Национальный центр защиты персональных данных Республики Беларусь
Государственное учреждение «Республиканский научно-практический центр медицинских технологий, информатизации, управления и экономики здравоохранения»

Заинтересованные государственные органы, иные организации и граждане

РЕКОМЕНДАЦИИ

по обработке персональных данных в сфере здравоохранения

Материал подготовлен Национальным центром защиты персональных данных Республики Беларусь (далее – Центр) совместно с государственным учреждением «Республиканский научно-практический центр медицинских технологий, информатизации, управления и экономики здравоохранения» с использованием правовых актов по состоянию на 18 октября 2024 г.

В соответствии с нормативной правовой базой в материале раскрываются подходы Министерства здравоохранения Республики Беларусь и Центра по вопросам обработки персональных данных и даются Рекомендации по организации такой обработки в сфере здравоохранения.

Правовое регулирование:

Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» (далее – Закон о защите персональных данных);

Закон Республики Беларусь от 18 июня 1993 г. № 2435-XII «О здравоохранении» (далее – Закон о здравоохранении);

Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» (далее – Закон об информации);

Указ Президента Республики Беларусь от 28 октября 2021 г. № 422 «О мерах по совершенствованию защиты персональных данных» (далее – Указ № 422);

Указ Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации»;

постановление Министерства здравоохранения Республики Беларусь от 7 июня 2021 г. № 74 «О формах и порядке дачи и отзыва согласия на внесение и обработку персональных данных пациента» (далее – Инструкция № 74);

постановление Министерства здравоохранения Республики Беларусь от 2 ноября 2005 г. № 44 «О порядке информирования населения об оказании медицинской помощи в организациях здравоохранения и о порядке направления для получения медицинской помощи» (далее постановление – № 44);

постановление Министерства юстиции Республики Беларусь от 24 мая 2012 г. № 140 «О перечне типовых документов Национального архивного фонда Республики Беларусь» (далее – Постановление № 140);

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» (далее – Приказ № 66);

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 194 «Об обучении по вопросам защиты персональных данных» (в ред. приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 23.11.2023 № 218) (далее – Приказ № 194);

приказ Департамента по архивам и делопроизводству Министерства юстиции Республики Беларусь от 1 апреля 2019 г. № 11 «Об установлении перечня документов Национального архивного фонда Республики Беларусь, образующихся в процессе деятельности государственных органов, иных организаций и индивидуальных предпринимателей по здравоохранению, физической культуре и спорту, туризму, с указанием сроков хранения» (далее – Приказ № 11);

приказ директора Национального центра защиты персональных данных Республики Беларусь от 15 ноября 2021 г. № 12 «О классификации информационных ресурсов (систем)» (далее – Приказ № 12);

приказ директора Национального центра защиты персональных данных Республики Беларусь от 15 ноября 2021 г. № 14 «О трансграничной передаче персональных данных» (в ред. приказа директора Национального центра защиты персональных данных Республики Беларусь от 26.12.2022 № 114) (далее – Приказ № 14).

Иные источники:

Рекомендации по составлению документа, определяющего политику оператора (уполномоченного лица) в отношении обработки персональных данных (режим доступа: https://cpd.by/pravovaya-osnova/metodologicheskiye-dokumenty-rekomendatsii/);

Рекомендации об обработке персональных данных в связи с трудовой (служебной) деятельностью (режим доступа: https://cpd.by/pravovaya-osnova/metodologicheskiye-dokumenty-rekomendatsii/);

Рекомендации о взаимоотношениях операторов и уполномоченных лиц при обработке персональных данных (режим доступа: https://cpd.by/pravovaya-osnova/metodologicheskiye-dokumenty-rekomendatsii/);

Постатейный комментарий к Закону Республики Беларусь «О защите персональных данных» (режим доступа: https://cpd.by/pravovaya-osnova/metodologicheskiye-dokumenty-rekomendatsii/postatejnyj-kommentarij-k-zakonu-respubliki-belarus-o-zashhite-personalnyh-dannyh/).

Настоящие Рекомендации подготовлены в целях определения единообразных подходов к обработке персональных данных организациями здравоохранения Республики Беларусь независимо от формы собственности и ведомственной подчиненности при организации оказания медицинской помощи гражданам, проведении научно-исследовательских работ и иной деятельности, необходимой для реализации функций организации.

Следует учитывать, что в организациях здравоохранения обработка персональных данных осуществляется в том числе при оформлении трудовых отношений, в процессе трудовой деятельности, а также соискателей на трудоустройство. Обработку персональных данных в этих целях необходимо осуществлять в соответствии с упомянутыми Рекомендациями Центра об обработке персональных данных в связи с трудовой (служебной) деятельностью.

I Общие положения законодательства о персональных данных и особенности обработки персональных данных в сфере здравоохранения

1. Понятие персональных данных

1.1. Закон о защите персональных данных регулирует отношения, связанные с защитой персональных данных при их обработке, осуществляемой:

с использованием средств автоматизации (например, обработка с использованием компьютера, мобильного телефона);

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 другое) (например, журнал учета посетителей).

В силу абзаца девятого статьи 1 Закона о защите персональных данных персональными данными признается любая информация,

относящаяся к идентифицированному физическому лицу (т.е. гражданину) или лицу, которое может быть идентифицировано.

С учетом этого можно выделить два вида информации, которая может признаваться персональными данными:

информация, относящаяся к идентифицированному лицу;

информация, относящая к лицу, которое может быть идентифицировано.

Идентифицированным является лицо, личность которого уже известна, которое однозначно выделено среди иных лиц (оно известно, на него можно конкретно указать, установить контакт с данным лицом и т.п.).

Как правило, информация, относящаяся к идентифицированному лицу, это указание ФИО лица в совокупности с другими данными, которые однозначно выделяют лицо среди иных лиц.

Пример.

Ковалев Михаил Михайлович, 31.12.1970 г.р., проживающий по адресу: г. Минск, ул. Уручская, 11-45.

Физическим лицом, которое может быть идентифицировано, признается лицо, которое может быть прямо или косвенно определено, в частности через фамилию, собственное имя, отчество (если таковое имеется), дату рождения, идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности (абзац семнадцатый статьи 1 Закона о защите персональных данных).

В свою очередь, физическое лицо, которое может быть прямо определено, – это лицо, личность которого можно установить на основании имеющейся информации, без использования дополнительных сведений.

Пример.

Главный врач учреждения здравоохранения "3-я городская клиническая больница имени Е.В. Клумова"; директор государственного учреждения "Минский научно-практический центр хирургии, трансплантологии и гематологии", заведующий кафедрой глазных болезней Белорусского государственного медицинского университета и т.п.

Физическое лицо, которое может быть косвенно определено, – это лицо, личность которого нельзя установить на основании той имеющейся информации, но это можно сделать путем объединения такой информации с иными располагаемыми сведениями или сведениями, которые могут быть получены из других легальных источников.

Так, поскольку в большинстве случаев имя и фамилия не являются уникальными (например, имя и фамилию Михаил Ковалев могут носить несколько десятков или даже сотен человек), то для определения

конкретного лица может потребоваться получение дополнительной информации, например, даты и места рождения, информации о месте работы, учебы, месте жительства. Схожим образом знания места работы (например, юрисконсульт такой-то организации здравоохранения) в ряде случаев недостаточно для идентификации лица, если соответствующих работников в организации несколько, и может потребоваться дополнительная информация (например, имя).

Пример.

Напрямую не известно, кто защитил диссертации на соискание ученой степени доктор медицинских наук в 2023 году, но этих лиц можно идентифицировать, получив информацию из других источников, например, на сайте Высшей аттестационной комиссии Республики Беларусь.

1.2. В работе с персональными данными необходимо также учитывать такие категории персональных данных, как:

1.2.1. общедоступные персональные данные – персональные данные, распространенные самим субъектом персональных данных (т.е. гражданином) либо с его согласия или распространенные в соответствии с требованиями законодательных актов (абзац седьмой статьи 1 Закона).

Пример.

Общедоступными персональными данными являются:

персональные данные, размещенные в открытом аккаунте в социальной сети;

сведения о руководителе и его заместителях на интернет-сайте учреждения здравоохранения.

1.2.2. специальные персональные данные – персональные данные, касающиеся расовой либо национальной принадлежности, политических взглядов, членства в профессиональных союзах, религиозных или других убеждений, здоровья или половой жизни, привлечения к административной или уголовной ответственности, а также биометрические и генетические персональные данные.

В части шестой статьи 46 Закона о здравоохранении установлено, что информация о факте обращения пациента за медицинской помощью и состоянии его здоровья, сведения о наличии заболевания, диагнозе, возможных методах оказания медицинской помощи, рисках, связанных с медицинским вмешательством, а также возможных альтернативах предлагаемому медицинскому вмешательству, иные сведения, в том числе личного характера, полученные при оказании пациенту медицинской помощи, а в случае смерти – и информация о результатах патологоанатомического исследования составляют врачебную тайну.

Персональные данные, касающиеся здоровья человека, относятся к специальным персональным данным, для которых установлен особый режим обработки.

Пример.

Специальными персональными данными, обрабатываемыми в учреждениях здравоохранения, являются сведения, содержащиеся в медицинских справках (заключениях), листках нетрудоспособности, сведения о диагнозе пациента и др. Также к специальным персональным данным относятся сведения о членстве в профессиональных союзах работников организаций здравоохранения, сведения из единого государственного банка данных о правонарушениях в отношении отдельных должностных лиц;

1.2.3. биометрические персональные данные – информация, характеризующая физиологические и биологические особенности человека, которая используется для его уникальной идентификации (отпечатки пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображение и другое).

Для отнесения персональных данных к биометрическим данным необходимо, чтобы одновременно выполнялись два условия:

информация должна характеризовать физиологические и биологические особенности человека (отпечатки пальцев рук, ладоней, и другое);

такая информация используется для уникальной идентификации соответствующего лица.

Последний признак предполагает наличие специальных технических средств, обеспечивающих уникальное сопоставление отпечатков пальцев и др. с имеющимся в базе образцом.

Пример.

