Ссылка для цитирования этой статьи:

Даниелян Т.А. Роль защиты конфиденциальной информации и персональных данных в контрактных исследовательских организациях (КИО) // Human Progress. 2023. Том 9, Вып. 1. С. 6. URL: http://progress-human.com/images/2023/Tom9_1/Danielyan.pdf, DOI 10.34709/IM.191.6. EDN XENCEQ.

УДК 004.056.5

РОЛЬ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И ПЕРСОНАЛЬНЫХ ДАННЫХ В КОНТРАКТНЫХ ИССЛЕДОВАТЕЛЬСКИХ ОРГАНИЗАЦИЯХ (КИО)

Даниелян Тамара Ашотовна
Магистрант
Финансовый университет при Правительстве Российской Федерации

tamara_danelyan@yahoo.com
55, Ленинградский просп.,
Москва, Россия, 127015
+7 (985) 190-38-77

Аннотация. Целью статьи является исследование регуляторов и политики защиты конфиденциальной информации и персональных данных в контрактной исследовательской организации. Производители фармацевтических препаратов, а также аутсорсинговые организации, оказывающие услуги в этой сфере, должны удовлетворять нормативным требованиям в области защиты конфиденциальной информации и персональных данных. Соответственно, фармацевтические производители, контрактные исследовательские организации разрабатывают, внедряют или совершенствуют элементы комплаенс в области защиты персональных данных и конфиденциальной информации. В данной статье мы рассматриваем общий регламент по защите данных (GDPR) как лучшую практику защиты конфиденциальной информации и персональных данных в контрактных исследовательских организациях, а также нормативные правовые акты и законы, регулирующие эту отрасль. В качестве объекта исследования проанализированы стандарты и политики по защите конфиденциальной информации и персональных данных, действующие в контрактной исследовательской организации. По результатам исследований, проведенных в настоящей работе, мы можем заключить, что внедрение и соблюдение политик и стандартов защиты данных, основанной на GDPR, помогает обеспечить ведение устойчивой деятельности организации и повысить безопасность персональных данных.

Ключевые слова: контрактная исследовательская организация; конфиденциальная информация; персональные данные; клинические испытания; политика по защите данных;

регламент по защите данных; безопасность данных; элементы комплаенс.

JEL коды: D82; C81.

Введение

Конфиденциальность личных данных не является новой концепцией, когда речь идет о здравоохранении. Право на неприкосновенность частной жизни не изменилось за более чем 130 лет. Несмотря на то, что средства защиты личной медицинской информации существовали десятилетиями, сегодняшние быстро растущие темпы внедрения технологий, появление нового программного обеспечения [1] и сложность потоков данных создали новый спрос на исследования процессов сбора данных пациентов и других участников клинических испытаний [2], их хранения и распределения между спонсорами, контрактной исследовательской организацией (contract research organization), внутренними и внешними заинтересованными сторонами. Поэтому важно понимать, как регулирование потока данных влияет на работу контрактной исследовательской организации.

В настоящей работе мы рассматриваем вопрос использования GDPR как основу комплаенса в сфере обеспечения сохранности данных.

Контрактная исследовательская организация (КИО) – это компания, которая предоставляет услуги по клиническим испытаниям для фармацевтической, биотехнологической и медицинской промышленности. Существуют различные типы КИО, типичные услуги КИО в отрасли медицинских устройств включают регистрацию препаратов, планирование клинических испытаний, поддержку набора персонала, клинический мониторинг, управление данными, логистику испытаний, формирование биостатистики и управление отраслевыми проектами. Организация нанимается спонсорами, которые хотят провести клиническое испытание. Ее найм устраняет необходимость во введении в штат сотрудников для завершения проекта и дает возможность работать с КИО в рамках проекта. КИО нанимается для планирования, координации, безопасного и эффективного выполнения и управления жизненным циклом клинического испытания. Она является связующим звеном между спонсором и другими заинтересованными сторонами на протяжении всего процесса клинических испытаний, контактирует с комитетами по этике и соответствию, регулирующими органами, поставщиками, врачами и координаторами исследований. Сотрудники контрактных исследовательских организаций должны обладать достаточными знаниями, компетенциями, быть в курсе процессов и процедур, которые необходимы для разработки и проведения успешного клинического испытания, обеспечивая при этом качество испытаний и соблюдение национальных и международных стандартов.

