Всемирная организация здравоохранения
Европейское региональное бюро

Защита персональных данных в информационных системах здравоохранения: принципы и процедуры, применяемые в сфере охраны общественного здоровья

Всемирная организация здравоохранения
Европейское региональное бюро

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ЗДРАВООХРАНЕНИЯ: ПРИНЦИПЫ И ПРОЦЕДУРЫ, ПРИМЕНЯЕМЫЕ В СФЕРЕ ОХРАНЫ ОБЩЕСТВЕННОГО ЗДОРОВЬЯ

Резюме

В последние годы во многих странах Европы вводятся новые или значительно ужесточаются существующие законы о защите данных и кибербезопасности. Эти законы продолжают оказывать существенное влияние на информационные системы здравоохранения (ИСЗ) и большинство видов деятельности в сфере общественного здравоохранения в более широком смысле. Цель настоящего документа – проанализировать воздействие этой концепции и предложить несколько рекомендаций относительно методов принятия конкретных решений, необходимых для нахождения равновесия между затронутыми правами и интересами.

С помощью нескольких простых для реализации мер любая организация общественного здравоохранения может значительно повысить свой уровень соблюдения требований к защите данных. Поскольку опорные принципы защиты данных менялись с течением времени, в разделе 2 приводится краткий обзор истории вопроса, после чего авторы проводят глубокий анализ правовых принципов защиты данных. В разделе 3 описывается практическое применение этих принципов и обсуждаются права субъектов данных, поскольку именно их интересы призвана защищать нормативная база. В разделе 4 рассматриваются элементы, которыми не следует пренебрегать в пользу прав субъектов данных, в том числе право на здоровье и общественное здоровье в целом. В разделе 5 авторы вновь обращаются к вопросам вторичного использования данных в целях общественного здравоохранения и способам нахождения равновесия затрагиваемых интересов в этом контексте. Наконец, в разделе 6 приводится обзор мер, которые необходимо предпринять для достижения подобного равновесия, включая создание механизмов надзора и расширения прав и возможностей.

Настоящее руководство подготовлено в рамках работы Европейского регионального бюро ВОЗ по содействию государствам-членам в укреплении их информационных систем здравоохранения (ИСЗ). Оказание странам помощи в подготовке качественной информации по вопросам здравоохранения и создании институциональных механизмов для разработки политики с учетом фактических данных, традиционно относится к приоритетным направлениям работы ВОЗ и остается таковым в рамках Европейской программы работы на 2020–2025 гг.

Ключевые слова
HEALTH INFORMATION SYSTEMS; DATA PROTECTION; DATA SECURITY; COMPUTER SECURITY.

Номер документа: WHO/EURO:2021-1994-41749-58517

Образец библиографической ссылки. Защита персональных данных в информационных системах здравоохранения: принципы и процедуры, применяемые в сфере охраны общественного здоровья. Копенгаген: Европейское региональное бюро ВОЗ; 2020. Лицензия: CC BY-NC-SA 3.0 IGO.

Данные каталогизации перед публикацией (CIP). Данные CIP доступны по ссылке: http://apps.who.int/iris.

Содержание

Выражение признательности

Настоящий документ был разработан подразделением по вопросам данных, показателей и аналитики Отдела страновых стратегий и систем здравоохранения Европейского регионального бюро ВОЗ. Основным автором является Tobias Schulte in den Baeumen. Marieke Verschuuren и David Novillo Ortiz руководили процессом подготовки доклада и предоставляли технические консультации при разработке концепции, написании и рецензировании документа. Особая благодарность выражается Natasha Azzopardi-Muscat за ее стратегическое руководство.

Для получения дополнительной информации свяжитесь с подразделением по вопросам данных, показателей и аналитики (euhiudata@who.int).

Цель настоящего руководства

Настоящее руководство подготовлено в рамках работы Европейского регионального бюро ВОЗ по содействию государствам-членам в укреплении их информационных систем здравоохранения (ИСЗ). Оказание странам помощи в подготовке качественной информации по вопросам здравоохранения и создании институциональных механизмов для разработки политики с учетом фактических данных, традиционно относится к приоритетным направлениям работы ВОЗ и остается таковым в рамках Европейской программы работы на 2020–2025 гг.[1]

Одним из инструментов, используемых ВОЗ в этой работе, являются оценки ИСЗ. После проведения этих оценок был сделан общий для всех государств-членов Европейского региона ВОЗ вывод о наличии проблем с формированием статистики в сфере здравоохранения, вызванных тем, что существующий инструментарий механизмов защиты данных не позволяет использовать вторичные данные в статистических и исследовательских целях. В связи с этим ВОЗ разработала настоящее руководство как составную часть набора инструментов по укреплению потенциала ИСЗ.

1 Европейская программа работы. В: ЕРБ ВОЗ [веб-сайт]. Копенгаген: Европейское региональное бюро ВОЗ; 2020 (https://www.euro.who.int/ru/health-topics/health-policy/european-programme-of-work/about-the-european-programme-of-work).
Все ссылки приведены по состоянию на 5 февраля 2021 г.

Сокращения

ОВЗД	оценка воздействия на защиту данных
ЕС	Европейский союз
GDPR	Общий регламент по защите данных
ИСЗ	информационная система здравоохранения
ISO	Международная организация по стандартизации
ИТ	информационные технологии

1. Введение и цели

В последние годы во многих странах Европы вводятся новые или значительно ужесточаются существующие законы о защите данных и кибербезопасности. Эти законы продолжают оказывать существенное влияние на информационные системы здравоохранения (ИСЗ) и большинство видов деятельности в сфере общественного здравоохранения в более широком смысле. В то время как необходимость защиты данных – или, точнее, основополагающее право, лежащее в основе концепции защиты данных, – становится общепризнанным постулатом, следует понимать, что это право не является абсолютным и не должно препятствовать осуществлению других основополагающих прав и общественных интересов, включая право на здоровье. Цель настоящего документа – проанализировать воздействие этой концепции и предложить несколько рекомендаций относительно методов принятия конкретных решений, необходимых для нахождения равновесия между затронутыми правами и интересами.

Даже с учетом того, что главное намерение авторов – предоставить читателю готовые к применению рекомендации, они считают весьма важным сначала ознакомить его с понятиями и принципами концепции защиты данных. Следует отметить, что эффективная защита данных не представляет собой нечто недостижимое: она требует четко определенных действий, которые осуществимы как при разработке, так и при внедрении системы управления информацией здравоохранения. Аналогичным образом соблюдение требований в области защиты данных не требует особых затрат ни с точки зрения людских ресурсов, ни в контексте финансовых вложений в технологии. С помощью нескольких простых для реализации мер любая организация общественного здравоохранения может значительно повысить свой уровень соблюдения требований к защите данных. Цель настоящего руководства заключается в том, чтобы сформировать у читателя некоторое представление о практических методах защиты данных.

