Елена ВОЛЬСКАЯ, МГМСУ им. А.И. Евдокимова, **Оксана АЛЕКСАНДРОВА,** МОНИКИ им. М. Владимирского

10.21518/1561–5936–2018–10-6-11

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ

Движение массивов персональных данных, обмен данными из разных баз – неизбежные процессы, которые со временем будут только активизироваться. При этом необходимо обеспечить права граждан на конфиденциальность, защиту персональных данных и неприкосновенность частной жизни. Особенно актуальны эти проблемы в сфере здравоохранения, ведь на повестке дня весьма деликатный вопрос – защита персональных данных пациентов как при оказании им медицинской помощи, так и в рамках медико-социальных проектов и научных исследований.

Ключевые слова:
персональные данные, данные о здоровье, неприкосновенность частной жизни, обработка данных, псевдонимизация, Федеральный закон о персональных данных, Регламент ЕС 2016/679 о защите персональных данных

Проблема защиты персональных данных (ПД) оказалась в центре внимания и в нашей стране, и за рубежом. Это редкое совпадение интересов неслучайно: обеспечение конфиденциальности ПД является оборотной стороной процессов информатизации, цифровизации, глобализации информационных потоков и обмена данными, формирования объемных массивов информации, непосредственно относящейся к гражданам, и их последующего многоцелевого использования. Накопление информационных массивов открывает перед специалистами – аналитиками, учеными, менеджерами – небывалые перспективы. В то же время в процессе обработки информационных ресурсов, включающих сведения о конкретных личностях и их частной жизни, в т. ч. данные о здоровье, эта информация должна быть защищена от несанкционированного доступа.

Государство повсеместно берет на себя функцию регулирования сферы обращения ПД. 2017–2018 гг. стали новым этапом развития государственного регулирования в данной сфере как в России, так и за рубежом.

SUMMARY

Keywords: *personal data, data concerning health, protection of natural persons, data processing, pseudonymisation, Federal law on personal data, General data protection Regulation*

The issues of protecting personal data while providing medical services to the patients and in the framework of medical and social projects and scientific research become topical in a highly evolved IT technologies in healthcare and medicine. The article discusses the main provisions of the federal law on personal data, as compared with the norms of the European General Data Protection Regulation GDPR.

Elena Volskaya, Evdokimov Moscow State University of Medicine and Stomatology
Oksana Aleksandrova, Vladimirsky Moscow Regional Research Clinical Institute
PROTECTING PERSONAL DATA RESPECTING PATIENTS' PRIVACY

РЕГУЛЯТОРНЫЕ НОРМЫ В ОБЛАСТИ ПД В РОССИИ И В ЕС

Закон, регулирующий общие вопросы информационной безопасности, был принят в нашей стране в 2006 г., с тех пор он неоднократно актуализировался, и теперь его название «федеральный закон "Об информации, информационных технологиях и о защите информации"» [1]. В ЕС эти задачи решает рамочный законодательный акт – Директива 2016/1148, направленная на обеспечение безопасности коммуникационных сетей и информационных систем [2].

Принятый в 2006 г. федеральный закон «О персональных данных» № 152-ФЗ (далее по тексту – закон № 152-ФЗ) имеет целью обеспечение защиты ПД граждан при их обработке [3]. Обращение с ПД при оказании гражданам медицинских услуг специально регулируется федеральным законом «Об основах охраны здоровья граждан в Российской Федерации» № 323-ФЗ [4]. Требование защиты ПД субъектов клинических исследований прописано в федеральном законе «Об обращении лекарственных средств» № 61-ФЗ [5] и в соответствующих подзаконных

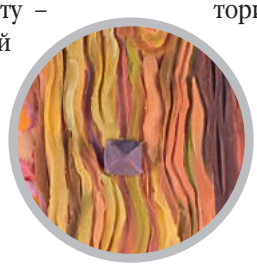
актах, например в приказе Минздрава России № 200н от 01.04.2016 г. [6].

С 01 июля 2017 г. вступили в силу изменения, внесенные в Кодекс об административных правонарушениях РФ (КоАП), которые ужесточили ответственность за нарушения законодательства в области ПД. Статья 13.11 КоАП получила новое название – «Нарушение законодательства Российской Федерации в области персональных данных» [7] (старое название – «Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)»). В настоящее время предусматривается семь составов правонарушений вместо одного, указанного в старой редакции, а размеры штрафов значительно увеличены для физических, должностных и юридических лиц (максимальный размер штрафа для них 75 тыс. руб.). Это свидетельствует о внимании законодателей к проблеме защиты ПД.

