24. Меры по обеспечению безопасности персональных данных при их обработке для обеспечения исполнения обязанностей оператора устанавливаются в соответствии с локальными правовыми актами, регламентирующими вопросы обеспечения безопасности персональных данных при их обработке (включая, но не ограничиваясь):

предоставление субъектам персональных данных необходимой информации до получения их согласий на обработку персональных данных; предоставление субъекту персональных данных информации о его персональных данных, а также о представлении его персональных данных третьим лицам, за исключением случаев, предусмотренных законодательными актами;

разъяснение субъектам персональных данных их прав, связанных с обработкой персональных данных;

получение согласий субъектов персональных данных на обработку их персональных данных, за исключением случаев, предусмотренных законодательством;

назначение лиц, ответственных за внутренний контроль за обработкой персональных данных в больнице;

издание документов, определяющих политику в отношении обработки персональных данных;

обеспечение неограниченного доступа, в том числе с использованием глобальной компьютерной сети Интернет, к документам, определяющим политику в отношении обработки персональных данных, до начала такой обработки;

ознакомление работников, непосредственно обрабатывающих персональные данные, с положениями законодательства о персональных данных;

установление порядка доступа к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе), ограничивая и регламентируя состав работников, функциональные обязанности которых требуют доступа к информации, содержащей персональные данные (в том числе путем использования паролей доступа к электронным информационным ресурсам), а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

осуществление технической и криптографической защиты персональных данных в порядке, установленном Оперативно-аналитическим центром при Президенте Республики Беларусь, в соответствии с классификацией информационных ресурсов (систем), содержащих персональные данные;

установление правил обработки персональных данных в больнице, внесение изменений и дополнений в Политику, самостоятельно в рамках требований законодательства разрабатывать и применять формы документов, необходимых для исполнения обязанностей оператора;

прекращение обработки персональных данных, а также осуществление их удаления или блокирования (обеспечение прекращения обработки персональных данных, а также их удаления или блокирования уполномоченным лицом) при отсутствии оснований для обработки персональных данных, предусмотренных законодательными актами;

обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

уведомление уполномоченного органа по защите прав субъектов персональных данных о нарушениях систем защиты персональных данных незамедлительно, но не позднее трех рабочих дней после того, как оператору стало известно о таких нарушениях, за исключением случаев, предусмотренных уполномоченным органом по защите прав субъектов персональных данных;

расследование случаев несанкционированного доступа или разглашения персональных данных с привлечением виновных работников к ответственности, принятием иных мер;

внедрение программных и технических средств защиты информации в электронном виде; восстановление персональных данных модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

определение угроз безопасности персональных данных при их обработке;

применение организационных мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных;

учет машинных носителей персональных данных;

изменение, блокирование или удаление недостоверных или полученных незаконным путем персональных данных субъекта персональных данных по требованию уполномоченного органа по защите прав субъектов персональных данных, если иной порядок внесения изменений в персональные данные, их блокирования или удаления не установлен законодательными актами;

внесение изменений в персональные данные, которые являются неполными, устаревшими или неточными, за исключением случаев, когда иной порядок внесения изменений в персональные данные установлен законодательными актами либо если цели обработки персональных данных не предполагают последующих изменений таких данных;

ограничение обработки персональных данных достижением конкретных, заранее заявленных законных целей;

хранение персональных данных в форме, позволяющей идентифицировать субъектов персональных данных, не дольше, чем этого требуют заявленные цели обработки персональных данных;

обеспечение условий для хранения документов, содержащих персональные данные, в ограниченном доступе;

предоставление уполномоченному органу по защите прав субъектов персональных данных информации, необходимой для определения законности действий операторов (уполномоченных лиц);

осуществление иных прав, предусмотренных законодательством и локальными правовыми актами в области обработки и защиты персональных данных;

исполнение иных требований уполномоченного органа по защите прав субъектов персональных данных об устранении нарушений законодательства о персональных данных;

исполнение иных обязанностей, предусмотренных законодательными актами.

25. В целях обеспечения требований соблюдения конфиденциальности и безопасности при обработке персональных данных больница предоставляет должностным лицам, работающим с персональными данными, необходимые условия для выполнения указанных требований:

знакомит работника под подпись с требованиями Политики, с должностной инструкцией и иными локальными правовыми актами по вопросам конфиденциальности и безопасности персональных данных;

представляет архивы для документов, средства для доступа к информационным ресурсам (ключи, пароли и т.п.);

обучает правилам эксплуатации средств защиты информации;

проводит иные необходимые мероприятия.

Должностным лицам, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

Должностные лица, работающие с персональными данными, обязаны использовать информацию о персональных данных исключительно для целей, связанных с исполнением своих трудовых обязанностей.