Поскольку опорные принципы защиты данных менялись с течением времени, в разделе 2 приводится краткий обзор истории вопроса, после чего авторы проводят глубокий анализ правовых принципов защиты данных. В разделе 3 описывается практическое применение этих принципов и обсуждаются права субъектов данных, поскольку именно их интересы призвана защищать нормативная база. В разделе 4 рассматриваются элементы, которыми не следует пренебрегать в пользу прав субъектов данных, в том числе право на здоровье и общественное здоровье в целом. В то время как общественное здравоохранение в целом занимает привилегированное положение, с точки зрения безопасности информационных технологий (ИТ) оно, очевидно, обязано подчиняться тем же стандартам, что и любая другая область деятельности. В разделе 5 авторы вновь обращаются к вопросам вторичного использования данных в целях общественного здравоохранения и способам нахождения равновесия затрагиваемых интересов в этом контексте. Наконец, в разделе 6 приводится обзор мер, которые необходимо предпринять для достижения подобного равновесия, включая создание механизмов надзора и расширения прав и возможностей.

2. История и основополагающие принципы защиты данных

2.1 История и определения

В 1890 г. американские юристы Сэмюэл Д. Уоррен и Луис Брэндис написали эссе «Право на конфиденциальность», в котором утверждалось, что люди имеют «право быть оставленными в покое»: эта формулировка использовалась в качестве определения конфиденциальности[2]. В 1948 г. была принята Всеобщая декларация прав человека, в которую вошло двенадцатое основополагающее право — право на неприкосновенность личной жизни[3]. По мере ускорения технического прогресса развивалась и правовая база в сфере защиты данных. В 1980 г. в условиях все более широкого использования компьютеров для обработки данных и роста их вычислительной мощности Организация экономического сотрудничества и развития выпустила руководство по защите данных[4]. Годом позже Совет Европы принял Конвенцию о защите данных (Конвенцию № 108), ставшую первым документом в законодательстве европейских стран, закрепившим право на конфиденциальность личных данных[5]. Изначально эта нормативная база должна была защищать отдельных граждан от посягательств на конфиденциальность их личных данных со стороны государства.

В конце 1983 г. Федеральный конституционный суд Германии принял принципиальное решение по так называемому «делу о переписи населения»[6]. Этот вердикт рассматривается как историческая веха в сфере защиты данных, так как в нем сформулировано «право на информационное самоопределение». В течение последующих десятилетий это решение суда будет продолжать стимулировать расширение защиты данных. В 1995 г. была принята Европейская директива о защите данных 95/46/ЕС, в которой были отражены технологические достижения и внедрены новые понятия, включая, в частности, обработку данных, конфиденциальные персональные данные и согласие. Директива была призвана в частности нивелировать растущее неравенство в соотношении правовых приоритетов между частными корпорациями и гражданами и уточняла, что право на информационное самоопределение действительно носит универсальный характер и может быть использовано против кого бы то ни было.

2 Warren SD, Brandeis LD. The right to privacy. Harv Law Rev. 1890;4(5):193–220.

3 Всеобщая декларация прав человека. Нью-Йорк: Организация Объединенных Наций; 1948 (https://www.un.org/ru/universal-declaration-human-rights/index.html).

4 OECD work on privacy. In: Organisation for Economic Co-operation and Development [веб-сайт]. Paris: OECD Publishing; 2020 (http://www.oecd.org/sti/ieconomy/privacy.htm).

5 Конвенция № 108 и протоколы к ней. В: Совет Европы [веб-сайт]. Страсбург: Совет Европы; 2020 (https://www.coe.int/ru/web/conventions/full-list/-/conventions/rms/0900001680078c46).

6 Выдержка из решения Федерального конституционного суда Германии от 15 декабря 1983 г., 1 BvR 209, 269, 362, 420, 440, 484/83 [CODICES]. Karlsruhe: Federal Constitutional Court; 1993 (https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html).

В 2016 г. после четырех лет обсуждения Европейский парламент утвердил Общий регламент по защите данных (GDPR)[7]. GDPR служит основой для принятия различных законов о защите данных по всему миру. В 2018 г. Организация Объединенных Наций приняла документ «Принципы защиты персональных данных и неприкосновенности личной информации» в качестве основного руководства по защите персональных данных во всех учреждениях Организации Объединенных Наций[8].

Согласно законам о защите данных, действующим в разных странах мира, персональные данные – это любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу. Идентифицируемое физическое лицо – это физическое лицо, которое может быть идентифицировано, прямо или косвенно, в частности, посредством идентификационного номера (например, номера в системе социального страхования) или через один или несколько признаков, характерных для его физической, физиологической, психологической, экономической, культурной или социальной идентичности (например, фамилия и имя, дата рождения, биометрические данные, отпечатки пальцев и т. д.).

Важным термином в этом определении является слово «относящаяся», поскольку оно подразумевает и то, что такие данные не принадлежат субъекту данных (как объект права собственности), и то, что такие данные могут в равной степени относиться более чем к одному лицу. Например, информация о том, что лицо страдает дальтонизмом (заболеванием, которое чаще затрагивает мужчин), в равной степени относится и к его матери как к носителю соответствующего гена, и к отцу его матери, который также будет являться дальтоником. Следовательно, обработка таких данных на основе информированного согласия может потребовать согласия всех субъектов данных, к которым относятся эти данные. Таким образом, субъект данных – это любое идентифицированное или идентифицируемое физическое лицо, к которому относятся персональные данные.

Персональные данные, которые были обезличены, зашифрованы или псевдонимизированы, но все еще остаются потенциальным средством повторной идентификации лица, сохраняют статус персональных данных и подпадают под действие законов о защите данных.

Персональные данные, предоставленные анонимно таким образом, что лицо не идентифицируется или более не может быть идентифицировано, более не считаются персональными данными. Для того, чтобы данные считались действительно обезличенными, обезличивание должно быть необратимым.

7 Регламент Европейского парламента и Совета Европейского союза (EU) 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/EC (Общий Регламент о защите персональных данных) (https://ogdpr.eu/ru/gdpr-2016-679).

8 Personal data protection and privacy principles. Geneva: United Nations System; 2018 (https://www.unsystem.org/personal-data-protection-and-privacy-principles).

2.2 Основные принципы защиты данных в контексте общественного здравоохранения

Процесс защиты данных построен на соблюдении основных принципов, закрепленных в таких важных документах, как Конвенция № 108 Совета Европы, Хартия Европейского союза (ЕС) об основных правах[9] и национальные конституции многих стран.

Для обеспечения полного соблюдения применимых законов и нормативных актов в области защиты данных физические или юридические лица, обрабатывающие персональные данные (процессоры), должны придерживаться следующих принципов защиты данных.

- **Справедливость, законность и прозрачность:** обработка персональных данных должна производиться справедливо, законно и прозрачным образом по отношению к субъекту данных. В частности, персональные данные следует обрабатывать только в том случае, если это разрешено законом и когда для этого имеются основания: преобладающий законный интерес процессора или согласие на то субъекта данных.
- **Ограничение целью:** персональные данные можно получать только для одной или более конкретных и законных целей; обрабатывать их каким-либо образом, не способствующим достижению этой цели (целей), запрещено.
- **Точность:** персональные данные должны быть точными, и при необходимости их следует обновлять.
- **Минимизация данных:** персональные данные должны быть актуальными, соответствовать цели их обработки, а также ограничиваться лишь необходимым для ее достижения.
- **Ограничение срока хранения:** персональные данные, обрабатываемые в каких-либо целях, не должны храниться дольше, чем требуется для достижения этих целей**.**
- **Права субъектов данных:** персональные данные должны обрабатываться с соблюдением прав субъектов данных, как того требует применимое законодательство в области защиты данных**.**
- **Целостность и конфиденциальность:** необходимо принять соответствующие физические, технические, юридические и организационные меры для предотвращения несанкционированной или незаконной обработки персональных данных и их случайной потери, изменения или повреждения.
- **Передача персональных данных на международном уровне:** персональные данные не должны передаваться в третьи страны или в международные организации, если в этих странах/организациях не обеспечен соответствующий уровень защиты прав и свобод субъектов данных в связи с обработкой персональных данных[10].