Регуляторы Европейского союза пошли похожим путем, выстроив иерархию нормативно-правовых актов: в 2016 г. Европарламент принял новый закон прямого действия – общий законодательный акт «Регламент № 2016/679 Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС» (далее по тексту – Регламент № 679) [8], который вступил в силу 25 мая 2018 г. Регламент № 679 устанавливает правила обработки ПД, общие для всех стран ЕС, и учитывает произошедшие в последние годы изменения в сфере компьютерных технологий, существенно повлиявшие на процесс не только обработки данных, но и их хранения. Этим актом существенно детализированы требования к организациям и лицам, работающим с ПД. Вопрос обеспечения конфиденциальности физических лиц отражен также в нормативных актах, посвященных медицинскому и социальному обеспечению на территории ЕС, например в Директиве 2011/24 Европарламента и Совета ЕС о правах пациентов при трансграничном медицинском обеспечении [9]. Защита ПД субъектов клинических исследований, соответственно, регулируется Регламентом № 536/2014 о клинических исследованиях ЛС [10].

Хотелось бы отметить, что действующее регулирование в сфере ПД в нашей стране и в ЕС очень сходно, регламентирующие требования вовсе не противоречат друг другу и отражают единые принципы обеспечения прав субъектов на защиту ПД и неприкосновенность личной сферы, т.е. частной жизни. При этом субъект ПД рассматривается как единственная персона, полномочная принимать решения в отношении личной информации (за исключением особых случаев, оговоренных законом).

Правда, степень детализации положений и требований в Регламенте № 679 более высокая, чем в законе № 152, в частности, это касается ПД о здоровье. Однако концептуальная близость регулирования является позитивным фактором, важным для взаимодействия операторов при выполнении международных проектов, связанных с ПД, на территории стран ЕС и России.



ПРИНЦИПЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Принципы защиты ПД при их обработке в целях обеспечения прав субъектов сформулированы как в законе № 152, так и в Регламенте № 679.

Одним из основных принципов является информированное добровольное согласие субъекта ПД на их обработку, которая может включать сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, предоставление доступа, обезличивание, блокировку, удаление, уничтожение, т.е. все действия и операции в отношении ПД с использованием средств автоматизации или без них.

При этом субъект ПД имеет право отозвать свое согласие на обработку в любой момент.

Законодательно установлены требования к защите ПД при их обработке:

обработка ПД должна осуществляться на законной основе;

содержание и объем обрабатываемых ПД должны соответствовать заявленным целям обработки;

обрабатываемые ПД не должны быть избыточными по отношению к заявленным целям их обработки.

В Регламенте № 679 даны краткие, но емкие формулировки этих принципов:

- «законность, беспристрастность и прозрачность»;
- «целевое ограничение» (сбор и обработка в соответствии с поставленной целью);
- «минимизация данных» (недопущение избыточного сбора данных, не соответствующих цели);
- «точность»;
- «ограничение по хранению» (сроки хранения оговариваются заранее);
- «целостность и конфиденциальность».

Еще одним принципом защиты ПД можно считать строгую ответственность юридического или физического лица, осуществляющего обработку ПД.

Российский закон № 152 вводит для этого лица термин «оператор ПД». В англоязычной версии Регламента № 679 это лицо названо контролером ПД. Однако определения сути этих терминов позволяют считать, что под ними подразумевается одно и то же *(табл.)*. К тому же в версиях Регламента № 679, опубликованных на других языках в официальных бюллетенях государств – членов ЕС, которые имеют равную силу, это же лицо называется и контролером,

и оператором, и просто ответственным лицом за обработку ПД.

Согласие субъекта на обработку ПД остается основным условием деятельности оператора/контролера, причем на него возлагается обязанность в случае необходимости подтвердить, что субъект данных дал свое добровольное информированное согласие на обработку его ПД.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ МЕДИЦИНСКОГО ХАРАКТЕРА

В Российской Федерации закон №152-ФЗ под ПД понимает любую информацию, относящуюся прямо или косвенно к определенному или определяемому физическому лицу.

Регламент №679 дает идентичное толкование данному термину, но раскрывает его содержание: персональные данные – любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу («субъект данных»), «идентифицируемое лицо – это лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством таких идентификаторов, как имя, идентификационный номер, сведения о местоположении, идентификатор в режиме онлайн, или через один или несколько признаков, характерных для физической, психологической, генетической, умственной, экономической, культурной или социальной идентичности указанного субъекта».