Использование интеллектуальных систем распознавания лиц (изображение лица человека и его характеристики) для целей организации пропускного режима;

1.2.4. генетические персональные данные – информация, относящаяся к наследуемым либо приобретенным генетическим характеристикам человека, которая содержит уникальные данные о его физиологии либо здоровье и может быть выявлена, в частности, при исследовании его биологического образца.

Информацией, содержащей генетические персональные данные, располагают организации здравоохранения, имеющие в своем составе специализированные лаборатории (структурные подразделения), осуществляющие молекулярно-генетические, цитогенетические (кариотипирование), молекулярно-цитогенетические исследования. Объектом такого исследования является молекула ДНК (РНК).

Сведения о состоянии здоровья пациента, содержащиеся в биологических образцах (кровь, слюна, соскоб слизистой рта, выделения из половых органов, околоплодной жидкости, волосы, ногти и т.д.), медико-генетических заключениях, медицинских справках о состоянии

здоровья содержат информацию о физиологии и здоровье человека, однако не обладают уникальностью и не относятся к генетическим персональным данным.

Примером обработки генетических персональных данных могут быть положения Закона о здравоохранении, в соответствии с которыми гражданам Республики Беларусь гарантируется медико-генетическая диагностика по медицинским показаниям в государственных учреждениях здравоохранения в целях медицинской профилактики возможных наследственных заболеваний у потомства.

2. Оператор и уполномоченное лицо, субъект персональных данных

В соответствии с абзацем восьмым статьи 1 Закона о защите персональных данных **оператором** является государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, в том числе индивидуальный предприниматель, самостоятельно или совместно с иными указанными лицами организующие и (или) осуществляющие обработку персональных данных.

Учреждения здравоохранения и организации, оказывающие медицинские услуги, при оказании медицинской помощи (медицинской услуги) лицу руководствуются положениями законодательства о здравоохранении, клиническими протоколами, устанавливающими требования к обследованию и лечению в амбулаторно-поликлинических организациях здравоохранения и организациях здравоохранения, оказывающих медицинскую помощь в стационарных условиях; медицинскими показаниями. В процессе оказания медицинской помощи организация здравоохранения ведет документацию по формам, утвержденным Министерством здравоохранения Республики Беларусь (далее – Министерство здравоохранения). В этой связи организации здравоохранения осуществляют обработку персональных данных пациентов (клиентов) исходя из требований законодательства о здравоохранении и в этом случае выступают в качестве **самостоятельного оператора**.

На оператора возлагаются обязанности по организации и осуществлению работы, направленной на защиту персональных данных.

Обработка персональных данных в организации здравоохранения **ведется по следующим направлениям**:

- оказание медицинской помощи гражданам;
- осуществление научно-исследовательской деятельности;

- оформление трудовых отношений и ведение кадрового делопроизводства;
- осуществление действий в рамках гражданско-правовых договоров;
- выдача справок и иных документов в рамках осуществления административных процедур;
- подготовка ответов на обращения граждан, в том числе индивидуальных предпринимателей, юридических лиц по вопросам, входящим в компетенцию оператора;
- обеспечение пропускного и внутриобъектового режимов на объектах оператора;
- выполнение иных функций, полномочий и обязанностей, возложенных на оператора законодательством.

В соответствии с абзацем шестнадцатым статьи 1 Закона о защите персональных данных **уполномоченное лицо** – государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, которые в соответствии с актом законодательства, решением государственного органа, являющегося оператором, либо на основании договора с оператором осуществляют обработку персональных данных от имени оператора или в его интересах.

Пример.

Аутсорсинговые организации применительно к процессам обработки персональных данных, переданных организацией здравоохранения на аутсорсинг (например, сопровождение работы программного обеспечения организации здравоохранения, оказание юридических услуг), как правило, являются уполномоченными лицами.

С учетом того, что одно и то же лицо может являться оператором в одних правоотношениях и уполномоченным лицом в других, вопрос об определении правового статуса такого лица подлежит рассмотрению в каждом конкретном случае.

Так, например, организации здравоохранения в рамках оказания медицинских услуг по конкретному договору добровольного страхования медицинских расходов осуществляют обработку персональных данных в интересах страховщика (оператора). В отличие от страховщика, организация здравоохранения не определяет ключевые параметры обработки персональных данных (они определены в договоре) и действует в интересах страховой организации в соответствии с ее поручениями за вознаграждение. Именно страховая организация определяет, какие персональные данные подлежат обработке, и предоставляет указания (инструкции) по обработке, которым должно следовать уполномоченное лицо.

Соответственно, организация здравоохранения при осуществлении взаимодействия со страховой организацией ограничена в определении ключевых параметров исполнения договора, в частности, о круге лиц, целях и сроках обработки, объеме оказываемых услуг и др.

В этой связи организации здравоохранения действуют по поручению и в интересах страховых организаций (оператора) и в рассматриваемых отношениях (взаимодействие со страховой организацией) выступают **в качестве уполномоченного лица**.

В то же время при оказании непосредственно медицинской помощи застрахованному лицу и ведении медицинской документации организация здравоохранения является самостоятельным оператором.

В соответствии с Законом о защите персональных данных **субъект** – физическое лицо, в отношении которого осуществляется обработка персональных данных.

Субъектами персональных данных **могут выступать**:

- пациенты (физические лица, обратившиеся за медицинской помощью, находящиеся под медицинским наблюдением либо получающее медицинскую помощь);
- близкие родственники пациентов (родители, усыновители (удочерители), совершеннолетние дети, в том числе усыновленные (удочеренные), родные братья и сестры, дед, бабка, совершеннолетние внуки);
- законные представители пациентов (представляющие интересы недееспособных граждан, граждан, не обладающих полной дееспособностью, и граждан, признанных ограниченно дееспособными);
- водители (физические лица, управляющие транспортными средствами, самоходной машиной), кандидаты в водители;
- доноры (пациенты, прошедшие медицинский осмотр и сдающие кровь, ее компоненты, а также пациенты, отдающие свои органы для трансплантации другому лицу);
- посетители организации здравоохранения (например, сопровождающие);

(далее все перечисленные категории – пациенты, если не указано иное)

- заявители;
- медицинские работники и иные работники организаций здравоохранения;
- соискатели (физические лица, которые желают занять определенную вакансию у оператора и заявляют об этом, например, посредством направления резюме).

3. Правовые основания обработки персональных данных

Согласно абзацу шестому статьи 1 Закона о защите персональных данных под обработкой персональных данных понимается любое действие или совокупность действий, совершаемые с персональными данными, включая сбор, систематизацию, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление персональных данных.

В соответствии с частью первой пункта 3 статьи 4 Закона о защите персональных данных обработка персональных данных осуществляется с согласия субъекта персональных данных, за исключением случаев, предусмотренных Законом о защите персональных данных и иными законодательными актами.

3.1 Обработка персональных данных без согласия пациента

3.1.1. Случаи (правовые основания), когда для обработки персональных данных согласие пациента не требуется, перечислены в статьях 6 и 8 Закона о защите персональных данных. При наличии хотя бы одного из этих правовых оснований обработка персональных данных осуществляется без согласия субъекта персональных данных.

3.1.2. При этом **особого внимания требует** применение основания обработки специальных персональных данных, предусмотренного абзацем шестым пункта 2 статьи 8 Закона о защите персональных данных, которое позволяет вести обработку специальных персональных данных без получения согласия 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.

Справочно.

Согласно абзацу двадцать девятому части 1 статьи 1 Закона о здравоохранении работниками здравоохранения признаются лица, занимающие в установленном законодательством порядке должности медицинских, фармацевтических работников, а также иные лица, работающие в области здравоохранения.

К числу иных лиц, работающих в области здравоохранения, следует относить работников, обеспечивающих оказание медицинской помощи, например, дезинфекторов, медицинских регистраторов, сестер-хозяек, а также лиц, занимающих должности служащих, занятых в здравоохранении и иных работников, выполняющих вспомогательные функции в здравоохранении.

Нередки случаи, когда при организации оказания медицинской помощи пациенту доступ к его персональным данным необходим

работникам организации здравоохранения, на которых прямо не распространяется обязанность сохранять врачебную тайну, например, бухгалтеру или юрисконсульту. В этом случае также применяется упомянутое основание, например, когда бухгалтер обрабатывает информацию о платежах пациента, который получал платные медицинские услуги в организации здравоохранения.

Положения абзаца шестого пункта 2 статьи 8 Закона являются самостоятельным правовым основанием для обработки специальных персональных данных и не требуют получения согласия субъекта персональных данных.

Вместе с тем пунктом 3 статьи 3 Закона о защите персональных данных предусмотрено, что 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.

Таким законодательным актом в данном случае является Закон о здравоохранении. В части тринадцатой статьи 44 Закона о здравоохранении установлено, что при **формировании электронной медицинской карты пациента**, **информационных систем, информационных ресурсов, баз (банков) данных, реестров (регистров)** в здравоохранении согласие, отзыв согласия на внесение и обработку персональных данных пациента или лиц, указанных в части второй статьи 18 Закона о здравоохранении, информации, составляющей врачебную тайну, отказ от их внесения и обработки оформляются на бумажном носителе или иным способом, не запрещенным законодательством.

Следовательно, если обработка специальных персональных данных в целях организации оказания медицинской помощи осуществляется организацией здравоохранения только на бумажных носителях, то такое согласие получать не требуется. А в случае использования организацией здравоохранения средств автоматизации (включая внесение сведений в информационные ресурсы (информационные системы)) необходимо получить согласие пациента. *Справочно.*

Примеры систематизации персональных данных без использования средств автоматизации (получение согласия на обработку персональных данных в этом случае не требуется):

ведение журнала посетителей на вахте (в журнале отражается время прихода и ухода, ФИО посетителя и данные подразделения, которое он посещает), поиск данных и доступ к ним осуществляются на основе хронологического критерия (время посещения);

хранение медицинских карт пациентов в поликлинике, поиск и доступ к данным осуществляются на основе двух критериев – размещение медицинских карт по участкам и ФИО пациента.

К информационным ресурсам и системам относится в том числе любой медицинский аппарат, куда вносятся сведения о пациенте (компьютерный томограф, магнитно-резонансный томограф и т.п.).

Таким образом, при определении необходимости наличия согласия субъекта на обработку персональных данных следует, в первую очередь, исходить из применяемых способов обработки персональных данных. При этом обработкой с использованием средств автоматизации признаются любые действия с персональными данными, осуществляемые в электронной форме.