9 Хартия Европейского союза об основных правах (https://eulaw.ru/treaties/charter/).

10 Более подробную информацию см. в Handbook on European data protection law – 2018 edition. Vienna: European Union Agency for Fundamental Rights; 2018 (https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition).

Соблюдение этих принципов гарантирует способность контролеров данных, таких как учреждения общественного здравоохранения, продемонстрировать, что их деятельность в полной мере подотчетна, а обработка данных осуществляется справедливым и сбалансированным образом, затрагивающим право на информационное самоопределение или право на конфиденциальность лишь в той мере, в какой это необходимо для соблюдения общественных интересов в сфере здравоохранения.

Рекомендуемые действия

- Выработать комплексное понимание принципов.
- Разработать план реализации принципов в конкретных условиях.
- Разработать долгосрочный план систематического соблюдения этих принципов.

2.3 Законные основания для обработки данных

Вне зависимости от цели обработки персональных данных она не допускается при отсутствии неопровержимых доказательств того, что у контролера данных имеются веские законные основания для подобной обработки (статья 6 GDPR). Это положение закреплено в первом принципе защиты данных. Для обработки данных существует шесть законных оснований. Ни одно из этих оснований не является более правильным или важным, чем остальные: выбор в пользу того или иного основания делается исходя из цели обработки и взаимоотношений с соответствующим физическим лицом. Законное основание должно быть определено до начала обработки и надлежащим образом задокументировано согласно типу обработки. Подробное описание этих шести категорий приведено ниже.

- **Согласие:** лицо дало явное информированное согласие на обработку персональных данных для конкретной задачи.
- **Договор:** обработка данных необходима для выполнения условий договора, заключенного между контролером и лицом, или в силу того, что субъект данных попросил начать процедуру обработки до заключения договора**.**
- **Правовая обязанность:** обработка необходима для соблюдения законодательства (не включая договорные обязательства).
- **Жизненно важные интересы:** обработка необходима для защиты чьей-либо жизни.
- **Общественная задача:** обработка необходима для исполнения задачи в интересах общества или осуществления части официальной задачи или функции, у которых есть четкое правовое основание.
- **Законные интересы:** обработка необходима для защиты законных интересов третьей стороны и при этом нет веской причины защищать персональные данные лица, которая являлась бы более значительной, чем законные интересы такой стороны; это юридическое основание, однако, не применимо в тех случаях, когда орган государственной власти обрабатывает персональные данные в рамках осуществления своих официальных задач.

Очевидно, что для деятельности по обработке данных в контексте задач управления информацией здравоохранения некоторые виды законных оснований будут применяться с большей вероятностью. Скорее всего, обработка данных будет осуществляться на основании юридических обязанностей и государственных задач; в редких случаях может применяться основание, связанное с жизненными интересами. Одним из важнейших правовых оснований является информированное согласие субъекта данных: оно безусловно играет значительную роль при осуществлении исследовательской деятельности, но также может использоваться для задач общественного здравоохранения, решить которые можно только располагая наборами данных без существенных пробелов.

Следовательно, информированное согласие субъекта данных может не понадобиться при наличии законного основания (например, при ведении онкорегистра) или явного преобладающего государственного интереса (например, в случае пандемии). Концепция информированного согласия применима лишь при условии, что субъект данных располагает «реальным» выбором, а также если отказ дать согласие не влечет за собой негативных последствий для субъекта данных[11].

На практике информированное согласие субъекта данных часто применяется неправомерно в качестве практически универсального правового основания; информированное согласие может оказывать существенное влияние на результаты деятельности в сфере общественного здравоохранения. В связи с этим зачастую рекомендуется выбирать альтернативное правовое основание. Однако необходимо соблюдать осторожность, поскольку действие требований к прозрачности может быть прекращено только при введении конкретных исключений.

Рекомендуемые действия

- Определить конкретное правовое основание для обработки данных.
- Тщательно проанализировать перспективы использования информированного согласия в качестве правового основания.
- Использовать основание, связанное с жизненными интересами, только в исключительных случаях, когда вмешательство в сфере общественного здравоохранения приносит непосредственную пользу субъектам данных.
- Надлежащим образом документировать все обсуждения и любые принятые решения.

11 Краткую информацию о законных основаниях обработки данных см. в: Lawful basis for processing. In: ICO [веб-сайт]. Wilmslow: Information Commissioner's Office; 2020 (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/).
Об информированном согласии см.: Guidelines 05/2020 on consent under Regulation 2016/679. In: EDPB [веб-сайт]. Brussels: European Data Protection Board; 2020 (https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en).

2.4 Принцип информированного согласия

Поскольку для любой обработки данных необходимо правовое основание, исследователи зачастую прибегают к информированному согласию субъектов данных, в том числе для легитимизации обработки персональных данных[12]. Тем не менее, как уже отмечалось выше, информированное согласие является лишь одним из шести правовых оснований; оно должно использоваться в общественном здравоохранении только при выполнении определенных условий.

- Согласие подразумевает, что субъекты данных располагают реальным выбором и возможностями для управления ситуацией.
- Согласие требует положительного ответа субъекта данных, то есть ясного выражения его воли.
- Согласие должно быть конкретным и детальным – в частности, в том, что касается целей обработки данных. В исследовательской деятельности применяются исключения из этого правила: так, формулировка «согласие на онкологические исследования» может оказаться достаточно конкретной, если субъект данных способен понять последствия этого согласия.
- В том случае, если информация о субъекте данных поступает в распоряжение объектов инфраструктуры общественного здравоохранения или исследований, например в национальный биологический банк, также допустимо использование широкого согласия[13].

Согласие может применяться только в том случае, если учреждение общественного здравоохранения или медицинское учреждение предлагает субъектам данных реальный выбор, и если субъекта данных ни прямо, ни косвенно не принуждают дать согласие на обработку данных. Это требование всегда имеет большое значение в тех случаях, когда получение согласия происходит в медицинском учреждении, поскольку отказ дать согласие может серьезно повлиять на уровень оказываемой медицинской помощи. Аналогичным образом согласие не может применяться тогда, когда контролер данных не способен (или не намерен) предложить субъекту реальный выбор, поскольку в таком случае процедура получения согласия направлена на введение в заблуждение и несправедлива по своей сути.

Согласие должно быть задокументировано надлежащим образом, причем используемые для этого документы должны иметь четкую структуру, ясное содержание и составляться на языке, понятном субъекту данных. Субъекту данных следует дать достаточно времени для обдумывания своего выбора и при необходимости обеспечить ему доступ к дополнительной информации и консультациям. Определение «информированное» не менее важно, чем само слово «согласие»; подробно этот вопрос рассматривается ниже в разделе 2.5, посвященном теме прозрачности.

12 Guidelines 05/2020 on consent under Regulation 2016/679. In: EDPB [веб-сайт]. Brussels: European Data Protection Board; 2020 (https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en).