При прекращении выполнения трудовой функции, связанной с обработкой персональных данных, все носители информации, содержащие персональные данные (оригиналы и копии документов, машинные и бумажные носители и пр.), которые находились в распоряжении должностного лица в связи с исполнением должностных обязанностей, данный работник должен передать своему непосредственному руководителю.

Обеспечение конфиденциальности персональных данных не требуется в случае:

обезличивания персональных данных (действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных);

для общедоступных персональных данных (персональные данные, распространенные самим субъектом персональных данных либо с его согласия или распространенные в соответствии с требованиями законодательных актов).

26. Должностные лица, работающие с персональными данными, обязаны немедленно сообщать своему непосредственному руководителю обо всех ставших им известными фактах получения третьими лицами несанкционированного доступа либо попытки получения доступа к персональным данным, об утрате или недостатке носителей информации, содержащих персональные данные, удостоверений, пропусков, ключей от сейфов (хранилищ), личных печатей, электронных ключей и других фактах, которые могут привести к несанкционированному доступу к персональным данным, а также о причинах и условиях возможной утечки этих сведений.

27. Безопасность персональных данных при их обработке в компьютерной сети обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в компьютерной сети информационные технологии.

Технические и программные средства защиты информации должны удовлетворять устанавливаемым в соответствии с г законодательством требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в компьютерной сети, в установленном порядке проходят процедуру оценки соответствия.

Работа с персональными данными в компьютерной сети должна быть организована таким образом, чтобы обеспечивалась сохранность носителей персональных данных и средств защиты информации, а также исключалась возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа.

Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернета, запрещается.

При обработке персональных данных в компьютерной сети пользователями должно быть обеспечено:

недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

недопущение несанкционированного выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

При обработке персональных данных в компьютерной сети работниками отдела автоматизированных систем управления должны обеспечиваться:

обучение лиц, использующих средства защиты информации, применяемые в компьютерной сети, правилам работы с ними;

учет лиц, допущенных к работе с персональными данными в компьютерной сети, прав и паролей доступа;

учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

описание системы защиты персональных данных.

Специфические требования по защите персональных данных в отдельных автоматизированных системах определяются утвержденными в установленном порядке инструкциями по их использованию и эксплуатации.

Все находящиеся на хранении и в обращении съемные носители (диски, дискеты, USB флеш-накопители, пр.), содержащие персональные данные, подлежат учету. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

Учет и выдачу съемных носителей персональных данных осуществляют работники отдела автоматизированных систем управления.

При работе со съемными носителями, содержащими персональные данные, запрещается: хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах либо оставлять их без присмотра или передавать на хранение другим лицам;

выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т.д.

О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений должно быть немедленно сообщено заместителю главного врача по медицинской части.

28. При хранении персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных.

Документы, включающие в себя персональные данные, содержащиеся на бумажных носителях, находятся в специально отведенных для этого местах с ограниченным доступом в

условиях, которые обеспечивают их защиту от несанкционированного доступа. Перечень мест хранения документов определяется больницей.

Персональные данные, хранящиеся в электронном виде, защищаются от несанкционированного доступа с помощью специальных технических и программных средств защиты. Хранение персональных данных в электронном виде вне применяемых больницей информационных систем и специально обозначенных баз данных (внесистемное хранение персональных данных) не допускается.

Персональные данные должны храниться в форме, позволяющей идентифицировать субъекта персональных данных, но не дольше, чем этого требуют цели их обработки, если иной срок не установлен законодательством или договором, стороной которого является субъект персональных данных.

29. Уничтожение или обезличивание персональных данных должно производиться способом, исключающим дальнейшую обработку этих персональных данных. При этом в случае необходимости следует сохранять возможность обработки иных данных, зафиксированных на соответствующем материальном носителе (удаление, вымарывание).

Если иное не предусмотрено законодательством, обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки, в случае утраты необходимости в достижении этих целей или по истечении сроков их хранения.

При необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

30. Контроль за соблюдением работниками законодательства и локальных правовых актов в области персональных данных, в том числе требований к защите персональных данных, осуществляется с целью проверки соответствия обработки персональных данных работниками законодательству и локальным правовым актам в области персональных данных, в том числе требованиям к защите персональных данных, а также принятых мер, направленных на предотвращение и выявление нарушений законодательства в области персональных данных, выявления возможных каналов утечки и несанкционированного доступа к персональным данным, устранения последствий таких нарушений.

31. Персональная ответственность за соблюдение требований законодательства и локальных нормативных актов в области персональных данных в структурных подразделениях, а также за обеспечение конфиденциальности и безопасности персональных данных возлагается на их руководителей. Лица, виновные в нарушении требований законодательства, несут ответственность, предусмотренную законодательными актами. В случае, если больница поручает обработку персональных данных уполномоченному лицу, ответственность перед субъектом персональных данных за действия указанного лица несет больница. Уполномоченное лицо несет ответственность перед больницей.