3.1.3. Согласие субъекта персональных данных на обработку персональных данных не требуется в случаях, когда обработка персональных данных является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами (законами, декретами и указами Президента Республики Беларусь).

Обработку персональных данных по данному основанию могут осуществлять как **государственные органы** для выполнения своих задач и функций, так и **иные организации** при выполнении возложенных на них обязанностей (полномочий) в общественных интересах.

Пример.

Частью второй статьи 19 Закона Республики Беларусь от 30 ноября 2010 г. № 197-З «О донорстве крови и ее компонентов» установлено, что волонтерами не могут быть лица, имеющие непогашенную или неснятую судимость, а также признанные в установленном порядке недееспособными или ограниченно дееспособными. Для выполнения этой обязанности необходимо получить соответствующие сведения.

Обработка указанных персональных данных волонтеров осуществляется без согласия субъекта персональных данных на основании абзаца двадцатого статьи 6 и абзаца семнадцатого пункта 2 статьи 8 Закона о защите персональных данных.

Как обработка персональных данных, которая является необходимой для выполнения таких обязанностей (полномочий), рассматриваются и случаи, когда **законодательный акт содержит отсылочную норму** об определении порядка реализации обязанностей (полномочий) в иных нормативных правовых актах, например, в постановлениях Совета Министров Республики Беларусь, республиканских органов государственного управления.

Пример.

В соответствии с положениями статьи 31-1 Закона Республики Беларусь от 13 июля 2012 г. № 408-З «О наркотических средствах, психотропных веществах, их прекурсорах и аналогах» в целях профилактики потребления наркотических средств, психотропных веществ, аналогов создается Единая система учета лиц, потребляющих наркотические средства, психотропные вещества, их аналоги.

Формирование и ведение Единой системы учета лиц, потребляющих наркотические средства, психотропные вещества, их аналоги, осуществляются Министерством здравоохранения в порядке, устанавливаемом Советом Министров Республики Беларусь.

Министерством здравоохранения обеспечивается незамедлительное представление сведений о лицах, включенных в Единую систему учета лиц, потребляющих наркотические средства, психотропные вещества, их аналоги, в органы внутренних дел по их месту жительства (месту пребывания) для последующего принятия мер профилактического характера, а также по письменным запросам органов внутренних дел в установленные в них сроки.

Постановлением Совета Министров Республики Беларусь от 4 июня 2015 г. № 468 утверждено Положение о порядке формирования и ведения Единой системы учета лиц, потребляющих наркотические средства, психотропные вещества, их аналоги, где определяется порядок формирования и ведения Единой системы учета лиц, потребляющих наркотические средства, психотропные вещества, их аналоги, содержащей сведения о пациентах, потребляющих наркотические средства, психотропные вещества, их аналоги без назначения врача-специалиста и состоящих на профилактическом или диспансерном наблюдении в государственных организациях здравоохранения, оказывающих наркологическую помощь в порядке, установленном законодательством Республики Беларусь.

Обработка персональных данных для целей формирования и ведения названной Единой системы осуществляется на основании абзаца двадцатого статьи 6 и абзаца семнадцатого пункта 2 статьи 8 Закона о защите персональных данных без согласия субъекта персональных данных.

3.1.4. Еще одним случаем обработки персональных данных **без согласия пациента** является **оказание ему экстренной медицинской помощи.** В этом случае следует руководствоваться абзацем восемнадцатым статьи 6 и абзацем шестнадцатым пункта 2 статьи 8 Закона о защите персональных данных, согласно которым согласие субъекта персональных данных на обработку специальных данных не требуется для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно.

Для применения этого основания необходимо одновременное соблюдение двух условий:

- обработка персональных данных необходима для целей защиты жизни, здоровья или иных жизненно важных интересов пациента;
- получение согласия пациента на обработку персональных данных невозможно, т.к. его состояние не позволяет оценить представленную ему информацию, указанную в части первой пункта 5 статьи 5 Закона о защите персональных данных, и выразить свободное однозначное согласие на обработку его персональных данных.

Таким образом, обработка персональных данных пациента, в том числе с помощью средств автоматизации, при оказании ему экстренной медицинской помощи при соблюдении указанных условий осуществляется без согласия пациента. В последующем, как только состояние пациента позволяет перейти на оказание ему медицинской помощи в иной форме, его согласие на обработку персональных данных должно быть получено, если такая обработка предполагается с использованием средств автоматизации.

3.1.5. Согласие пациента на обработку его персональных данных также не требуется при осуществлении в отношении него административных процедур, осуществляемых организациями здравоохранения, в пределах установленного законодательством объема запрашиваемых документов и (или) сведений.

Такая обработка осуществляется на основании абзаца двадцатого статьи 6 Закона с учетом положений Закона Республики Беларусь от 28 октября 2008 г. № 433-З «Об основах административных процедур», а в отношении специальных персональных данных – абзаца тринадцатого пункта 2 статьи 8 Закона о защите персональных данных.

3.2 Согласие на обработку персональных данных и согласие на медицинское вмешательство

Важно различать согласие на обработку персональных данных и добровольное информированное согласие на предоставление медицинской помощи (согласие на медицинское вмешательство).

Медицинское вмешательство – любое воздействие и (или) иная манипуляция, выполняемые медицинским работником при оказании медицинской помощи (статья 1 Закона о здравоохранении). Медицинские вмешательства делятся на простые (определены в постановлении Министерства здравоохранения Республики Беларусь «Об установлении перечня простых медицинских вмешательств» Беларусь от 31 мая 2011 г. № 49) и сложные (все остальные случаи).

При простом медицинском вмешательстве согласие на него дается устно пациентом или лицами, указанными в части второй статьи 18 Закона о здравоохранении с отметкой медицинского работника в медицинских документах о получении такого согласия. При сложном – письменно лечащему врачу в соответствии с формой согласия, утвержденной постановлением Министерства здравоохранения от 15 апреля 2021 г. № 36 «Об установлении формы согласия пациента на сложное медицинское вмешательство».

Согласие на обработку персональных данных должно быть получено в соответствии с законодательством о персональных данных.

Таким образом, согласие на медицинское вмешательство (согласия на осуществление в отношении лица каких-либо действий, медицинских

манипуляций) является обязательным условием для организации оказания медицинской помощи пациенту и дается каждый раз перед каждым вмешательством медицинскому работнику в соответствии с законодательством о здравоохранении. Согласие на обработку персональных данных (при необходимости) пациент дает либо в соответствии с требованиями Инструкции № 74 либо в соответствии со статьей 5 Закона о защите персональных данных.

3.3. Получение согласия на обработку персональных данных пациента

Согласно статье 5 Закона о защите персональных данных согласие субъекта персональных данных представляет собой свободное, однозначное, информированное выражение его воли, посредством которого он разрешает обработку своих персональных данных.

Согласие может быть получено в письменной форме, в виде электронного документа, в иной электронной форме, предусмотренной пунктом 3 статьи 5 Закона о защите персональных данных (например, указание определенного кода после получения субъектом персональных данных СМС-сообщения или проставление соответствующей отметки на интернет-ресурсе).

Согласно пункту 4 статьи 5 Закона о защите персональных данных законодательными актами может быть предусмотрена необходимость получения согласия субъекта персональных данных только в письменной форме или в виде электронного документа.

Так, как упоминалось, часть тринадцатая статьи 44 Закона о здравоохранении устанавливает, что при формировании электронной медицинской карты пациента, информационных систем, информационных ресурсов, баз (банков) данных, реестров (регистров) в здравоохранении согласие оформляется на бумажном носителе или иным способом, не запрещенным законодательством, по формам и в порядке, устанавливаемым Министерством здравоохранения.

В развитие данной нормы Министерством здравоохранения утверждена Инструкция № 74. Пунктом 4 данного документа определено, что перед внесением персональных данных, информации, составляющей врачебную тайну, в электронную медицинскую карту пациента, информационную систему должно быть **получено письменное согласие пациента.** Причем согласие дается однократно при первичном посещении государственной организации здравоохранения.

В настоящее время законодательством не определены форма и порядок получения согласия пациента на обработку персональных данных для негосударственных организаций здравоохранения. В связи с отсутствием законодательного регулирования у негосударственных

организаций здравоохранения есть три варианта определения формы и порядка получения согласия на обработку персональных данных при использовании ими средств автоматизации для обработки персональных данных пациентов:

- воспользоваться формой и порядком получения согласия, определенными Инструкцией № 74;

- самостоятельно определить форму и порядок получения согласия;

- использовать примерную форму, разработанную Центром и самостоятельно определить порядок получения согласия.

Данная форма доступна на официальном сайте Центра по адресу: https://cpd.by/forma-soglasija-na-obrabotku-personalnyh-dannyh-razrabotana-centrom/.

При этом получение согласия субъекта для указанной цели не исключает также необходимости получения согласия субъекта персональных данных для иных целей (например, осуществление рекламной рассылки, размещение фото- и видеоизображения пациентов на сайте организации и др.).

Для подобных целей обработки персональных данных пациентов при необходимости получения согласия следует руководствоваться требованиями статьи 5 Закона о защите персональных данных.

В соответствии с частью второй пункта 9 статьи 5 Закона о защите персональных данных 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.

Согласно пункту 7 статьи 5 Закона обязанность доказывания получения согласия субъекта персональных данных возлагается на оператора.

Поэтому получение согласия следует организовать таким образом, чтобы организация здравоохранения в любой момент могла подтвердить данный факт. Механизм подтверждения получения согласия субъекта персональных данных определяется организацией здравоохранения самостоятельно.

С учетом заложенного в Законе о защите персональных данных риск-ориентированного подхода, организации здравоохранения целесообразно организовать учет полученных согласий.

Не обязательно хранить все полученные согласия централизованно, в одном месте. Например, хранение согласий соответствующим подразделением, ответственным за реализацию конкретных процессов или функций, не является нарушением Закона о защите персональных данных.