13 Donnelly M, McDonagh M. Health research, consent and the GDPR exemption. Eur J Health Law. 2019;26(2):97–119.

Рекомендуемые действия

- Информированное согласие нельзя использовать как средство «упрощения» выбора правового основания: необходимо тщательно оценить, правильным ли будет его использование в вашей ситуации, связанной с обработкой данных.
- Тщательно оценить степень свободы выбора субъекта данных.
- Четко донести до субъекта данных, что у него/нее есть реальный выбор.
- Придерживаться принципов детальности и конкретности: по возможности избегать использования широкого или общего согласия.

2.5 Прозрачность

Как уже отмечалось выше, одним из основных принципов современного законодательства в области защиты данных является принцип прозрачности. Этот факт напрямую связан с историческим решением германского суда по делу о переписи населения 1983 г. (см. раздел 2.1), в котором суд заявил:

> *«Исходя из понятия самоопределения, общее право личности включает в себя предоставленную отдельному лицу возможность самостоятельно принимать принципиальное решение о том, раскрывать ли какие-либо аспекты своей личной жизни и если да, то в какой степени. <…> Если лицо не способно с достаточной уверенностью определить, какого рода личная информация известна его окружению, а также трудно установить, какая информация доступна его потенциальным партнерам по коммуникации, это может серьезно нарушить свободу осуществления самоопределения»*[14].

Таким образом, принцип прозрачности имеет фундаментальную и неотъемлемую связь с принципом справедливости. Принцип прозрачности обработки данных в контексте общественного здравоохранения заключается в том, что взаимодействие с субъектами данных должно осуществляться понятным, открытым и честным образом; для этого необходимо, чтобы учреждения общественного здравоохранения раскрывали суть основных элементов деятельности по обработке данных[15].

Четкая и краткая информация должна предоставляться на понятном субъекту данных языке вне зависимости от того, получены ли данные непосредственно от субъекта или от третьей стороны.

Предоставление информации также крайне важно в случае изменения цели обработки (например, при вторичном использовании информации здравоохранения), если к ситуации не применимы конкретные исключения. Основными примерами таких

14 Выдержка из решения Федерального конституционного суда Германии от 15 декабря 1983 г., 1 BvR 209, 269, 362, 420, 440, 484/83 [CODICES]. Karlsruhe: Federal Constitutional Court; 1993 (https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html).

15 О концепции прозрачности в соответствии с GDPR см.: Guidelines on transparency under Regulation 2016/679 (wp260rev.01). Brussels: European Commission; 2018 (https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025).

исключений являются ситуации, в которых предоставление подобной информации оказывается невозможным или требует несоразмерных цели усилий, либо ситуации, в которых исключение предусмотрено законом.

Для обеспечения надлежащей прозрачности контролеры данных в сфере общественного здравоохранения могут руководствоваться статьями 13 и 14 GDPR, содержащими перечень информации, предоставляемой субъекту данных. Помимо непосредственной коммуникации с субъектами данных посредством уведомлений о конфиденциальности или условий соблюдения конфиденциальности, государственным учреждениям здравоохранения также рекомендуется вести активный диалог с гражданским обществом и регулярно отчитываться перед общественностью о своей деятельности в области защиты данных.

Рекомендуемые действия

- Разработать политику конфиденциальности и опубликовать ее на веб-сайте или иным образом.
- Убедиться, что она написана простым языком, доступным пониманию непрофессионалов.
- Обеспечить наличие каналов связи с субъектами данных.
- Активно работать с гражданским обществом, доводя до его сведения используемые вами концепции и процедуры защиты данных.

3. Защита субъектов данных в законодательстве о защите персональных данных

3.1 Права субъектов данных

Цель современных законов о защите данных заключается в том, чтобы дать гражданам возможность осуществлять свои права в мире, который все больше контролируют технологические компании и другие стороны, обрабатывающие огромные объемы данных, относящихся к гражданам. В контексте оказания медицинской помощи и смежных ситуаций, связанных со здоровьем (например, в области принятия решений на заключительном этапе жизни), расширение прав и возможностей граждан играет не менее важную роль.

Соблюдение прав субъектов данных, также как получение медицинской помощи надлежащего уровня, неразрывно связаны с принципом прозрачности, поскольку только информированные и обладающие полномочиями граждане способны осуществлять свои права. Ответственность за соблюдение прав субъектов данных лежит на контролере данных. Выступая в этом качестве, контролер данных также обязан обеспечить, чтобы любой процессор (или, в случае передачи данных между контролерами, любой получатель данных) соблюдал права субъектов данных[16]. Подробное описание прав субъекта данных приведено ниже.

- **Право на доступ к данным** означает: а) право субъекта данных знать, обрабатываются ли относящиеся к нему данные, и б) если дело обстоит именно так, то право на доступ к таким данным и получение копии этих данных.
- **Право на внесение исправлений** означает, что если персональные данные являются неточными, субъект данных вправе потребовать от контролера исправления фактически неточных данных.
- **Право на удаление** (в некоторых юрисдикциях, если персональные данные были обнародованы, оно называется правом на забвение) – это основное право, позволяющее ограничить обработку данных и обеспечить соблюдение сроков их хранения.
- **Право на ограничение обработки** по сути представляет собой право гражданина ограничить обработку своих персональных данных в том случае, если он может претендовать на преимущественное право такого ограничения.
- **Право на получение информации** является основополагающим правом, которое следует воспринимать как ключевой элемент прав субъекта данных.

16 Подробнее см.: Voigt P, von dem Bussche A. Rights of data subjects. In: The EU General Data Protection Regulation (GDPR). Cham: Springer; 2017: 141–87.

Большинство законов о защите данных, действующих в европейских и других странах, требуют от контролеров информировать субъектов данных по ряду вопросов; как правило, информирование должно осуществляться заранее, четко, кратко и в доступных пониманию неспециалиста терминах. Это право может не применяться в ряде исключительных случаев, которые, например, касаются исследований в сфере медицины или здравоохранения либо другой деятельности, относящейся к охране общественного здоровья. Тем не менее любое исключение из права на получение информации должно быть тщательно проанализировано и задокументировано.

- **Право на переносимость данных** во многих юрисдикциях является относительно новым; оно связано с правом на доступ к данным, поскольку предусматривает право получать относящиеся к лицу данные в формате, пригодном для машинного считывания, причем, возможно, гражданин даже может попросить контролера данных передать данные другому контролеру. Как правило, право на переносимость данных распространяется только на данные, полученные на основании согласия субъекта данных или договора с субъектом данных. Оно не распространяется на обработку, осуществляемую на законных основаниях, и не может применяться в тех случаях, когда его соблюдение может нарушить важные общественные интересы, включая охрану общественного здоровья.

- Одним из важных прав, в том числе в контексте мероприятий по охране общественного здоровья, является **право субъекта данных на возражение**. Оно означает, что субъект данных может высказать свои возражения против обработки его персональных данных. Несмотря на то, что этому праву отводится важная роль в ситуациях прямого маркетинга или составления профилей, оно может быть ограничено, если орган общественного здравоохранения или другой государственный орган обладает преимущественной заинтересованностью в обработке данных и осуществляет ее для общего блага. Например, в ситуации пандемии граждане могут быть лишены права возражать против обработки данных, если такая обработка необходима для отслеживания и наблюдения за их действиями. Тем не менее в таких случаях применение права на возражение против обработки может фактически обязать государственные учреждения обеспечить, чтобы обработке подвергался только минимальный объем данных, необходимый для выполнения поставленной задачи.