Конфиденциальность в контрактной исследовательской организации – это защита всех личных или клинически идентифицируемых данных, информации и записей, собираемых, используемых и поддерживаемых организацией. Этический долг конфиденциальности относится к обязанности физического лица или организации защищать доверенную информацию и предполагает наличие обязательств по защите информации от несанкционированного доступа, использования, раскрытия, изменения, потери или кражи. Выполнение этического долга конфиденциальности важно для доверительных отношений между исследователем и участником клинических испытаний (пациент), а также для целостности исследовательского проекта и, в конечном счете, для эффективности функционирования контрактной исследовательской компании.

Защита конфиденциальной информации и персональных данных в контрактных исследовательских организациях

Вовлечение клинических исследовательских организаций фармацевтическими и медицинскими компаниями для управления некоторыми проектами, связанными с клиническими испытаниями, становится все более актуальным, поскольку число глобальных клинических испытаний увеличивается каждый год, а соответствующая нормативная структура с клиническими испытаниями и последующим коммерческим развитием лекарств и медицинского оборудования становится более сложным. Международные клинические испытания особенно сложны для спонсоров. В таких случаях аутсорсинг клинических исследований у организации с местным опытом может снизить общие затраты для спонсоров и способствовать выполнению испытаний эффективным образом и в короткие сроки. Сотрудники КИО, специализирующиеся на службах поддержки клинических испытаний, обладают глубокими знаниями и опытом в применимых юрисдикциях, где организации предлагают свои услуги. КИО способствуют облегчению коммерциализации продуктов при более низких общих затратах на основе ускоренных регулирующих нормативов.

В то время как многие компании поддерживают идею большей прозрачности данных, спонсоры также борются с тем, чтобы удалить идентификаторы пациентов, сделать данные приемлемыми и совместимыми. В отрасли по-прежнему не хватает опыта в области анонимизации данных. Стремясь защитить данные и информацию граждан, ЕС принял Общий регламент по защите данных (GDPR), который вступил в силу в мае 2018 года. Конечно, данные о здоровье попадают в эту категорию. Данные клинических испытаний считаются конфиденциальными персональными данными, поэтому GDPR требует более жестких условий обработки данных по сравнению с требованиями других стран [3]. Что

касается клинических испытаний, спонсоры должны будут изучить процесс, где они получают согласие пациента, и также провести оценку воздействия рисков на защиту данных. В компаниях, где собирают личные данные и позволяют более чем одному сотруднику их обрабатывать, рекомендуется поддерживать соответствующую политику по защите данных (data protection policy)[1] [4]. Можно предположить, что это относится только к компаниям, расположенным в странах Европейского Союза, но это не так. Любая компания, которая получает данные от европейского резидента, должна будет соблюдать требования положения о защите данных (General data protection regulation- GDPR[2]). Даже если компания базируется на территории страны, не входящей в ЕС, и соблюдает свое законодательство, но в режиме онлайн оказывает услуги гражданам из ЕС, эта компания обязана соблюдать GDPR. Общее регулирование защиты данных (GDPR) по способу их обработки в разных отраслевых секторах различны. Есть особенности и у требований к клиническим исследованиям. Целью GDPR является усиление и стандартизация защиты личных данных. GDPR определяет две функции с данными.

1. Контроллеры данных определяют цели и средства обработки личных данных. Юридически большинство обязательств в GDPR падает на контроллеров.

2. Обработчики данных обрабатывают персональные данные, действуя по инструкции контроллера данных.

В то время как обработчики данных имеют меньше обязательств, чем контроллеры данных в рамках GDPR, на практике такие организации, как КИО, реализующие функции обработки данных, выполняют некоторые из обязательств контроллеров данных, поскольку они обрабатывают персональные данные. В контексте клинических испытаний правила GDPR распространяются не только на тех участников, которые участвуют в исследованиях, но и на сотрудников исследовательских организаций, клиентов и контрагентов. В соответствии с GDPR, КИО и другие поставщики клинических испытаний являются как обработчиками данных, так и контроллерами данных. С точки зрения участников исследования, КИО является процессором данных. По отношению к собственному персоналу, КИО является контроллером данных. Соответственно, существует несколько вопросов GDPR, на которые КИО должны ориентироваться.