ПД медицинского характера представляют собой особую, чрезвычайно чувствительную для граждан категорию ПД. Поэтому организациям, осуществляющим сбор, обработку, а также использование ПД пациентов, предписывается особенно внимательно относиться к вопросу обеспечения конфиденциальности столь деликатной информации, тем более что федеральный закон №323-ФЗ требует от медицинских работников соблюдения врачебной (профессиональной) тайны в отношении любых данных о пациентах, их диагнозе, процессе лечения, результатах медицинских обследований и т. п.

Наше законодательство не содержит специального термина для таких данных. Регламент №679 вводит понятие «данные, относящиеся к здоровью» и определяет его как «персональные данные, касающиеся физического или психического здоровья физического лица, в т. ч. предоставления медицинских услуг, которые содержат информацию о состоянии его/ее здоровья»*, а также поясняет, что связанные со здоровьем ПД должны включать в себя все данные, которые относятся к состоянию здоровья субъекта и содержат информацию о прошлом, текущем и будущем физическом или психологическом состоянии субъекта данных. Сюда относится:

- информация о физическом лице, собранная при предоставлении медицинских услуг,
- номер, символ или знак, присвоенные физическому лицу для его однозначной идентификации в медицинских целях (например, номер страхового свидетельства),
- информация, полученная в результате исследования или обследования части тела или телесного материала, включая генетические данные и биологические образцы,
- любая информация, например о заболевании, инвалидности, риске заболевания, медицинском анамнезе, лечении или о физиологическом или медико-биологическом состоянии субъекта данных, независимо от источника данных.

Как и закон №152-ФЗ, Регламент №679 дает определение генетическим данным: это «персональные данные в отношении унаследованных или приобретенных характеристик физического лица, которые были получены в результате анализа биологического образца соответствующего лица, в частности в результате хромосомного анализа, анализа ДНК или РНК, или анализа иных элементов, позволяющего получить эквивалентную информацию».

Еще один законодательно введенный термин – «биометрические данные», он применяется в особых случаях, когда требуется на основании какой-либо информации с помощью специальных средств идентифицировать личность гражданина (например, при дактилоскопической экспертизе или по генетическим образцам при розыскной работе правоохранительных органов), однако это не относится к оказанию медицинской помощи или научным исследованиям.

ЧАСТНЫЙ СЛУЧАЙ ПД – БИООБРАЗЦЫ В БИОБАНКАХ

Биобанки, позволяющие хранить в течение многих лет в условиях низких температур коллекции биообразцов тканей, клеток, крови и других

ТАБЛИЦА Сходство в определении терминов

Закон «О персональных данных» №152-ФЗ	Регламент №679
Оператор – **государственный орган,** муниципальный орган, **юридическое или физическое лицо, самостоятельно или совместно с другими** лицами организующие и (или) осуществляющие обработку персональных данных, а также **определяющие цели обработки персональных данных**, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными	Контролер – **физическое или юридическое лицо, органы государственной власти,** агентство или иной орган, который **самостоятельно или совместно с другими определяет цели** и способы **обработки персональных данных**

* *Подстрочный перевод автора.*

жидкостей организма людей (пациентов), играют ключевую роль в развитии медицинской науки. Они являются источниками для исследования причин заболеваний и их маркеров, способствуют созданию новых способов диагностики и лечения.

В то же время биобанки можно рассматривать как собрания ПД пациентов, поскольку они содержат большие объемы информации об организме, заболевании и состоянии здоровья доноров биообразцов, особенно если биообразцы позволяют получить результаты генетических анализов, о чем прямо говорится в Регламенте № 679.

Соответственно, к биобанкам применимо законодательство о ПД, как российское, так и европейское, особенно в отношении защиты содержащихся в них ПД от несанкционированного доступа. В соответствии с Регламентом № 679, для биобанков следует описывать жизненный цикл хранящихся в них ПД с указанием длительности хранения и основания для хранения данных.

К теме биобанков близка проблематика больших данных (big data), которая в последнее время привлекает к себе пристальное внимание. С формированием массивов больших данных многие специалисты связывают надежды на серьезный прогресс медицины. На ресурсе Pubmed при поиске по ключевому слову «big data» в октябре 2018 г. было найдено 12 817 публикаций [11], что свидетельствует о том, что этой теме исследователи уделяют большое внимание.