- **Право субъекта данных не становиться объектом решения, основанного исключительно на автоматизированной обработке**, включая составление профиля, которое порождает юридические последствия в отношении субъекта данных или аналогичным образом существенно влияет на него, имеет такие же ограничения, что и право на возражение, в контексте мероприятий по охране общественного здоровья. Следует отметить, что при осуществлении деятельности на благо общества учреждения должны обеспечивать полное соблюдение сути права на информационное самоопределение и гарантировать, что субъект данных не выступает объектом решения, основанного исключительно на автоматической обработке[17].

17 Подробнее см.: Chapter 6.1 of Handbook on European data protection law – 2018 edition. Vienna: European Union Agency for Fundamental Rights; 2018 (https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition).

Соблюдение прав субъектов данных имеет первостепенное значение, в том числе в контексте деятельности по охране общественного здоровья, ведь когда медицинские учреждения соблюдают эти права, граждане относятся к деятельности по обработке данных с бóльшим доверием. Например, если в ситуации, подобной пандемии COVID-19, приложение для отслеживания контактов будет игнорировать права субъектов данных и создавать возможность применения таких данных для вторичных целей, например для сбора налогов, граждане могут отказаться от использования подобного приложения. В онлайновом мире доверие является самой ценной валютой; органам здравоохранения будет практически невозможно вернуть однажды утраченное доверие[18].

Рекомендуемые действия

- Четко и эффективно информировать субъектов данных об их правах.
- Определить процедуры и платформы для подачи запросов субъектами данных.
- Обеспечить партнерские отношения с субъектами данных, которые являются «клиентами».
- Документировать запросы субъектов данных и меры для их выполнения.
- Гарантировать, что ИТ-системы содействуют выполнению запросов субъектов данных (например, об удалении данных).
- Разработать стратегию информирования о любых причинах, по которым происходит отклонение запросов субъектов данных.

18 Hodges C. Delivering data protection: trust and ethical culture. Eur Data Prot L Rev. 2018;4(1):65–79.

4. Защита данных и общественное здравоохранение: правовая основа и ограничения привилегированного положения здравоохранения

4.1 Защита данных в ИСЗ (включая нормативные подходы к здравоохранению)

За последние три десятилетия охват регулирования в области защиты данных и кибербезопасности существенно вырос. Настоящее руководство уделяет меньше внимания документам высокого уровня, например Хартии ЕС об основных правах, и посвящено уровню регулирования, который в большей степени затрагивает специалистов, работающих в сфере ИСЗ.

Чтобы рассмотреть данный уровень регулирования, важно провести разграничение между отраслевыми законами, регулирующими обработку информации здравоохранения, общими законами о защите данных (например, GDPR) и законами, которые регулируют обработку персональных данных и могут прямо или косвенно воздействовать на работу ИСЗ (примером может служить Постановление ЕС о защите конфиденциальности в секторе электронных средств связи (ePrivacy)).

Отраслевые законы важны потому, что предоставляют четкие руководящие указания по обработке персональных данных для целей здравоохранения, и зачастую выступают правовой основой деятельности по обработке данных. Такие законы могут либо касаться конкретных задач общественного здравоохранения (например, ведения онкорегистров), либо регулировать использование информации здравоохранения в клинических/медицинских учреждениях (как в случае с электронными медицинскими картами), а также последующее вторичное использование данных для целей охраны общественного здоровья. Разработка и применение таких законов действительно необходимы для защиты данных, поскольку они помогают добиться максимального уровня прозрачности и демократической легитимности.

Как правило, применение общих законов о защите данных и в особенности влияние более общего законодательства значительно осложняет обработку данных для использования в ИСЗ. Во всех общих законах о защите данных обработка персональных данных в медицинских целях занимает привилегированное положение. Это касается не только

обработки данных в целях охраны здоровья («жизненные интересы»), но и использования персональных данных для целей общественного здравоохранения.

Например, преамбула 46 GDPR гласит:

> *«Обработка персональных данных также считается правомерной, когда необходимо защищать интерес, который жизненно важен для субъекта данных или иного физического лица.* [19]*... Некоторые виды могут осуществляться на основании как важных публичных интересов, так и жизненно важных интересов субъекта данных, например, если обработка необходима в гуманитарных целях, в том числе для мониторинга эпидемий и их распространения или в чрезвычайных ситуациях гуманитарного характера, в частности, во время техногенных или природных катастроф».*

Следовательно, общественное здравоохранение занимает привилегированное положение с точки зрения правовой основы (обоснования) для обработки данных, объема деятельности по обработке и, в особенности, вторичного использования персональных данных для ведения ИСЗ.

В повседневной практике влияние последней категории законов часто приводит к возникновению серьезных сложностей, в т. ч. в сфере электронной конфиденциальности (например, служебные файлы cookies на веб-сайтах), критической инфраструктуры, норм ИТ-безопасности и других областях. Для применения всех этих законов и правил на практике и прогнозирования их прямого и косвенного воздействия на разработку и ведение ИСЗ необходимо глубокое понимание предмета и соответствующие юридические знания.

Специалисты в области управления информацией здравоохранения также должны знать, что привилегии, которыми пользуется общественное здравоохранение, не распространяются на защиту целостности и доступности данных. Иными словами, служение благим целям (например, целям охраны общественного здоровья) не оправдывает снижения стандартов ИТ-безопасности. Подобные привилегии жестко привязаны к конкретным целям общественного здравоохранения и не оправдывают вторичного использования данных для других целей как такового. Допускается создание дополнительных структур, служащих для вторичного использования данных (например, регистров или биобанков), но каждый такой случай вторичного использования следует тщательно анализировать в целях защиты интересов субъектов данных и общества[20].

19 Термин «физическое лицо» совпадает с определением субъекта данных, например, в пункте 1 статьи 4 GDPR. Антонимом в данном случае является «юридическое лицо», например, общество с ограниченной ответственностью или орган власти.

20 Подробнее см.: Chapter 9.3 of Handbook on European data protection law – 2018 edition. Vienna: European Union Agency for Fundamental Rights; 2018 (https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition).

Рекомендуемые действия

- Добиться четкого понимания отраслевого закона о защите данных.
- Добиться четкого понимания отраслевых законов, которые обязывают или по крайней мере разрешают обрабатывать персональные данные.
- Наладить процесс поиска и анализа информации о будущих изменениях и их возможном влиянии на общественное здравоохранение.
- Обеспечить строгое соблюдение стандартов ИТ-безопасности, поскольку на них не распространяются привилегии общественного здравоохранения.

4.2 Практические аспекты защиты данных в ИСЗ (включая проектируемую защиту данных и защиту данных по умолчанию)

Сложные и широкомасштабные мероприятия по обработке данных в секторе общественного здравоохранения требуют тщательного планирования и выполнения. Нормативные документы в области защиты данных предписывают, что контролеры данных должны обеспечивать учет вопросов конфиденциальности и защиты данных на этапе проектирования любой системы, услуги, продукта или процесса, а затем на протяжении всего жизненного цикла их эксплуатации в той мере, в какой подобные системы предусматривают обработку персональных данных. Разработка и интеграция решений по защите данных на ранних стадиях проекта позволяет заблаговременно выявить любые потенциальные проблемы, чтобы предотвратить их в долгосрочной перспективе. Таким образом, соблюдение принципа проектируемой защиты данных и защиты данных по умолчанию входит в сферу ответственности контролеров данных[21].