[1] IMPACT-data-protection-policy_EN_2019_EN_v1.1.pdf (impact-initiatives.org) (дата обращения 23.10.2021)
[2] EU General Data Protection Regulation (GDPR) (gdprinfo.eu) (дата обращения 24.10.2021)

КИО должны разработать политику системы управления информацией о конфиденциальности (Privacy information management system- ISO 27701:2019[3]), основанной на GDPR, которая содержит следующие принципы конфиденциальности:

- согласие и выбор;
- легитимность и конкретизация цели;
- ограничение сбора;
- минимизация данных;
- использование, хранение и раскрытие информации;
- точность и качество;
- открытость, прозрачность и уведомление;
- индивидуальное участие и доступ;
- подотчетность;
- информационная безопасность;
- соблюдение конфиденциальности.

Сказанное позволяет заключить, что соблюдение GDPR в клиническом исследовании будет способствовать коммерциализации продуктов и минимизировать риски нарушения защиты персональных данных, что в свою очередь позволит избежать больших штрафов.

В России в 2006 г., был принят закон, регулирующий общие вопросы информационной безопасности. С тех пор он неоднократно актуализировался и теперь это федеральный закон «Об информации, информационных технологиях и о защите информации»[4]. В ЕС эти задачи решает рамочный законодательный акт – Директива 2016/1148, направленная на обеспечение безопасности коммуникационных сетей и информационных систем[5].

Принятый в 2006 г. федеральный закон «О персональных данных» №152-ФЗ (далее по тексту – закон №152-ФЗ) имеет целью обеспечение защиты персональных данных граждан при их обработке[6]. Обращение с персональными данными при оказании гражданам медицинских услуг специально регулируется федеральным законом «Об основах охраны

[3] ISO - ISO/IEC 27701:2019 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines (дата обращения 03.02.2023)

4 Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ. /Federal Law No 149-FZ “On Information, Information Technologies and Information Protection” dated July 27, 2006 URL: http://www.consultant.ru/document/cons_doc_LAW_61798/(дата обращения 24.10.2021)

5 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 in the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN (дата обращения 24.11.2022)

6 Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция). URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ Federal Law No. 152-FZ “On Personal Data” dated July 27, 2006 (last revision). URL: http://www.consultant.ru/document/cons_doc_LAW_61801(дата обращения 24.11.2022)

здоровья граждан в Российской Федерации» №323-ФЗ[7]. Требование защиты персональных данных субъектов клинических исследований содержится в федеральном законе «Об обращении лекарственных средств» №61-ФЗ[8] и в соответствующих подзаконных актах, например в приказе Минздрава России №200н от 01.04.2016 г.[9].
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 персональных данных. Статья 13.11 КоАП получила новое название – «Нарушение законодательства Российской Федерации в области персональных данных» (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 персональных данных. Безопасное хранение данных человека с соответствующим уровнем анонимности, конфиденциальности или деидентификации является ключевым фактором в обеспечении низкого порога риска для участников, исследователей и организации [5]. Сегодня спонсоры должны иметь возможность легко и быстро публиковать данные своих клинических испытаний, соблюдая при этом правила конфиденциальности и прозрачности данных [6]. В государствах, где регистрируются медицинские лекарства и препараты, предпринимаются шаги, чтобы повысить прозрачность клинических испытаний, качество исследований и безопасность пациентов. Однако в то же время нормативные акты теперь направлены на защиту персональных данных граждан, включая идентификаторы пациентов [3; 7]. В соответствии с ч.2 ст. 43 Федерального закона от 12.04.2010 № 61-ФЗ «Об обращении лекарственных средств», пациент или его законный представитель должен быть информирован в письменной форме, в том числе: «о гарантиях конфиденциальности участия пациента в клиническом исследовании лекарственного препарата для медицинского