Потенциал больших данных заключается не столько в сборе и хранении огромных массивов информации, сколько в возможностях их анализа. Речь идет об особых информационных технологиях, позволяющих с помощью специальных аналитических программ и алгоритмов получить ответы на вопросы, которые раньше даже не ставились ни в клинической практике, ни в научных исследованиях.

Однако при формировании массивов больших данных эксперты рекомендуют учитывать важные правовые аспекты [12].

Опыт работы с массивами больших данных показал, что сбор информации, произведенный без учета заранее сформулированной конкретной цели, не оправдывает себя, поскольку использованные аналитические алгоритмы без четкой постановки вопроса могут дать корреляции между группами данных, на самом деле независимых друг от друга. Возникает лишний, способный ввести в заблуждение «информационный шум». Очевидно, целесообразно говорить не столько о больших данных, сколько об «умных данных» (smart data). Для этого нужно иметь в массиве данные, необходимые для решения определенной проблемы или ответа на конкретный вопрос, т. е. решающее значение имеет не гигантский объем данных, а их качество с точки зрения поставленной цели. Целенаправленный поиск данных, важных для решения проблемы, соответствовал бы принципу «минимизации» (Регламент № 679) больше, чем метод накопления любых медицинских ПД. Для ответа на исследовательский вопрос следует собирать только те данные, которые необходимы. Термин «smart data» постепенно входит в обращение и применяется все чаще (5 432 результата поиска в pubmed в середине октября 2018 г.), в то время как «big data» стал уже привычным.

Однако возможности, связанные с аналитическими технологиями обработки больших данных, таят в себе потенциальный риск: в огромных массивах данных может оказаться легче идентифицировать отдельных пациентов, несмотря на широко применяемую методику псевдонимизации. Более того, есть сообщения о том, что при обработке больших массивов медицинских данных, содержащих различные сведения о конкретных пациентах, случается

кроме того...

Проект по изменению правила формирования лотов при госзакупках лекарств

Федеральная антимонопольная служба (ФАС) внесла в Правительство РФ проект постановления «О требованиях к формированию лотов при осуществлении закупок лекарственных препаратов для медицинского применения, являющихся объектом закупки для обеспечения государственных и муниципальных нужд». Документом предусматривается запрет на объединение в одном лоте поставки лекарственных препаратов и услуг по их хранению или отпуску, что препятствует участию в закупках предприятий, не обладающих лицензией на производство либо оптовые поставки ЛС. Документ без замечаний согласован Минфином и Минпромторгом РФ, а также получил положительное заключение по результатам антикоррупционной экспертизы Минюста РФ.

«Магнит» приобретает «СИА Групп»

Совет директоров ретейлера «Магнит» поддержал предложение менеджмента компании о приобретении фармдистрибьютора «СИА Групп». Одобренный проект является частью стратегии развития бизнес-направлений «Магнит косметик» и «Аптеки». Сумма сделки по покупке «СИА Групп» не должна превышать 5,7 млрд руб., средства будут выплачиваться в форме обыкновенных акций «Магнита» без права их продажи в течение трех лет после приобретения. «СИА Групп» входит в Marathon Group Александра Винокурова, которая стала акционером «Магнита» в мае 2018 г., выкупив 11,82% акций ретейлера у ВТБ. «Магнит» запустил пилотный проект собственной аптечной сети в 2017 г., по итогам первого полугодия 2018 г. в ней насчитывалось около 50 точек. В сентябре текущего года стало известно о покупке ретейлером 100% акций фармдистрибьютора «Фармасистемс».

идентификация (ре-идентификация) личности [13, 14].

Так, сочетания трех демографических признаков (пола, 5-значного почтового индекса домашнего адреса и даты рождения) оказалось достаточно, чтобы идентифицировать 87% американского населения [15].

Некоторые эксперты указывают, что в настоящее время в больших массивах медицинских данных обеспечить анонимность личности, если сведений о ней в массиве достаточно, очень сложно [16].

В этой ситуации единственный надежный выход из положения – получение, в соответствии с действующими требованиями, информированного согласия пациента на использование ПД в массивах больших данных.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ СУБЪЕКТОВ КЛИНИЧЕСКИХ ИССЛЕДОВАНИЙ

ПД субъектов клинических и других научных исследований подлежат особенно строгой защите. С одной стороны, это обусловлено их участием в проекте с целью в первую очередь способствовать прогрессу науки и лишь во вторую (и то далеко не всегда) – получить передовое лечение. С другой стороны, собранные в ходе исследования и зафиксированные в индивидуальных регистрационных картах (case report form) медицинские данные являются наиболее ценным материалом для спонсора проекта, т. к. служат доказательной базой регистрационного досье на лекарственный препарат. Поэтому спонсор не менее заинтересован в защите этих данных.