Защита данных по умолчанию предполагает предоставление контролерами гарантии того, что они обрабатывают только те данные, которые необходимы для достижения конкретной цели. Это требование связано с основополагающими принципами защиты данных – минимизацией данных и ограничением целью. Для сектора общественного здравоохранения это не означает необходимости отказаться от собственных интересов, поскольку принцип проектируемой защиты данных и защиты данных по умолчанию также требует соблюдения равновесия затрагиваемых интересов и ограничения целей жизненно важными интересами, такими как защита и укрепление здоровья.

Если взять в качестве примера ситуацию с COVID-19, то широкомасштабная обработка персональных данных, относящихся ко всем гражданам, может быть оправданной и полностью соответствовать этим принципам в той мере, в которой такая обработка необходима для смягчения риска пандемии COVID-19. Однако эти принципы также определяют необходимость действительных гарантий, позволяющих избежать использования персональных данных или злоупотребления ими во вторичных целях за исключением случаев, когда вторичная цель является столь же оправданной,

21 О концепции см.: Guidelines 4/2019 on Article 25 data protection by design and by default. In: EDPB [веб-сайт]. Brussels: European Data Protection Board; 2020 (https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en).

что и первичная (например, исследование на основе псевдонимизированных или обезличенных данных).

Вследствие этого учреждения общественного здравоохранения также должны тщательно отбирать партнеров и поставщиков услуг, включая первичных и вторичных процессоров. Требования к ИТ-безопасности и защите данных должны быть определены в рамках любого соответствующего тендерного или закупочного процесса, а договорные обязательства партнеров и поставщиков услуг должны отражать все соответствующие нормативные требования к контролерам данных или любые дополнительные требования, которые контролер данных может счесть необходимыми (например, для снижения репутационных рисков).

Рекомендуемые действия

- Наладить процесс управления разработкой, закупкой и внедрением новых систем обработки данных.
- Разработать стратегию минимизации последствий для субъектов данных в зависимости от цели обработки.
- Вести непрерывный мониторинг и контроль за соответствием требованиям.
- Тщательно отбирать партнеров, обеспечивать соблюдение необходимых стандартов и соответствие требованиям защиты данных с их стороны.

4.3 Защита данных и ИТ-безопасность

Если ИТ-безопасность традиционно занимается вопросами целостности и доступности данных, то защита данных обычно связывается с конфиденциальностью их обработки. В последние годы эти темы все чаще рассматриваются как единое целое; в нормативных актах, включая GDPR, предусмотрены чрезвычайно строгие требования к безопасности данных для контролеров данных[22].

В связи с этим контролеры (и процессоры) должны применять соответствующие меры безопасности для предотвращения случайной или преднамеренной компрометации персональных данных, находящихся в их распоряжении. Так, контролеры должны помнить, что хотя иногда информационная безопасность сводится к мерам кибербезопасности (т. е. защиты сетей и информационных систем от атак), она также охватывает и другие аспекты, включая меры физической и организационной безопасности.

Следовательно, достаточные организационные и технические меры по защите персональных данных имеют жизненно важное значение для сохранения доверия субъектов данных к их обработке и помогают системам здравоохранения обеспечить поддержку общества и соблюдение требований субъектами данных. Эти меры могут

22 Подробнее о требованиях безопасности в области обработки персональных данных см.: Handbook on security of personal data processing. Athens: European Union Agency for Cybersecurity; 2018 (https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing).

включать в себя не только технические мероприятия, включая шифрование данных при хранении и передаче, но и надежные подходы к управлению идентификацией, доступом или работой с данными, включая классификацию данных (например, деление на строго конфиденциальные / конфиденциальные / общедоступные). Одним из ключевых аспектов защиты является жесткое управление правами на администрирование и доступ; государственные учреждения здравоохранения (и учреждения здравоохранения в целом) зачастую не применяют во всей строгости принцип необходимого знания.

В таких нормативных документах, как GDPR, необходимые меры безопасности могут не быть изложены подробно. Вместо этого такие документы содержат требование о том, чтобы контролеры обеспечивали уровень безопасности, «соответствующий» связанным с обработкой рискам. Органы общественного здравоохранения и другие представители этого сектора должны учитывать данное требование в контексте новейших достижений и затрат на внедрение, а также характера, масштаба, условий и целей обработки.

Принимая во внимание, что перед сектором общественного здравоохранения часто ставятся задачи по обработке конфиденциальных персональных данных, включая данные, относящиеся к здоровью и физическому благополучию, субъекты данных рассчитывают на обеспечение чрезвычайно высокого уровня безопасности данных при осуществлении таких действий. В связи с этим отсутствие финансовых средств на принятие мер по обеспечению безопасности данных не является оправданием в той мере, в какой эти меры необходимы для достижения «соответствующего» уровня защиты.

Одной из важных тем является борьба с нарушениями безопасности персональных данных, то есть нарушениями безопасности, ведущими к случайному или незаконному уничтожению, потере, изменению, несанкционированному разглашению или доступу к персональным данным[23]. Нарушения безопасности могут быть результатом как случайных, так и преднамеренных действий. Ситуация, связанная с нарушением безопасности данных, легко может дестабилизировать работу учреждения любого масштаба и структуры. В связи с этим государственным учреждениям здравоохранения рекомендуется иметь план действий в подобных случаях (возможно, даже с задействованием учений по ликвидации киберпроисшествия). Должен существовать план действий на случай нарушения безопасности данных, где будут четко распределены задачи и обязанности, включая стратегию информирования о нарушении безопасности данных.

Одним из важных инструментов для решения этих задач являются регулярные тесты на проникновение, проводимые независимой третьей стороной: иными словами, контролер данных должен задействовать так называемых «белых хакеров» для проверки слабых мест системы. Во многих странах существуют агентства ИТ-безопасности или кибербезопасности, которые помогают учреждениям общественного здравоохранения создавать системы защиты. Для учреждений, выполняющих оперативные задачи, не менее важным и критически необходимым является наличие плана аварийно-восстановительных работ.

23 Руководящие указания см. в: Personal data breaches. Wilmslow: Information Commissioner's Office; 2020 (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/?q=data+breach).

Рекомендуемые действия

- Определить и задокументировать технические и оперативные мероприятия.
- Определить и наладить контроль выполнения требований к ИТ-безопасности, желательно с опорой на передовые практики, включая серию стандартов 270XX Международной организации по стандартизации (ISO).
- Настроить и поддерживать управление идентификацией и доступом, обеспечивая ограниченность прав администратора и соблюдение концепции необходимого знания.
- Гарантировать постоянное шифрование данных при передаче и хранении.
- В применимых ситуациях разработать стратегию безопасности для облачных вычислений, включая использование общедоступных облачных сервисов.
- Регулярно оценивать и контролировать ИТ- безопасность (например, с помощью тестов на проникновение со стороны).
- Разработать план действий и стратегию информирования в случае нарушения безопасности данных.
- При необходимости разработать план аварийно-восстановительных работ.