Независимо от установленного способа получения согласия на обработку персональных данных пациенту работник организации здравоохранения обязан простым и ясным языком разъяснить его права, связанные с обработкой персональных данных, механизм реализации таких прав, а также последствия дачи согласия или отказа в его даче. Эта информация должна быть предоставлена в форме, соответствующей форме выражения его согласия, отдельно от иной предоставляемой информации.

3.4. Обработка персональных данных при отказе пациента от дачи согласия или отзыве согласия

Отказ в оказании медицинской помощи в связи с отказом пациента в даче согласия на обработку персональных данных или отзыве ранее данного согласия **не допускается.**

Если пациент не дает согласия на внесение персональных данных в электронную медицинскую карту пациента или иную информационную систему, то обработка его персональных данных должна вестись на бумажных носителях медицинским, фармацевтическим или иным работником здравоохранения, на которого возложены обязанности по обеспечению защиты персональных данных.

Законодательно закреплено и право пациента без объяснения причин отозвать ранее данное согласие посредством подачи заявления в письменной форме либо в виде электронного документа.

При этом отзыв согласия имеет действие только на будущее время и не затрагивает правомерность обработки персональных данных в прошлом (часть первая пункта 4 статьи 10 Закона о защите персональных данных).

Следует также проверить, существуют ли основания для обработки персональных данных без согласия пациента. Например, если обработка требуется для формирования официальной статистической информации или для научных исследований, то организация здравоохранения вправе продолжить обработку, пока цели не будут достигнуты.

В связи с этим Инструкцией № 74 определено, что **в целях обеспечения полноты и достоверности статистического учета данных о случаях оказания медицинской помощи пациентам оператор информационной системы** с момента оформления отказа от внесения и обработки персональных данных пациента, информации, составляющей врачебную тайну, **вправе продолжить хранение и обработку обезличенных данных (информации) пациента**.

Таким образом, в случае отзыва пациентом или лицом, указанным в части второй статьи 18 Закона о здравоохранении, согласия на обработку персональных данных в информационных системах (ресурсах), при принятии организацией здравоохранения решения о продолжении хранения и обработки персональных данных пациента, необходимо осуществить обезличивание его персональных данных. Дальнейшую обработку персональных данных, информации, составляющей врачебную тайну, пациента или лица, указанного в части второй статьи 18 Закона о здравоохранении, следует осуществлять на бумажном носителе в порядке, определенном приказом Министерства здравоохранения Республики Беларусь от 30 августа 2007 г. № 710 «Об утверждении форм первичной медицинской документации в амбулаторно-поликлинических организациях», приказом Министерства здравоохранения Республики Беларусь от 1 октября 2007 г. № 792 «Об утверждении форм первичной медицинской документации в организациях здравоохранения, оказывающих стационарную помощь».

4. Сроки хранения документации в организациях здравоохранения на бумажных носителях

В соответствии с требованиями к обработке персональных данных, установленными статьей 4 Закона о защите персональных данных, обработка должна ограничиваться достижением конкретных, заранее заявленных законных целей, а хранение персональных данных должно осуществляться в форме, позволяющей идентифицировать субъекта персональных данных, не дольше, чем этого требуют заявленные цели обработки персональных данных.

В силу необходимости соблюдения требований о хранении документов, предусмотренных Законом Республики Беларусь от 25 ноября 2011 г. № 323-З «Об архивном деле и делопроизводстве в Республике Беларусь» и принятыми в его развитие нормативными правовыми актами оператор обязан обрабатывать (в частности, хранить) определенные документы, содержащие персональные данные физических лиц в течение установленного законодательством срока.

Например, постановлением № 140 определены следующие сроки хранения для:

согласия субъектов персональных данных на обработку их персональных данных – 1 год после окончания срока, на который дается согласие;

заявления субъектов персональных данных – 1 год;

уведомления о нарушениях систем защиты персональных данных – 3 года.

Форма согласия (отказа, отзыва согласия) пациента на обработку персональных данных, установленная в Инструкцией № 74, не предусматривает срока действия согласия. При этом практика получения согласия в настоящее время предполагает, что эти документы хранятся в медицинской карте пациента, а значит целесообразно установить срок хранения согласий аналогичный сроку, предусматриваемому для хранения такой медицинской документации.

В случае, когда медицинская документация ведется только в электронном виде в информационной системе организации здравоохранения при отсутствии бумажных носителей, то хранить согласия пациентов на обработку персональных данных целесообразно в отдельной папке с учетом систематизации таких согласий, например по ФИО пациента, для удобного поиска.

Сроки хранения медицинских документации, в частности, медицинской карты амбулаторного больного или медицинской карты стационарного пациента, установлены Приказом № 11.

Справочно.

В соответствии с частью тринадцатой статьи 46 Закона о здравоохранения организации здравоохранения обеспечивают хранение медицинских документов в соответствии с требованиями сохранения врачебной тайны: не допускается несанкционированный доступ посторонних лиц к медицинским документам, хранение документов в открытом доступе.

Если срок хранения не определен в акте законодательства, то он определяется самой **организацией здравоохранения**. Ориентиром выступает рассматриваемая норма Закона о защите персональных данных, а именно – возможность хранить данные не дольше, чем это необходимо для достижения цели их обработки.

Хранение персональных данных без правового основания, в том числе, если такие данные более не требуются для достижения заявленной цели, является незаконной обработкой персональных данных и влечет административную ответственность по части 1 ст. 23.7 Кодекса Республики Беларусь об административных правонарушениях.

5. Обмен персональными данными между организациями здравоохранения

В целях своевременного оказания медицинской помощи граждане Республики Беларусь закрепляются за государственными учреждениями здравоохранения по их месту жительства (месту пребывания) (часть

восьмая статьи 14 Закона о здравоохранении) или по их месту работы (ведомственные учреждения здравоохранения).

Абзацем пятым части первой статьи 9 Закона о здравоохранении определены полномочия главных управлений по здравоохранению областных исполнительных комитетов, Комитета по здравоохранению Минского городского исполнительного комитета, к которым относится, в частности, организация оказания организациями здравоохранения, осуществляющими в установленном законодательством порядке медицинскую деятельность, медицинской помощи пациентам, проживающим на соответствующей территории, а также координация в пределах своей компетенции деятельности этих организаций.

Таким образом, передача сведений о пациентах из одной организации здравоохранения в другую (например, выписки из медицинских документов) является составным элементом организации оказания медицинской помощи и может быть осуществлена без их согласия. Правовым основанием обработки персональных данных выступает абзац шестой пункта 2 статьи 8 Закона.

Постановлением № 44 утверждена Инструкция о порядке направления пациентов для получения медицинской помощи в организациях здравоохранения (далее по тексту данного раздела – Инструкция), которой урегулирован порядок такого направления, в том числе установлены документы, необходимые для оказания квалифицированной медицинской помощи и передаваемые из организации здравоохранения в другую организацию здравоохранения и обратно.

Так, пунктом 9 Инструкции установлено, что пациенту, направляемому для получения медицинской помощи в организации здравоохранения республиканского подчинения, лечащим врачом выдаются:

сопроводительное письмо направляющей организации;

выписка из медицинской документации больного с заключением специалистов о необходимости оказания медицинской помощи в организациях здравоохранения республиканского подчинения;

результаты клинических, рентгенологических и других методов исследования сроком не более месячной давности;

при направлении детей в выписке из медицинской документации дополнительно указываются данные о профилактических прививках.

При этом, исходя из анализа содержания указанного пункта, сопроводительные документы выдаются на руки пациенту, и он самостоятельно предоставляет их в организацию здравоохранения, в которую направлен для оказания ему медицинской помощи.

В соответствии с пунктами 10 и 11 Инструкции по результатам рассмотрения медицинской документации информация о принятом решении сообщается направившей организации с указанием даты приема пациента для очной консультации, обследования или госпитализации.

При отсутствии показаний для госпитализации в адрес направившей организации направляется консультативное заключение с подробными рекомендациями по дальнейшему лечению пациента в соответствующей организации здравоохранения.

Взаимодействие между организациями здравоохранения в настоящее время в отдельных случаях осуществляется в рамках использования медицинских информационных систем.

Согласно абзацу восьмому статьи 1 Закона о защите персональных данных в отношении используемых информационных систем, ресурсов, баз (банков) данных, реестров (регистров) организации здравоохранения выступают операторами, которые в соответствии с положениями Закона о защите персональных данных должны иметь надлежащее правовое основание для обработки персональных данных, в том числе для их предоставления. Юридические лица, индивидуальные предприниматели, которые по поручению организаций здравоохранения разрабатывают эти системы (ресурсы) и в дальнейшем их обслуживают, признаются уполномоченными лицами (абзац шестнадцатый статьи 1 Закона о защите персональных данных).

Таким образом, для осуществления обмена информацией в рамках использования подобных медицинских информационных систем согласия субъекта персональных данных на передачу его персональных данных не требуется. Однако, как упоминалось, при этом необходимо получать согласие субъекта персональных данных на внесение сведений о нем в указанные информационные системы.

6. Предоставление персональных данных организациями здравоохранения третьим лицам

В соответствии с абзацем десятым статьи 1 Закона о защите персональных данных предоставление персональных данных – действия, направленные на ознакомление с персональными данными определенного лица или круга лиц.

Предоставление персональных данных пациентов или работников организации здравоохранения сторонним организациям является обработкой персональных данных и должно осуществляться с соблюдением установленных Законом о защите персональных данных

требований, в том числе при наличии соответствующего правового основания.

В качестве правовых оснований предоставления персональных данных могут выступать положения статей 6 и 8 Закона о защите персональных данных, а также согласие субъекта персональных данных.

В частности, обработка персональных данных осуществляется без согласия субъекта персональных данных, когда она является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами (абзац двадцатый статьи 6, в отношении специальных персональных данных – абзац семнадцатый пункта 2 статьи 8 Закона о защите персональных данных). Данное правовое основание применяется и в том случае, если обязанности (полномочия) закреплены в законодательном акте, а порядок их реализации – в принятом в его развитие ином нормативном правовом акте.

При этом особенностью предоставления персональных данных пациентов организациями здравоохранения является то, что многие обрабатываемые ими сведения относятся к врачебной тайне. В этой связи при предоставлении сведений о пациентах третьим лицам организациям здравоохранения необходимо учитывать положения Закона о здравоохранении.