В Российской Федерации при проведении клинических исследований, спонсируемых зарубежными компаниями с намерением зарегистрировать исследуемый ЛП в ЕС, участникам исследования (CRO, медицинским организациям и независимым этическим комитетам) приходится учитывать требования европейского Регламента № 679, т. к. он предусматривает, что прописанные в нем требования по защите ПД должны применяться в отношении физических лиц вне зависимости от их гражданства или места жительства при обработке их ПД (п. 14 преамбулы). Несмотря на сходство принципов и способов защиты ПД, некоторые отличия в рассматриваемых документах все же имеются. Хотя они не принципиальные, а, скорее, чисто терминологические, при формальном включении в отечественный контент защиты субъектов исследований неизбежно возникают вопросы.

Обязательным условием сбора ПД медицинского характера в клинических исследованиях является защита кодами данных, с помощью которых можно идентифицировать личность. Закон № 152-ФЗ содержит на этот счет следующее положение: «Обработка персональных данных допускается в следующих случаях: ...9) обработка персональных данных осуществляется в статистических или иных исследовательских целях... при условии обязательного обезличивания персональных данных» (ст. 6).

Обезличивание ПД – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПД конкретному субъекту.

Регламент № 679 также содержит требования в отношении обработки ПД в целях научного исследования, в т. ч. проводимого в интересах общества в сфере здравоохранения. К таким проектам применяются специальные условия, в частности в отношении публикации или иного использования ПД, а именно: как и в российском законодательстве, требуется защита ПД посредством их псевдонимизации.

Под термином «псевдонимизация» Регламент № 679 понимает обработку ПД таким образом, что ПД не могут быть больше отнесены к определенному субъекту данных без использования дополнительной информации при условии, что дополнительная информация хранится отдельно и подлежит техническим и организационным мерам, гарантирующим, что ПД не могут быть отнесены к идентифицированному или идентифицируемому физическому лицу.

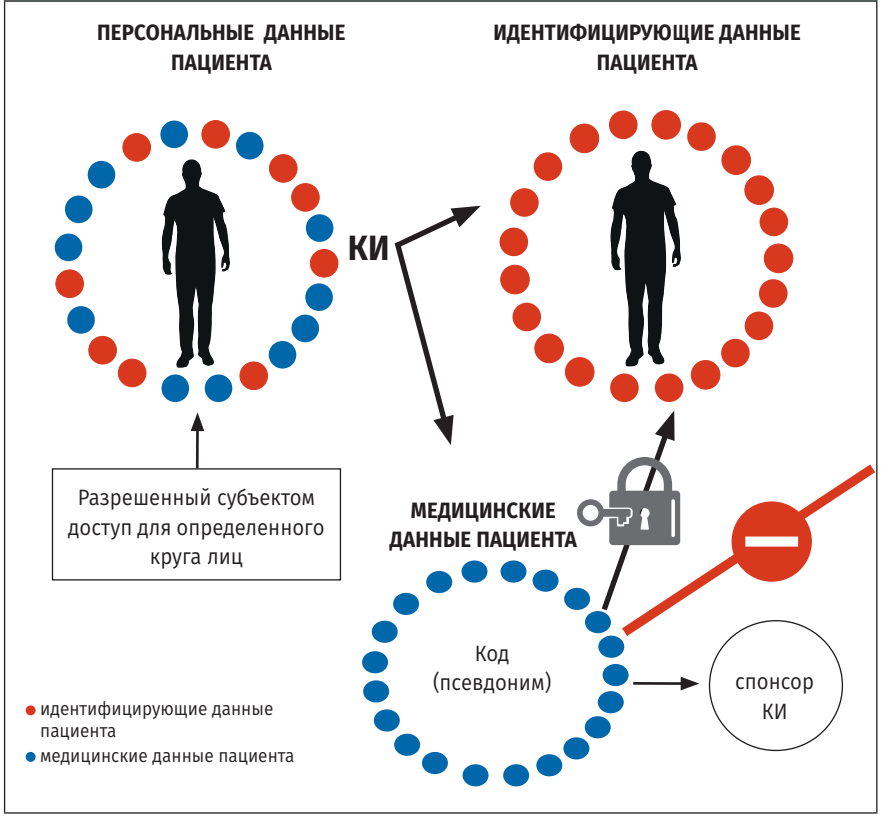
Непривычный термин, однако, не является новшеством: в российской нормативной базе имеется документ рекомендательного характера – ГОСТ Р 55036–2012 «Информатизация здоровья. Псевдонимизация» [17], предназначенный в т. ч. и для применения в области «клинических испытаний и пострегистрационного мониторинга побочных действий лекарственных препаратов».