7 Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации». URL: https://www.rosminzdrav.ru/documents/7025 /Federal Law No. 323-FZ “On the Fundamentals of Citizens' Health Protection in the Russian Federation” dated November 21. 2011 URL: https://www.rosminzdrav.ru/documents/7025 (дата обращения 20.11.2022)
8 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/ Federal Law No. 61-FZ “On Circulation of Medicinal Products” (with amendments and additions) dated 12 April 2010 GARANT system: http://base.garant.ru/12174909/#ixzz5VImikr00 (дата обращения 25.11.2022)
9 Приказ Минздрава России от 01.04.2016 г. № 200н «Об утверждении правил надлежащей клинической практики». /Order of the Ministry of Health of Russia No. 200n “On Approval of Good Clinical Practice” dated April 01. 2016 (дата обращения 24.11.2022)

применения». Основное содержание регламентов указанных нормативных актов представлено в GDPR. В частности, это касается согласия на обработку персональных данных. Обработка персональных данных, как правило, запрещена, за исключением случаев, когда это прямо разрешено законом или если субъект данных дал согласие на обработку. [8] Однако согласие является одним из наиболее известных правовых оснований для обработки персональных данных, оно является лишь одним из шести оснований, упомянутых в Общем регламенте по защите данных (GDPR). Законные основания для обработки персональных данных изложены в статье 6 GDPR[10]:

−согласие физического лица: в фармацевтической отрасли согласие может быть дано субъектом устно или в письменной форме;

−исполнение контракта: после подписания договора личные данные субъекта обрабатываются точно в соответствии с условиями, изложенными в договоре;

−соблюдение юридического обязательства: закон может потребовать от компании обработки персональных данных для определенной цели;

−необходимость защиты жизненно важных интересов человека: жизненно важные интересы могут быть законной причиной крупномасштабной обработки данных в гуманитарных целях, таких как мониторинг инфекционных заболеваний или обследование и защита населения во время национальных бедствий;

−необходимость выполнения задачи в общественных интересах: в рамках общественного интереса − это обработка данных о состоянии здоровья, если «обработка необходима по соображениям общественного интереса для обеспечения высоких стандартов качества и безопасности медицинской помощи, лекарственных средств или медицинских изделий;

−соблюдение законных интересов компании: в рамках "законного интереса" компания обрабатывает персональные данные в целях прямого маркетинга, для предотвращения мошенничества или для обеспечения сетевой и информационной безопасности ИТ-систем. [9]

Кроме того, GDPR вводит понятие «уведомление». Уведомление о конфиденциальности обычно требуется для любой законной обработки персональных данных в соответствии с GDPR, если законным основанием для такой обработки не является согласие субъекта данных. Некоторыми примерами уведомлений, которые могут быть использованы организацией, являются формы согласия, политики конфиденциальности,

[10] https://gdpr.eu/article-6-how-to-process-personal-data-legally/?cn-reloaded=1 (дата обращения 15.12.2022)

всплывающие окна с файлами cookie на веб-сайтах, контракты и лицензионные соглашения с конечными пользователями.

Также в соответствии с GDPR физические лица могут отправить запрос на доступ данным, чтобы воспользоваться своими правами и выбрать способ их обработки. Например, они могут попросить:

– доступ к копии персональных данных, которые хранятся в компании;

– удалить персональные данные, когда компании уже не нужны личные данные субъекта;

– запрещать использование их персональных данных;

– ограничить обработку своих персональных данных.

Заключение

Таким образом, клинической исследовательской организации обязательно нужно проверить свои политики уведомлений и разрешений, чтобы увидеть, что лучше всего подходит для обработки данных субъектов, участвующих в клинических исследованиях. Любые идентификаторы, которые могут использоваться в комбинации для идентификации человека, считаются персональными данными [10]. Когда речь идет о защите персональных данных, очень важно понимать, какие категории персональных данных обрабатываются на законных основаниях и как их защитить.

Литература

1. Gambarelli, G.; Gangemi, A.; Tripodi, R. Is Your Model Sensitive? SPEDAC: A New Resource for the Automatic Classification of Sensitive Personal Data // IEEE Access. 2023. Том 11. С.: 10864-10880.

2. Чайка, В.К.; Вустенко, В.В.; Морозова, Н.А. О рисках цифровизации здравоохранения // Медико-социальные проблемы семьи. 2022. Том 27. № 4. С.: 64-74.