В соответствии с частью седьмой статьи 46 Закона о здравоохранении предоставление информации, составляющей врачебную тайну, без согласия пациента или лиц, указанных в части второй статьи 18 Закона о здравоохранении, допускается по запросу в письменной форме и (или) в виде электронного документа, оформленного в соответствии с законодательством об электронных документах и электронной цифровой подписи органам и организациям, перечисленным в абзацах втором – одиннадцатом части восьмой статьи 46 Закона о здравоохранении, а также в иных случаях, установленных законодательными актами (абзац двенадцатый части седьмой статьи 46 Закона о здравоохранении).

В запросе на предоставление персональных данных пациентов или работников запрашивающая организация должна указать цели обработки персональных данных, объем и содержание запрашиваемых персональных данных, а также правовые основания на обработку персональных данных пациентов или работников. При этом запрашивающей организации необходимо также указать конкретную норму законодательного акта, которая наделяет ее обязанностью (полномочием), требующей обработки персональных данных или специальных персональных данных. Если правовым основанием для обработки персональных данных является согласие субъекта персональных данных, то запрос направляется с приложением копии согласия.

Оценка правовых оснований предоставления персональных данных пациентов и работников организацией здравоохранения должна осуществляться самостоятельно с учетом информации, содержащейся в запросе.

Имеют место случаи, когда организации здравоохранения допускают нарушения и Закона о защите персональных данных, и Закона о здравоохранении, предоставляя персональные данные по любым поступающим в их адрес запросам без их должного критического осмысления с позиции соблюдения требований законодательства.

Пример.

Страховая организация с целью оценки страховых рисков при заключении договора добровольного медицинского страхования направила в организацию здравоохранения запрос с целью уточнения достоверности сведений о состоянии здоровья, указанных в анкете клиента. В качестве правового основания страховая организация указала абзац седьмой части седьмой статьи 46 Закона о здравоохранении. Организация здравоохранения предоставила запрашиваемые сведения о состоянии здоровья, диагнозах и наличии хронических заболеваний пациента страховой организации.

В то же время абзац седьмой части седьмой статьи 46 Закона о здравоохранении допускает предоставление информации, составляющей врачебную тайну, по запросам страховых организаций для решения вопроса о назначении страховых выплат, т.е. когда страховой случай уже наступил, и страховая организация желает удостовериться в определенных обстоятельствах, необходимых для назначения страховых выплат.

В рассматриваемом же примере речь идет о проверке правильности предоставленных потенциальным клиентом страховой организации сведений о состоянии здоровья для выбора оптимального страхового тарифа и конкретных условий добровольного медицинского страхования. Следовательно, организация здравоохранения не имела правовых оснований для предоставления указанных сведений в адрес страховой организации.

Пример.

Учреждение образования в рамках проводимого в соответствии с Положением о порядке признания детей находящимися в социально опасном положении, утвержденным постановлением Совета Министров Республики Беларусь от 15 января 2019 г. № 22, социального расследования запросило в организации здравоохранения сведения о наличии у законного представителя несовершеннолетнего психического расстройства (заболевания).

Организация здравоохранения правомерно отказала в предоставлении запрашиваемых сведений учреждению образования в соответствии со статьей 46 Закона о здравоохранении, поскольку организации здравоохранения права на предоставление такой информации законодательством не установлено.

Пример.

В организацию здравоохранения поступил запрос от предприятия с просьбой предоставить информацию о нахождении на лечении их работника для определения уважительности причины его отсутствия на работе. В качестве правового основания предприятие ссылалось на пункт 3 части первой статьи 55 ТК, обязывающий нанимателя вести учет фактически отработанного работником времени.

Однако абзац шестой части восьмой статьи 46 Закона о здравоохранении не предусматривает предоставление указанной информации по запросам нанимателя.

В числе часто встречающихся правовых оснований для запроса информации указываются, например, служебная необходимость, укрепление межведомственного взаимодействия, проведение воспитательной работы и др. без ссылок на конкретные нормы законодательных актов. Приведенные примеры и иные подобные формулировки не являются правовым основанием для предоставления запрашиваемых сведений.

Таким образом, для предоставления персональных данных третьим лицам у организации здравоохранения должны быть надлежащие правовые основания. Информация, составляющая врачебную тайну, может быть представлена третьим лицам только в случаях, предусмотренных законодательными актами либо с согласия пациента или лиц, указанных в части второй статьи 18 Закона о здравоохранении.

Ответственность за незаконное предоставление сведений о пациентах или работниках несет организация здравоохранения.

В этой связи, в случае если у организации здравоохранения возникли обоснованные сомнения относительно правовых оснований предоставления персональных данных, она вправе запрашивать дополнительную информацию для выполнения требований, предусмотренных статьей 4 Закона, в частности, уточнения целей и, соответственно, объема информации, необходимой для их достижения.

Аналогичный подход применяется и в случаях предоставления другими организациями персональных данных по запросу организации здравоохранения.

Пример.

Запрос у ЖЭС списка проживающих на определенной территории для целей уточнения списка пациентов, закрепленных за данной организацией здравоохранения, не имеет правового основания, поскольку в законодательстве отсутствуют порядок и основания такого взаимодействия.

Обращаем также внимание, что статья 12 Закона о защите персональных данных закрепляет право субъекта персональных данных получать от оператора информацию о предоставлении своих персональных данных третьим лицам. Наличие у субъекта такого права предполагает

обязанность организации здравоохранения обеспечить учет фактов передачи персональных данных третьим лицам.

7. Трансграничная передача персональных данных

Трансграничная передача персональных данных представляет собой передачу персональных данных на территорию иностранного государства.

Примерами трансграничной передачи могут быть следующие ситуации:

направление организацией здравоохранения персональных данных пациентов, работников в организации, расположенные в другой стране;

хранение файлов, содержащих персональные данные, на Google Диск, Яндекс Диск;

использование Viber и иных мессенджеров для передачи персональных данных;

передача персональных данных при зарубежных командировках и др.

Порядок трансграничной передачи персональных данных зависит от того, в какую страну передаются персональные данные:

на территории которой обеспечивается надлежащий уровень защиты прав субъектов персональных данных;

на территории которой не обеспечивается надлежащий уровень защиты прав субъектов персональных данных.

Перечень стран, на территории которых обеспечивается надлежащий уровень защиты прав субъектов персональных данных, определен Приказом № 14.

Справочно.

В перечень иностранных государств, на территории которых обеспечивается надлежащий уровень защиты прав субъектов персональных данных, включены иностранные государства, являющиеся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, принятой в г. Страсбурге 28 января 1981 года, а также иностранные государства, являющиеся членами Евразийского экономического союза.

Передача персональных данных на территорию таких государств осуществляется с соблюдением общих положений об обработке персональных данных (статьи 4, 6 и 8 Закона о защите персональных данных) без ограничений и необходимости получения каких-либо дополнительных разрешений.

В иные государства (например, США, Китай), по общему правилу, передача персональных данных запрещается, за исключением ситуаций, предусмотренных пунктом 1 статьи 9 Закона о защите персональных данных.

В частности, трансграничная передача персональных данных допускается в случаях, когда:

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

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, и др.

Так, например, операторы могут привлекать к обработке персональных данных уполномоченных лиц. Исходя из абзаца шестнадцатого статьи 1 Закона о защите персональных данных, наряду с государственными органами, юридическими лицами Республики Беларусь ими могут быть и иностранные организации, которые на основании договора с оператором осуществляют обработку персональных данных от имени оператора или в его интересах.

Факт осуществления трансграничной передачи персональных данных должен быть отражен в соответствии с принципом прозрачности (пункт 6 статьи 4 Закона о защите персональных данных) в документах, определяющих политику оператора в отношении обработки персональных данных. При этом если обработка персональных данных осуществляется на основании согласия, то информация о трансграничной передаче персональных данных дополнительно предоставляется субъекту до получения такого согласия.

Пример.

Получает широкое распространение использование организациями здравоохранения различных чат-ботов, например, Telegram-ботов. Учитывая, что сервера, на которых осуществляется обработка персональных данных посредством Telegram-ботов, находятся за пределами территории Республики Беларусь, такая обработка является трансграничной передачей персональных данных.

Следовательно, использование работниками учреждений здравоохранения Telegram-ботов при выполнении трудовых функций предполагает наличие у оператора соответствующего правового основания для трансграничной передачи.

Проведенный анализ законодательства не позволил установить правовых оснований для обработки персональных данных организацией здравоохранения посредством Telegram-ботов без согласия субъекта персональных данных.

В этой связи обработка персональных данных посредством Telegram-ботов допустима лишь с согласия субъекта персональных данных при условии, что субъект персональных данных проинформирован

о рисках, возникающих в связи с отсутствием надлежащего уровня их защиты (абзац второй пункта 1 статьи 9 Закона).

В отношении использования организацией здравоохранения информационных систем иностранного государства в целях организации обработки персональных данных полагаем возможным отметить следующее.

Необходимо учитывать положения пункта 2 Указа Президента Республики Беларусь от 1 февраля 2010 г. № 60 ”О мерах по совершенствованию использования национального сегмента сети Интернет“, согласно которому деятельность по оказанию услуг на территории Республики Беларусь с использованием информационных сетей, систем и ресурсов, имеющих подключение к сети Интернет, осуществляется юридическими лицами с использованием информационных сетей, систем и ресурсов национального сегмента сети Интернет, размещенных на территории Республики Беларусь и зарегистрированных в установленном порядке.

В соответствии с частью шестой статьи 37-6 Закона о здравоохранении организации здравоохранения являются поставщиками информации в централизованную информационную систему здравоохранения.

Постановлением Министерства здравоохранения Республики Беларусь от 31 июля 2021 г. № 91 утверждена Инструкция о порядке разработки, формирования, ведения, эксплуатации информационных систем, информационных ресурсов, баз (банков) данных и (или) реестров (регистров) в здравоохранении, входящих в состав централизованной информационной системы здравоохранения, требования к ним, порядке их взаимодействия с централизованной информационной системой здравоохранения.