В соответствии с определением указанного ГОСТа, являющегося авторизованным переводом стандарта ISO/TS 25237:2008, «Псевдонимизация (pseudonymization) – это особый случай обезличивания, при котором помимо удаления прямой связи с субъектом данных создается связь между конкретной совокупностью характеристик этого субъекта и одним или несколькими псевдонимами».

То есть если в случае обезличивания достигается замена идентифицирующих ПД пациента каким-либо кодом, так чтобы невозможно было без «ключа» идентифицировать его личность, то при псевдонимизации часть ПД, а именно данные медицинского характера, вносимые в CRF, под определенным псевдонимом (кодом) делаются доступными для обработки. Но эти данные связать с личностью субъекта возможно опять-таки только при наличии «ключа» *(рис.)*.

Однако в рамках клинических исследований возможен и прямой доступ к идентифицирующим данным субъекта КИ, содержащимся в оригинальных медицинских записях субъекта. Он может быть открыт для проверки процедур и/или данных клинического

РИСУНОК Схема защиты персональный данных субъектов клинических исследований



исследования определенному кругу сотрудников регуляторных органов (инспекторам), представителям спонсора (мониторам, аудиторам), членам этических комитетов. Все эти лица обязаны соблюдать конфиденциальность информации. Условием допуска является добровольное информированное согласие субъекта.

Таким образом, добровольное информированное согласие субъекта ПД является основным условием легальной обработки и использования принадлежащих личности сведений, включая биологическую (генетическую) информацию, полученную из биообразцов, во всех рассмотренных выше случаях.

ВМЕСТО ЗАКЛЮЧЕНИЯ

Защита ПД граждан в целом и пациентов в частности представляет собой сложную проблему, в которой переплетаются интересы общества, науки и ее представителей и отдельных личностей. В статье невозможно раскрыть все ее аспекты. Задачей авторов было сравнить основные регуляторные нормы, действующие в нашей стране и в европейских государствах, чтобы выявить общие тенденции в защите ПД и обеспечении права личности на конфиденциальность и увидеть различия в подходах. Как было показано, действующие в России и ЕС нормы вполне гармонично сочетаются.

ИСТОЧНИКИ

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/.
2. Directive (EU) 2016/1148 Of the European Parlament fnd of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri = CELEX:32016L1148&from = EN.
3. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (последняя редакция). URL: http://www.consultant.ru/document/cons_doc_LAW_61801/.
4. Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации». URL: https://www.rosminzdrav.ru/documents/7025.
5. Федеральный закон от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств» (с изменениями и дополнениями)/Система ГАРАНТ: http://base.garant.ru/12174909/#ixzz5VImikr00.
6. Приказ Минздрава России от 01.04.2016 г. № 200н «Об утверждении правил надлежащей клинической практики».
7. КоАП РФ. Статья 13.11. Источник: http://okoaprf.ru/st13.11.
8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) // Official Journal of the European Union, 4.5.2016.
9. Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri = CELEX:32011L0024&rid = 1.
10. Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC. URL: https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-1/reg_2014_536/reg_2014_536_en.pdf.
11. URL: https://www.ncbi.nlm.nih.gov/pubmed/?term = big+data, дата обращения 15 октября 2018 г.
12. Holger Koch et al. Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berueckschtigung der EU Datenschutz-Grundverordnung. – GMDS, 2017.
13. Franzosa et al. 2015. Identifying personal microbiomes using metagenomic codes. http://www.pnas.org/content/112/22/E2930.abstract.
14. Gymrek M, McGuire AL, Golan D, Halperin E, Erlich Y. Identifying Personal Genomes by Surname Inference. Science 2013, 339: 321ff.
15. Sweeney L. k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 2002. 10 (5): 557–570. http://dataprivacylab.org/dataprivacy/projects/kanonymity/kanonymity.pdf.
16. Tene O, Polonetsky J. Privacy in the Age of Big Data. Stanford Law Review. http://www.stanfordlawreview.org/online/privacy-paradox/big-data.
17. ГОСТ Р 55036–2012 «Информатизация здоровья. Псевдонимизация». URL: https://standartgost.ru/.