5. Обработка персональных данных в системах общественного здравоохранения: ограничения для первичного и вторичного использования данных

5.1 Использование персональных данных для ведения ИСЗ (включая концепцию вторичного использования)

Для целей настоящего документа термин «ИСЗ» обозначает систему, предназначенную для управления информацией здравоохранения в более широком смысле. Это определение включает в себя системы, которые собирают, хранят, обрабатывают и передают электронные медицинские карты пациентов, системы оперативного управления медицинскими учреждениями и системы поддержки стратегических решений в области здравоохранения. Очевидно, что различные виды ИСЗ могут сталкиваться с весьма различными и неоднородными проблемами в сфере защиты данных[24]. Например, если в контексте разработки политики здравоохранения временной недоступностью данных можно пренебречь, то в условиях медицинского учреждения она может привести к катастрофическим последствиям.

В настоящем руководстве основное внимание уделяется ведению ИСЗ и сфере разработки политики. Соответствующие данные зачастую бывают агрегированными или обезличенными и поэтому не подпадают под действие норм о защите данных. Вторичное использование данных играет важнейшую роль в контексте разработки политики общественного здравоохранения. Агрегирование или обезличивание персональных данных по возможности должно осуществляться на уровне источника, что позволит минимизировать риски в области защиты данных и сохранить контроль над деятельностью первичного контролера данных. В зависимости от способа использования данных (например, в онкорегистрах или биобанках) агрегирование или обезличивание на уровне источника может повлиять на качество данных, что требует централизованного подхода к обработке. Наборы персональных данных и агрегированные или обезличенные данные должны разделяться при хранении – как минимум за счет логичного структурного разграничения, и желательно в физически разделенных ИТ-системах.

24 Подробнее см.: Michelsen K, Brand H, Achterberg P, Wilkinson J. Повышение степени интеграции информационных систем здравоохранения: передовая практика и проблемы. Копенгаген: Европейское региональное бюро ВОЗ; 2015 (Обобщающий доклад Сети фактических данных в отношении здоровья № 40; https://www.euro.who.int/__data/assets/pdf_file/0010/298675/Promoting-better-integration-of-HIS-best-practices-and-challenges-ru.pdf).

По мере необходимости следует создавать инфраструктуру на основе принципа псевдонимизации (а не обезличивания)[25], что позволит контролерам данных общественного здравоохранения вновь обратиться к отдельному субъекту данных в той мере, в какой это будет служить для его прямой пользы. Примером такого подхода может служить обработка данных, касающихся экологических детерминант здоровья, например для исследования воздействия асбеста на здоровье людей в конкретном сообществе или отрасли[26].

Рекомендуемые действия

- По возможности обезличивать или агрегировать данные на уровне источника.
- Убедиться, что необработанные данные и обезличенные или агрегированные данные разделены как минимум логически (а желательно и физически).
- Если результаты обработки данных могут принести пользу отдельным лицам (пациентам), необходимо использовать псевдонимизированные данные.
- Разработать комплексную концепцию безопасности для регистров или биобанков.

5.2 Персональные данные и медицинские исследования (включая концепцию вторичного использования)

Одним из основных принципов защиты данных является принцип ограничения цели, в соответствии с которым контролер данных должен указать точную цель обработки до ее начала. Когда речь идет об информации здравоохранения, принцип целевого ограничения не является абсолютным, поскольку вторичное использование информации здравоохранения зачастую имеет жизненно важное значение для управления системами общественного здравоохранения и их улучшения. Таким образом, данные о здоровье, включая данные о различных детерминантах здоровья, представляют собой важный ресурс для разработки политики, управления системами здравоохранения и научных исследований[27]. Исследованиям отводится привилегированная роль, а принцип свободы исследований (и исследователей) принят во многих странах как основополагающее конституционное право и закреплен в различных международных политических документах[28].

Если исследование является основной целью обработки данных и эти данные были получены с информированного согласия субъектов данных, такое согласие ограничивает

25 Hintze M, El Emam K. Comparing the benefits of pseudonymisation and anonymisation under the GDPR. J Data Protect Priv. 2018;2(2):145–58.

26 Например, см.: Visonà SD, Villani s, Manzoni F, Chen T, Ardissino G, Russo F et al. Impact of asbestos on public health: a retrospective study on a series of subjects with occupational and non-occupational exposure to asbestos during the activity of Fibronit plant (Broni, Italy); J Public Health Res. 2018;7(3):1519. doi:10.4081/jphr.2018.1519.

27 Taylor MJ, Whitton T. Public interest, health research and data protection law: establishing a legitimate trade-off between individual control and research access to health data. Laws. 2020;9(1):6.

28 Chassang G. The impact of the EU General Data Protection Regulation on scientific research. Ecancermedicalscience. 2017;11:709. doi:10.3332/ecancer.2017.709. Интересный опыт Канады см.: Steeves V. Data protection and the promotion of health research. Healthc Policy. 2007;2(3):26–38.

возможность использования данных в каких-либо еще целях, если эти цели не связаны тесным образом с основной целью. На практике более сложная ситуация возникает при вторичном использовании данных в целях общественного здравоохранения (например, данных, первичная обработка которых производилась в медицинских учреждениях)[29].

В некоторых законах и нормативных актах необходимые правовые гарантии изложены весьма конкретно, а в GDPR содержится призыв к государствам-членам ЕС более подробно урегулировать этот вопрос в национальном законодательстве, поскольку здравоохранение как таковое в основном находится вне сферы компетенции ЕС. Вне зависимости от конкретных положений GDPR, вторичное использование допускается, если оно не является несовместимым с основной целью, для него имеется законное основание, а обработка проводится в соразмерном объеме и предпринимаются необходимые меры для сохранения данных в безопасности[30]. В случае, когда впоследствии данные продолжают служить целям общественного здравоохранения, их защита требует максимально возможной псевдонимизации, маскировки или даже обезличивания. Если данные хранятся в первоначальном виде и форме лишь из соображений удобства или для минимизации усилий по их обработке, это является нарушением законодательства о защите данных.

По причине неоднородности нормативной конъюнктуры в Европейском регионе ВОЗ перед запуском конкретного исследовательского проекта, предусматривающего вторичное использование данных, необходимо провести его детальную оценку на индивидуальной основе. В этой ситуации также крайне важно тщательно документировать дискуссию и сохранять максимальную прозрачность по отношению к субъектам данных и другим соответствующим заинтересованным сторонам. В тех случаях, когда осуществление проекта требует передачи данных другому государству или международной организации, могут применяться особые требования.

При обработке данных для целей охраны общественного здоровья и научных исследований могут применяться определенные ограничения прав субъектов данных. Работникам общественного здравоохранения и исследователям рекомендуется пользоваться этими исключениями лишь в той мере, в которой они строго необходимы. Аналогичным образом исключения могут применяться и в отношении хранения/удаления данных, поскольку при их вторичном использовании устанавливаются новые (а следовательно, и отличные от ранее оговоренных) сроки хранения.

Рекомендуемые действия

- Гарантировать разграничение между исследовательской деятельностью и мероприятиями по обработке данных для целей разработки политики.
- Отказаться от использования одной и той же ИТ-инфраструктуры для научных исследований и для оперативной обработки данных.

29 Peloquin D, DiMaio,Bierer B, Barnes M. Disruptive and avoidable: GDPR challenges to secondary research uses of data. Eur J Hum Genet. 2020;28:697–705. doi:10.1038/s41431-020-0596-x.