Пунктом 6 данной Инструкции определены условия, которые должны соблюдаться при ведении и эксплуатации указанных информационных систем, в числе которых следующие:

информационная система располагается на серверах, расположенных на территории Республики Беларусь, и зарегистрирована в соответствии с законодательством об информации, информатизации и защите информации;

используются средства технической и криптографической защиты информации, имеющие сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь или положительное экспертное заключение по результатам государственной экспертизы, проводимой Оперативно-аналитическим центром при Президенте Республики Беларусь.

В этой связи переход организации на информационную систему иностранного государства, влекущий передачу персональных данных клиентов данной организации на территорию иностранного государства, противоречит подходам к формированию и ведению централизованной информационной системы здравоохранения, закрепленным в Законе о здравоохранении.

Таким образом, при оказании медицинских услуг организации здравоохранения должны использовать информационные сети, системы и ресурсы национального сегмента сети Интернет, размещенные на территории Республики Беларусь и зарегистрированные в установленном порядке. Правовые основания для переноса обработки персональных данных на информационные системы, расположенные на серверах в иностранном государстве, отсутствуют.

8. Проведение диспансеризации взрослого и детского населения

Общие положения о диспансеризации населения определены статьей 18-2 Закона о здравоохранении. Частью второй указанной статьи предусмотрено, что порядок проведения диспансеризации устанавливается Министерством здравоохранения, если иное не предусмотрено законодательными актами.

Так, согласно абзацу второму подпункта 10.2 пункта 10 Инструкции о порядке проведения диспансеризации взрослого и детского населения Республики Беларусь, утвержденной постановлением Министерства здравоохранения Республики Беларусь от 30 августа 2023 г. № 125, в ходе диспансеризации медицинские работники амбулаторно-поликлинических организаций и (или) иных организаций здравоохранения проводят анкетирование пациентов с оформлением анкеты выявления факторов риска развития неинфекционных заболеваний (далее – анкета).

В соответствии с пунктом 20 названной Инструкции оформление анкеты допускается в электронном виде.

Вместе с тем, при заполнении анкет в электронном виде следует учитывать положения части тринадцатой статьи 44 Закона о здравоохранении.

Законом Республики Беларусь от 29 июня 2023 г. № 273-З «Об изменении законов по вопросам трудовых отношений» Трудовой кодекс Республики Беларусь (далее – ТК) дополнен статьей 103-1, устанавливающей гарантии для работников при прохождении диспансеризации.

При этом, в соответствии с частью пятой статьи 103-1 ТК работники обязаны предоставлять нанимателю документы, подтверждающие прохождение ими диспансеризации, по форме, установленной

республиканским органом государственного управления, проводящим государственную политику в области здравоохранения, если это предусмотрено локальными правовыми актами.

В соответствии с пунктом 21 названной Инструкции по результатам диспансеризации при необходимости оформляется выписка из медицинских документов по форме и в порядке, установленным постановлением Министерства здравоохранения Республики Беларусь от 9 июля 2010 г. № 92.

Постановлением Министерства здравоохранения от 17 ноября 2023 г. № 173 «Об изменении постановления Министерства здравоохранения Республики Беларусь от 9 июля 2010 г. № 92» определены порядок заполнения формы выписки из медицинских документов для целей доведения факта прохождения диспансеризации.

В этой связи при выдаче выписки из медицинских документов, содержащей информацию о подтверждении прохождения диспансеризации, в графе «Выписка дана для предоставления» указывается место работы (учебы, службы).

В графе «Дополнительные медицинские сведения (результаты медицинских осмотров, обследований, сведения о профилактических прививках и прочее)» указывается «Проведена диспансеризация» с указанием даты ее проведения. При этом иные сведения, в том числе информация о перенесенных заболеваниях (иных анамнестических сведениях), результатах медицинских осмотров, обследований, сведения о профилактических прививках, диагнозе основного и сопутствующего заболевания, проведенном лечении и иная подобная информация не указываются.

9. Видеонаблюдение в организациях здравоохранения

При применении систем видеонаблюдения необходимо стремиться к минимизации возможных угроз правам и основным свободам пациентов, включая их право на неприкосновенность личной жизни.

В частности, в соответствии с пунктом 2 статьи 4 Закона о защите персональных данных обработка персональных данных должна быть соразмерна заявленным целям их обработки и обеспечивать на всех этапах такой обработки **справедливое соотношение интересов** всех заинтересованных лиц. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям их обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки (пункт 5 статьи 4 Закона).

9.1. Осуществление видеонаблюдения с целью обеспечения общественного порядка.

Отдельные камеры видеонаблюдения в организациях здравоохранения устанавливаются в силу прямых требований законодательных актов.

В частности, на основании абзаца третьего подпункта 12.2 пункта 12 Указа Президента Республики Беларусь от 28 ноября 2013 г. № 527 «О вопросах создания и применения системы видеонаблюдения в интересах обеспечения общественного порядка» Советом Министров Республики Беларусь определены критерии отнесения объектов к числу подлежащих обязательному оборудованию средствами системы видеонаблюдения за состоянием общественной безопасности.

Кроме того, в развитие Указа Президента Республики Беларусь от 25 мая 2017 г. № 187 «О республиканской системе мониторинга общественной безопасности» и постановления Совета Министров Республики Беларусь от 10 ноября 2017 г. № 841 постановлением Министерства внутренних дел Республики Беларусь от 9 сентября 2022 г. № 234 утвержден Регламент функционирования республиканской системы мониторинга общественной безопасности, приложением 4 к которому определен типовой перечень зон обзора и задач видеонаблюдения.

Справочно.

В организациях здравоохранения (центральные районные (городские) больницы, центральные районные (городские) поликлиники, республиканские научно-практические центры, аптеки 1-й и 2-й категории, а также аптеки с круглосуточным режимом работы) зоны обзора камерами видеонаблюдения включают проезды на территорию объекта, территорию перед входами (выходами) в здания, а также прилегающую к ним, зоны обнаружения и идентификации лиц людей на входах (выходах) в здания, территорию вестибюля (фойе), приемное отделение, территорию помещения (коридора) перед регистратурой и (или) кабинетом распределения в стационар, а также помещения для хранения наркотических средств, психотропных веществ, их прекурсоров.

Видеонаблюдение с целью обеспечения общественной безопасности осуществляется на основании абзаца двадцатого статьи 6 и абзаца семнадцатого пункта 2 статьи 8 Закона о защите персональных данных и не требует согласия субъектов персональных данных.

Размещение камер видеонаблюдения с данной целью в иных зонах обзора не согласуется с требованиями Закона о защите персональных данных.

9.2. Осуществление видеонаблюдения для защиты жизни, здоровья или иных жизненно важных интересов.

Данное основание, как упоминалось в подпункте .3.1.4 пункта 3 настоящих рекомендаций, применяется в очень редких ситуациях, если

есть прямая угроза жизни, например, при оказании неотложной медицинской помощи (когда лицо не в состоянии выразить согласие по причине болезненного, бессознательного состояния такого лица и т. п.), в гуманитарных целях (контроль эпидемий и их распространения и т.п.) или в чрезвычайных ситуациях гуманитарного характера (техногенные или природные катастрофы, стихийное бедствие и т. п.), в иных исключительных ситуациях.

Приведенное правовое основание может быть использовано при одновременном соблюдении двух условий:

обработка персональных данных необходима для целей защиты жизни, здоровья или иных жизненно важных интересов либо самого субъекта персональных данных, либо иных лиц;

получение согласия субъекта персональных данных на обработку персональных данных невозможно.

К таким ситуациям могут быть отнесены, например, нахождение человека в реанимационном отделении в состоянии, требующем постоянного наблюдения, или необходимость организовать дистанционную консультацию со специалистом, связаться с которым оперативно другим способом не представляется возможным. В последнем случае видеонаблюдение может включать аудиозапись.

Видеонаблюдение в изложенных ситуациях осуществляется на основании абзаца восемнадцатого статьи 6 и абзаца шестнадцатого пункта 2 статьи 8 Закона о защите персональных данных без согласия субъектов персональных данных.

В других случаях, требующих наблюдения за состоянием пациента с использованием системы видеонаблюдения, необходимо получить его согласие, если иное не следует из законодательного акта (включая случаи, когда законодательный акт содержит отсылочную норму об определении порядка реализации соответствующих обязанностей (полномочий) в ином нормативном правовом акте.

Справочно.

В частности, в соответствии с пунктом 56 Санитарных норм и правил «Требования к условиям труда медицинских работников, занятых в кабинетах магнитно-резонансной томографии», утвержденных постановлением Министерства здравоохранения Республики Беларусь от 21 января 2013 г. № 7, наблюдение за состоянием пациента проводится через смотровое окно пультовой или с помощью системы видеонаблюдения.

9.3. Осуществление видеонаблюдения в целях противодействия коррупции.

В отдельных случаях в организациях здравоохранения устанавливаются камеры видеонаблюдения, включая кабинеты врачей, в целях противодействия коррупции.

В соответствии с абзацем вторым части первой статьи 43 Закона Республики Беларусь от 15 июля 2015 г. № 305-З «О борьбе с коррупцией» руководители государственных органов и иных организаций в пределах своей компетенции обязаны принимать установленные данным Законом и иными актами законодательства меры, направленные на борьбу с коррупцией. Вместе с тем, установленные законодательством меры не предусматривают норм, напрямую обязывающих использовать для этого непосредственно системы видеонаблюдения.

С учетом требований статьи 4 Закона о защите персональных данных системы видеонаблюдения, если иное не предусмотрено законодательством, должны использоваться только в том случае, если эта цель не может быть достигнута другими средствами, предусматривающими меньшее вмешательство в права и свободы субъектов персональных данных, включая работников организаций здравоохранения и пациентов.

Гипотетические возможности совершения правонарушений коррупционного характера или их единичные случаи касаются любой сферы деятельности и не могут являться основанием для сплошного видеонаблюдения за всеми гражданами, в том числе находящимися в организации здравоохранения.

Кроме того, наличие камер видеонаблюдения само по себе не является препятствием для совершения правонарушений коррупционного характера для лиц, намеревающихся их совершить.

Таким образом, видеонаблюдение в целях противодействия коррупции в организациях здравоохранения может иметь место при наличии конкретных высоких рисков коррупционного характера, например, в кабинетах административно-управленческого персонала.

9.4. Осуществление видеонаблюдения с целью повышения качества оказания медицинской помощи.