3. Chassang, G.; et al. The impact of the EU general data protection regulation on scientific research. 2017.

4. Zhang, D. Big data security and privacy protection / 8th international conference on management and computer science (ICMCS 2018). Atlantis Press, 2018. С.: 275-278.

5. Regulation, P. General data protection regulation // Intouch. 2018. Том 25. С.: 1-5.

6. Баишев, Н.П. К вопросу о государственно-правовом регулировании защиты персональных данных в медицине // Ростовский научный вестник. 2021. № 2. С.: 9-11.

7. Romanosky, S.; Acquisti, A. Privacy costs and personal data protection: Economic and legal perspectives // Berkeley Tech. LJ. 2009. Том 24. С.: 1061.
8. Аверченков, В.И. Защита персональных данных в организации. М.: Флинта. 2016. С.:17-20.
9. Бабаш, А.В.; Баранова, Е.К.; Мельников, Ю.Н. Информационная безопасность. Учебное пособие. М.: КноРус. 2018. С.: 10-15.
10. Пономарева, О.Н. Особенности защиты персональных данных в медицине // Вестник УГМУ. 2020. № 4. С.: 53-54.

THE ROLE OF CONFIDENTIAL INFORMATION AND PERSONAL DATA PROTECTION IN CONTRACT RESEARCH ORGANIZATIONS (CROs)

Tamara Danielyan

Master student of Financial University under the Government of the Russian Federation

Moscow, Russia

Abstract. The aim of the article is to study the regulations and policies for the protection of confidential information and personal data in a contract research organization. Pharmaceutical manufacturers, as well as outsourcing organizations providing services in this area, are subject to extensive regulatory requirements in the field of confidential information and personal data protection. Accordingly, pharmaceutical manufacturers, contract research organizations develop, implement or refine compliance elements that address areas of potential problems or high risk and are applicable to their own companies. In this article, we review the General Data Protection Regulation (GDPR) as the best practice for protecting confidential information and personal data in contract research organizations, as well as laws that regulate this industry. As an object, the standards and policies on confidential information and personal data in force have been analysed. Having conducted the research, we can conclude that the implementation and compliance with GDPR-based data protection policies and standards helps to solve the following issues: maintaining the sustainable companies' operation and improving the patient data security.

Keywords: contract research organization; confidential information; personal data; clinical trials; data protection policy; data protection regulation; data security; compliance elements.

JEL codes: D82; C81.

References

1. Gambarelli, G.; Gangemi, A.; Tripodi, R. (2023) Is Your Model Sensitive? SPEDAC: A New Resource for the Automatic Classification of Sensitive Personal Data // IEEE Access. Vol. 11. P.: 10864-10880.

2. Chaika, V.K.; Vustenko, V.V.; Morozova, N.A. (2022) On the risks of digitalization of healthcare // Medico-social problems of the family. Vol. 27. No. 4. P.: 64-74.

3. Chassang, G.; et al. (2017) The impact of the EU general data protection regulation on scientific research.

4. Zhang, D. (2018) Big data security and privacy protection / 8th international conference on management and computer science (ICMCS 2018). Atlantis Press. P.: 275-278.

5. Regulation, P. (2018) General data protection regulation // Intouch. Vol. 25. P.: 1-5.

6. Baishev, N.P. (2021) On the issue of state-legal regulation of the protection of personal data in medicine // Rostov Scientific Bulletin. No. 2. P.: 9-11.

7 Romanosky, S.; Acquisti, A. (2009) Privacy costs and personal data protection: Economic and legal perspectives // Berkeley Tech. L.J. Vol. 24. P.: 1061.

8. Averchenkov, V.I. (2016) Protection of personal data in the organization. M.: Flinta. P.: 17-20.

9. Babash, A.V.; Baranova, E.K.; Melnikov, Yu.N. (2018) Information Security. Tutorial. Moscow: KnoRus. P.: 10-15.

10. Ponomareva, O.N. (2020) Features of personal data protection in medicine // Vestnik USMU. No. 4. P.: 53-54.

Contact

Tamara Danielyan
Financial University under the Government of the Russian Federation
55, Leningradsky Ave., 127015, Moscow, Russia
tamara_danelyan@yahoo.com