Информация о видеонаблюдении в трудовых отношениях, в том числе на рабочих местах, содержится в пункте 7 Рекомендаций Национального центра защиты персональных данных об обработке персональных данных в связи с трудовой (служебной) деятельностью.

Так, по общему правилу, видеонаблюдение на рабочих местах допускается лишь при наличии специфических обстоятельств, требующих организации постоянного контроля на рабочем месте. Такое видеонаблюдение может иметь место, в частности, при работе с материальными ценностями или связанной с непрерывным обслуживанием клиентов.

Работа врача в большинстве случаев, действительно, связана с непрерывным приемом пациентов. Кроме того, в отдельных ситуациях видеозапись может являться единственным достоверным источником при

проведении экспертизы качества медицинской помощи, в том числе в рамках рассмотрения заявлений и жалоб на качество ее оказания. Осуществление такой экспертизы является элементом контроля за деятельностью организаций здравоохранения, направленного на повышение качества оказания медицинской помощи и защиту прав и законных интересов граждан, защиты работников здравоохранения от необоснованных жалоб на их действия.

Вместе с тем, необходимо учитывать, что такое видеонаблюдение обременено обработкой специальных персональных данных и персональных данных, входящих в состав врачебной тайны, а также иной информации о частной жизни физических лиц, включая сведения, составляющие личную и семейную тайну, защита которой в силу ее деликатности и уязвимости гарантируется Конституцией Республики Беларусь, Законом об информации, Законом о здравоохранении, Законом о защите персональных данных и иными законодательными актами.

Зачастую именно в кабинетах врачей пациенты при осуществлении их осмотра или медицинских манипуляций находятся в особо уязвимом состоянии (в обнаженном виде и т.п.).

При этом, как упоминалось, согласно части тринадцатой статьи 44 Закона о здравоохранении организации здравоохранения **при формировании информационных систем**, информационных ресурсов, баз (банков) данных, реестров (регистров) в здравоохранении **обязаны получать согласие** пациента на внесение и обработку его персональных данных, информации, составляющей врачебную тайну.

Справочно.

Система видеонаблюдения относится к информационным системам.

Обращаем внимание, что само по себе видеонаблюдение не включает в себя аудиомониторинг (запись голоса). Во время видеонаблюдения законодательством не предоставлено право прослушивать разговоры работников, пациентов и иных лиц, кроме исключительных ситуаций (таких как необходимость принятия мер безопасности и т.п.), о которых работники должны быть проинформированы.

Нереализация организацией здравоохранения надлежащим образом мер по обеспечению защиты персональных данных, в том числе по осуществлению технической и криптографической защиты персональных данных в порядке, установленном Оперативно-аналитическим центром при Президенте Республики Беларусь (абзац шестой пункта 3 статьи 17 Закона о защите персональных данных), создает дополнительные риски для прав субъектов персональных данных.

Таким образом, видеонаблюдение в кабинете врача, осуществляющего прием пациентов, возможно только с согласия пациентов, если иное не предусмотрено законодательным актом и (или) принятым в его развитие нормативным правовым актом.

II Меры по обеспечению защиты персональных данных

9. Назначение структурного подразделения или лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных

Организация внутреннего контроля за обработкой персональных данных оператором направлена на обеспечение соблюдения требований Закона о защите персональных данных, защиту интересов субъектов персональных данных и предотвращение возможных нарушений. Внедрение и эффективное функционирование института ответственного за осуществление внутреннего контроля способствует обеспечению безопасности и конфиденциальности персональных данных.

Организация здравоохранения, выступая оператором, должна в соответствии с абзацем вторым пункта 3 статьи 17 Закона о защите персональных данных назначить структурное подразделение или лицо, ответственное за осуществление внутреннего контроля за обработкой персональных данных.

В соответствии с квалификационной характеристикой специалист по внутреннему контролю за обработкой персональных данных должен иметь высшее образование.

Справочно.

Соответствующие функции лица, ответственного за осуществление внутреннего контроля, перечислены в Едином квалификационном справочнике должностей служащих (ЕКСД) «Должности служащих для всех видов деятельности», утвержденном постановлением Министерства труда Республики Беларусь от 30 декабря 1999 г. № 159, в который включена квалификационная характеристика специалиста по внутреннему контролю за обработкой персональных данных.

Вместе с тем, с учетом возлагаемых на данное лицо функций, такое лицо должно назначаться с учетом знания законодательства о персональных данных и практики его применения, а также **способности выполнять соответствующие функции**.

Вариантами реализации рассматриваемого требования являются следующие:

создать отдельное структурное подразделение. Такую модель, как правило, следует избирать крупным операторам, осуществляющим

масштабную обработку персональных данных, в том числе трансграничную передачу, и имеющим множество информационных ресурсов, содержащих персональные данные. В состав таких подразделений целесообразно включать не только юристов, но и лиц, имеющих техническое образование, в целях комплексного анализа бизнес-процессов, связанных с обработкой персональных данных;

назначить освобожденного работника. Условия реализации данной модели во многом схожи с условиями создания соответствующего структурного подразделения, при этом масштаб организации (масштаб обработки персональных данных) не такой значительный, что позволяет выполнять функции ответственного за контроль одному лицу;

возложить дополнительные функции на одного из работников. Для такого лица обработка персональных данных не должна быть основным видом деятельности, что призвано исключить потенциальный конфликт интересов. В связи с этим следует исключить назначение ответственного за осуществление внутреннего контроля из числа руководителей организации (их заместителей), а также структурных подразделений или работников, основные функции которых связаны с обработкой большого объема персональных данных (например, кадровые и бухгалтерские службы, структурные подразделения по обращениям граждан и т.п.);

возложение дополнительных функций на нескольких работников.

На практике, как правило, данная модель реализуется посредством возложения дополнительных функций на двух работников:

на одного (например, юрисконсульт) – в части организационных и правовых мер;

на другого (например, специалист по информационной безопасности) – в части реализации технических мер (мероприятий по осуществлению технической и криптографической защиты персональных данных).

При таком варианте требуется четкое распределение функций между указанными лицами, исключение дублирования в их деятельности. Кроме того, у назначенных работников также должна быть объективная возможность выполнять соответствующие функции с учетом уже имеющихся должностных обязанностей.

Одним из вариантов реализации рассматриваемого требования является возложение дополнительных функций на двух работников: на одного (например, специалиста с юридическим образованием) – в части организационных и правовых мер, на другого (например, специалист по информационной безопасности) – в части мер по технической и криптографической защите персональных данных.

В таком случае требуется четкое распределение функций между указанными лицами, исключение противоречий в их деятельности. При

этом у каждого назначенного работника должна быть объективная возможность выполнять соответствующие функции с учетом уже имеющихся должностных обязанностей.

Обращаем внимание, что в случаях, если оператор принимает решение о возложении дополнительных функций на работника, для такого лица обработка персональных данных не должна быть основным видом деятельности, чтобы исключить потенциальный конфликт интересов.

В целях надлежащего выполнения организацией возложенных Законом о защите персональных данных обязанностей рекомендуется обеспечить независимость ответственного за контроль посредством:

предоставления доступа к документам и информации, в том числе обрабатываемой в информационных системах (ресурсах) в объеме, необходимом для выполнения возложенных на него обязанностей;

организации непосредственной подчиненности руководителю организации или его заместителю.

Следует учитывать, что формальное выполнение этой меры по защите персональных данных (факт назначения) без реальной деятельности такого лица (проведения фактического контроля, ведения реестра обработок, консультирования иных работников и др.) в силу загруженности по основной должности не является надлежащим выполнением обязанности, предусмотренной абзацем вторым пункта 3 статьи 17 Закона о защите персональных данных, и служит основанием для привлечения юридического лица к административной ответственности согласно части 4 статьи 23.7 Кодекса Республики Беларусь об административных правонарушениях.

11. Издание документов, определяющих политику организации здравоохранения в отношении обработки персональных данных

Обработка персональных данных в организациях здравоохранения осуществляется в соответствии с документами, определяющим политику в отношении обработки персональных данных (далее – Политика). Разработка Политики относится к обязательным мерам организации здравоохранения по обеспечению защиты персональных данных.

На сайте Центра размещены рекомендации по составлению документа, определяющего политику оператора (уполномоченного лица) в отношении обработки персональных данных (https://cpd.by/pravovaya-osnova/metodologicheskiye-dokumenty-rekomendatsii/), а в рубрике Портфель оператора – примерные формы документов, которые следует принять оператору в целях реализации положений Закона о защите персональных данных (https://cpd.by/pravovaya-osnova/portfel-operatora/).

Кроме того, с учетом осуществляемой организациями здравоохранения масштабной обработки персональных данных необходимо провести «ревизию» всех бизнес-процессов в организации и рассмотреть вопрос о подготовке документов, определяющих политику в отношении обработки персональных данных, по отдельным направлениям деятельности (например, в отношении работников, клиентов (пациентов), пользователей интернет-сайта, видеонаблюдения, cookie-файлов и т.п.).

При работе над политикой следует учесть подходы, изложенные в Рекомендациях по составлению документа, определяющего политику оператора (уполномоченного лица) в отношении обработки персональных данных, которые разработаны Центром и размещены по адресу: https://cpd.by/rekomendacii-sostavlenie-politiki-obrabotki/.

Типичным нарушением при подготовке Политики является то, что в ней не отражены вовсе либо отражены только некоторые бизнес- и иные процессы, в ходе которых осуществляется обработка персональных данных пациентов в организации здравоохранения.

В этой связи представляется важным составление реестра обработки персональных данных, с учетом процессов, присущих каждому структурному подразделению организации здравоохранения, от поступления, например, в больницу, пациента до его выписки. Кроме того, в реестр необходимо также внести процессы предоставления организацией здравоохранения медицинской документации и биологических анализов с персональными данными пациентов другим организациям здравоохранения, связанные с организацией оказания медицинских помощи.

На операторе лежит обязанность обеспечить неограниченный доступ, в том числе с использованием глобальной компьютерной сети Интернет, к документам, определяющим политику оператора (уполномоченного лица) в отношении обработки персональных данных, до начала такой обработки.

Реализация указанного требования должна осуществляться с учетом круга субъектов персональных данных, на которых она распространяется. Так, Политика оператора в отношении ”внешнего контура“ (клиентов, контрагентов, граждан, направляющих обращения, и т.п.) размещается в сети Интернет на интернет-сайте оператора. Такая информация должна быть опубликована на странице не ниже второго уровня, а также дополнительно может размещаться на иных интернет-ресурсах или распространяться другими способами. При отсутствии у оператора (уполномоченного лица) сайта обеспечение неограниченного доступа к Политике осуществляется посредством ее размещения на информационных стендах или иными способами.

Иной подход может быть применен в отношении политики оператора в отношении работников. Такой документ нет необходимости размещать в открытом доступе для неограниченного круга лиц. В этом случае допустимо опубликовать соответствующий документ на корпоративном портале (при его наличии), и (или) на информационных стендах.

12. Ознакомление работников организации здравоохранения с положениями законодательства о персональных данных и внутренними документами, определяющими такую обработку, а также обучение персонала

Реализация рассматриваемой меры направлена на уяснение работниками организации здравоохранения сути возлагаемых на них обязанностей, связанных с обработкой персональных данных, и исключение ссылок на незнание как на оправдание допускаемых нарушений.

Данная обязанность распространяется на всех работников, в том числе и на вновь принимаемых.

Реализация этой меры включает в себя несколько самостоятельных мероприятий:

- *ознакомление с положениями законодательства о персональных данных, в том числе с требованиями по защите персональных данных, документами, определяющими политику оператора (уполномоченного лица) в отношении обработки персональных данных.*

Такое ознакомление не может быть простой отсылкой к Закону о защите персональных данных, размещенному на сайте или в сетевом ресурсе. Оно должно касаться тех положений актов законодательства, которые имеют отношение к функциям конкретного работника. Иными словами, ознакомление должно носить ”адресный“ характер, поскольку для разных категорий работников (например, для работников кадровой службы, врачей, среднего медицинского персонала) будут иметь значение различные институты законодательства.

Ознакомление осуществляется с:

положениями законодательства о персональных данных. Это Закон о защите персональных данных, иные акты, имеющие значение для выполнения функций конкретным работником. Например, для медицинских работников актуальными являются соответствующие положения Закона о здравоохранении и принятые в его развитие положения постановлений Совета Министров или Министерства здравоохранения, определяющие ключевые параметры обработки тех или иных

персональных данных. Кроме того, целесообразно доводить информацию о мерах ответственности, предусмотренных ТК, КоАП и УК;

требованиями по защите персональных данных. Это меры, предусмотренные статьей 17 Закона о защите персональных данных, а также иные меры, предусмотренные законодательством;

документами, определяющими политику оператора (уполномоченного лица) в отношении обработки персональных данных.

Порядок ознакомления (ознакомление под роспись и др.) определяет сам оператор (уполномоченное лицо);

➢ *обучение указанных работников и иных лиц в порядке, установленном законодательством.*

Само по себе ознакомление с информацией об обработке персональных данных может не дать желаемого результата как в силу различного образования у работников, так и в силу различных способностей людей самостоятельно воспринимать информацию.

В этой связи мера по ознакомлению с информацией об обработке персональных данных увязана Законом о защите персональных данных с требованием об организации обучения соответствующих лиц.

Подходы к такому обучению, в том числе, его периодичности, определены в подпункте 3.3 пункта 3 Указа № 422.

В соответствии с подпунктом 3.3 пункта 3 Указа № 422, операторы организуют не реже одного раза в пять лет прохождение обучения по вопросам защиты персональных данных.

Справочно.

Подпунктом 1.1 пункта 1 Приказа № 194 установлено, что в Национальном центре защиты персональных данных обучение по вопросам защиты персональных данных по образовательной программе повышения квалификации руководящих работников и специалистов проходят лица, ответственные за осуществление внутреннего контроля за обработкой персональных данных, выполняющие эти функции в организациях здравоохранения.

Кроме того, абзац седьмой подпункта 3.3 пункта 3 Указа № 422 обязывает организации здравоохранения предоставлять ежегодно не позднее 15 ноября сведения о лицах, ответственных за осуществление внутреннего контроля за обработкой персональных данных, а также лицах, непосредственно осуществляющих обработку персональных данных, которым необходимо пройти обучение в Центре.

В отличие от лиц, ответственных за внутренний контроль за обработкой персональных данных, для лиц, непосредственно осуществляющих обработку персональных данных, законодательно предусмотрена возможность проходить обучение как в Центре, так и в учреждениях образования, а также в иных организациях, которым предоставлено право реализации образовательной программы повышения

квалификации руководящих работников и специалистов, по образовательной программе повышения квалификации руководящих работников и специалистов, либо в других организациях по образовательной программе обучающих курсов (лекториев, тематических семинаров, практикумов, тренингов, офицерских курсов и иных видов обучающих курсов), либо у самого оператора (уполномоченного лица) путем изучения установленных требований в области защиты персональных данных и проверки им знаний по вопросам защиты персональных данных (в виде собеседования, опроса, тестирования и других форм контроля знаний).

Даже непреднамеренные нарушения законодательства о персональных данных могут иметь серьезные последствия как для работников, организаций здравоохранения, так и для граждан – субъектов персональных данных. Поэтому, при проведении обучения необходимо акцентировать внимание работников на их обязанностях при обработке персональных данных, запретах и ответственности, установленных законодательством.

После завершения обучения следует провести проверку уровня полученных знаний и навыков, а также оценить их применение в повседневной работе. Для этого могут быть использованы различные формы контроля, такие как собеседование, опрос, анкетирование, тестирование и другие подходящие методы.

Такой подход позволяет не только убедиться в получении знаний по соблюдению законодательства о персональных данных, но и минимизировать возможные негативные последствия.

Обучение упомянутых лиц можно возложить на лицо, осуществляющее внутренний контроль и прошедшее обучение непосредственно в Центре. Для этих целей в организации здравоохранения должен быть издан приказ руководителя организации об обучении лиц, непосредственно осуществляющих обработку персональных данных. В преамбуле приказа необходимо указать, что обучение таких лиц проводится на основании абзаца четвертого пункта 3 статьи 17 Закона о защите персональных данных и абзаца шестого подпункта 3.3 пункта 3 Указа № 422.

13. Установление порядка доступа к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе)

При разработке порядка доступа к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе), организации здравоохранения следует отразить различия в предоставлении такого

доступа к документам в информационных ресурсах и к документам в бумажном виде.

Доступ к персональным данным, отраженным в документах в бумажном виде, можно ограничить посредством организации мест их хранения.

Доступ к персональным данным, обрабатываемым в информационных ресурсах (системах), может быть ограничен посредством настроек программного обеспечения. При этом в зависимости от программного обеспечения доступ может значительно отличаться. Максимально возможные права закрепляются за администратором этого программного обеспечения.

Отсутствие такого порядка приводит к тому, что доступ к персональным данным имеют работники, должностные обязанности которых не связаны с обработкой персональных данных (например, обслуживающий персонал). При этом нецелесообразно осуществлять распределение доступа к персональным данным на поименной основе ввиду постоянного движения кадров.

Порядок доступа к персональным данным целесообразно закрепить в одном документе, но отдельные его положения могут быть детализированы в иных документах, в том числе положениях об информационных ресурсах (системах), о видеонаблюдении, о контроле управления доступом в помещения организации.

Важно подчеркнуть, что порядок доступа к персональным данным должен основываться на принципе предоставления минимально (объективно) необходимого уровня доступа к персональным данным исключительно в целях выполнения работниками своих должностных обязанностей, а уполномоченными лицами – обязательств, определенных договором, решением государственного органа или актом законодательства.

На практике может возникнуть необходимость предоставления временного доступа к персональным данным конкретному работнику (иному лицу), в частности, лицам, которые проходят практику в организациях здравоохранения либо оказывают консультационную помощь, сотрудникам кафедр учреждения высшего образования, которые находятся в организации здравоохранения. Механизм предоставления такого временного доступа также следует закрепить в порядке доступа к персональным данным.

14. Осуществление технической и криптографической защиты персональных данных

В качестве одной из обязательных мер по защите персональных данных абзацем шестым пункта 3 статьи 17 Закона о защите персональных данных предусмотрена необходимость осуществления 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.

Основу соответствующего правового регулирования составляет Закон об информации. Им предусматривается необходимость использования системы защиты информации, которая создается в порядке, определяемом ОАЦ.

Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» детализированы требования к собственникам (владельцам) информационных систем, обрабатывающим информацию, распространение и (или) предоставление которой ограничено. Например, закрепляется требование об использовании средств защиты информации, имеющих сертификат соответствия, выданный в национальной системе подтверждения соответствия. Кроме того, уточняется, что осуществлять мероприятия по технической защите информации должны ответственные работники (подразделения) собственника (владельца) информационной системы либо организации, имеющие лицензию на осуществление данной деятельности.

Конкретные технические требования к защите информации, в том числе и персональных данных, определяются Приказом № 66, которым утверждено Положение о технической и криптографической защите информации, распространение и (или) предоставление которой ограничено, не отнесенной в установленном порядке к государственным секретам.

После реализации таких мер проводится аттестация системы защиты информации, которая представляет из себя окончательную проверку корректности выполнения мероприятий по технической защите. Успешное прохождение данной проверки позволяет получить аттестат соответствия, срок действия которого составляет 5 лет.

Конкретные требования к технической и криптографической защите персональных данных при их обработке в информационных системах зависят от класса информационной системы.

Такая классификация, исходя из требований пункта 5 статьи 17 Закона о защите персональных данных, устанавливается уполномоченным органом по защите прав субъектов персональных данных. В развитие указанной нормы принят Приказ № 12. Данным приказом установлено, что информационные ресурсы (системы), содержащие персональные данные,

в целях определения предъявляемых к ним требований технической и криптографической защиты персональных данных подразделяются на информационные ресурсы (системы), содержащие:

общедоступные персональные данные;

специальные персональные данные (кроме биометрических и генетических персональных данных);

биометрические и генетические персональные данные;

персональные данные, не являющиеся общедоступными или специальными.

В этой связи организации здравоохранения необходимо обеспечить выполнение рассматриваемого требования.

СОГЛАСОВАНО

Министерство здравоохранения
Республики Беларусь