30 Chico V. The impact of the General Data Protection Regulation on health research. Br Med Bull. 2018;128(1):109–18. doi:10.1093/bmb/ldy038.

- Поощрять работу исследователей с данными и информировать их о привилегированном положении научных исследований.
- Тщательно анализировать правовую базу, регулирующую трансграничную исследовательскую деятельность.
- Надлежащим образом документировать исследовательскую деятельность (например, решения относительно обоснованности вторичного использования и хранения данных в исследовательских целях).

5.3 Нахождение равновесия между защитой данных и охраной общественного здоровья

Как уже отмечалось выше, персональные данные не являются «собственностью» субъекта данных, поскольку даже относясь к одному лицу они могут в равной степени относиться и к другим лицам. Законы, нормативные акты и суды также отмечают, что отдельные лица являются частью общества: они взаимодействуют с обществом и подчиняются различным законным интересам, которые могут требовать аналогичной степени защиты. В контексте охраны общественного здоровья и управления ИСЗ право на здоровье является одним из основных фундаментальных прав, признаваемых во всем мире в качестве одного из наиболее важных прав человека.

Право на здоровье впервые было сформулировано в Уставе ВОЗ 1946 г., в котором заявляется, что «обладание наивысшим достижимым уровнем здоровья является одним из основных прав всякого человека». В преамбуле Устава здоровье определяется как «состояние полного физического, душевного и социального благополучия, а не только отсутствие болезней и физических дефектов»[31].

Право на здоровье представляет собой инклюзивное право, которое включает в себя не только право на своевременные и адекватные услуги в области здравоохранения, но и на такие основополагающие предпосылки здоровья как доступ к безопасной питьевой воде и адекватным санитарным услугам, безопасные условия труда и окружающей среды, а также доступ к просвещению и информации в области здоровья, в том числе полового и репродуктивного здоровья. Хотя право на здоровье является одним из основополагающих прав, защищающих личность, оно также обосновывает деятельность государственных органов и других заинтересованных сторон, направленную на содействие осуществлению права на здоровье. Таким образом, создание и ведение ИСЗ, поддерживающих доступ к информации здравоохранения и управление системами здравоохранения, является законно признанным интересом, который должен быть уравновешен с защитой данных.

Сохранение равновесия в этом контексте следует воспринимать не как однозначный выбор в пользу одного или другого, а скорее как попытку наилучшим возможным образом защитить как интересы, так и лежащие в их основе фундаментальные права.[32] Следовательно, все субъекты общественного здравоохранения должны определить интересы общественного здравоохранения, которые они намерены преследовать

31 Устав Всемирной организации здравоохранения. Женева: Всемирная организация здравоохранения; 1946 (https://www.who.int/ru/about/who-we-are/constitution).

32 Dworkin R. A matter of principle. Cambridge, MA: Harvard University Press; 1985.

(«цель»), а затем выбрать методы и средства, которые будут представлять наименьшую возможную угрозу нарушения права на информационное самоопределение. В редких случаях анализ может показать, что интересы общественного здравоохранения не оправдывают ограничения права на информационное самоопределение; в других ситуациях (например, во время пандемии) приемлемыми с точки зрения закона могут оказаться даже серьезные негативные последствия для защиты данных. Следует отметить, что первостепенное значение в этом контексте имеет концепция цели, поскольку обработка данных, полученных с помощью приложения для отслеживания контактов с больными COVID-19, может оказаться приемлемой для целей защиты общественного здоровья, но в то же время неприемлемой для целей правоохранительной деятельности, направленной на борьбу с мелкими правонарушениями.

Соблюдение равновесия затрагиваемых интересов – и в особенности соблюдение основополагающих прав – должно быть в равной степени отражено в процессах разработки политики, включая разработку законов и других законодательных актов. По большей части для этого существует надлежащая правовая процедура, поскольку решения, определяющие такое равновесное соотношение, требуют суждений, которые зачастую выносятся в ситуациях неопределенности (например, как в ситуации с COVID-19, поскольку изначально неясно, каким образом будет распространяться пандемия). В этих ситуациях крайне важно обеспечивать прозрачность дискуссий и надлежащим образом информировать граждан и других субъектов гражданского общества.

Процесс нахождения равновесия затрагиваемых интересов и основополагающих прав не может быть простым, и универсального рецепта здесь не существует. Для достижения согласованности прав необходимо надлежащее документирование и соблюдение принципа прозрачности по отношению ко всем заинтересованным сторонам, включая широкую общественность и субъектов данных, затронутых соответствующими действиями. Этот процесс также важен, чтобы определить, может ли деятельность по обработке данных требовать согласия субъекта данных, или ее оправдывает законный и обладающий преимущественной силой правовой интерес.

Рекомендуемые действия

- Обучать специалистов общественного здравоохранения соблюдению равновесия между затрагиваемыми основополагающими правами.
- Взаимодействовать с гражданским обществом в контексте признания важности обработки данных для мероприятий по охране общественного здоровья.
- Установить этические и правовые критерии для исключительных ситуаций, таких как пандемия COVID-19.

6. Выстраивание системы управления защитой данных в сфере общественного здравоохранения

6.1 Практическое осуществление защиты данных в ИСЗ

Действующие во всем мире законы о защите данных предлагают использовать для обеспечения конфиденциальности, целостности и доступности данных и устойчивости систем подходы, основанные на оценке рисков и применении процессов. Для этого необходима процедура регулярного пересмотра эффективности мер безопасности и их непрерывное совершенствование. Защита данных представляет собой не единичное мероприятие, а задачу, которая должна быть интегрирована во все виды деятельности, связанные с управлением ИСЗ. Аналогичным образом защита данных является задачей и обязанностью каждого участника процесса обработки данных и не должна быть возложена исключительно на специалистов по защите данных или отдел управления данными.

Одним из важных инструментов, позволяющим всем соответствующим заинтересованным сторонам в составе организации оценить требования к защите данных, является оценка воздействия на защиту данных (ОВЗД). Эта официальная процедура и инструмент документирования широко используется для сопряженной с высокими рисками деятельности по обработке данных; типовые формы для него предоставляют различные органы, занимающиеся защитой данных, и другие заинтересованные стороны. ОВЗД рекомендуется проводить до запуска новой ИТ-системы или процесса обработки[33].

Руководить организацией этого процесса должны специалисты по защите данных, однако повседневная ответственность за соблюдение законов о защите данных лежит на контролере данных как субъекте, выполняющем обязанности по обработке данных.

Защита данных сама по себе предполагает наличие достаточных ресурсов, постоянное обучение и поддержку со стороны высшего руководства. Контролер данных должен также обеспечивать наличие соответствующих возможностей для аудита защиты данных и содействовать аудиторам, проводящим проверку от имени органов по защите данных. Под аудитом защиты данных подразумевается систематическая и независимая проверка соответствия деятельности, связанной с обработкой персональных данных, внутренней политике и процедурам в области защиты данных, а также требованиям применимой нормативной базы[34]. По итогам программы аудита должен приниматься

33 Руководящие указания см. в: Data protection impact assessments. Wilmslow: Information Commissioner's Office; 2020 (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/).

34 См. руководство французского органа по защите данных: What you should know about our standard on data processing audits. Paris: Commission Nationale de l'Informatique et des Libertés; 2020 (https://www.cnil.fr/en/what-you-should-know-about-our-standard-data-processing-audits).

план непрерывного повышения качества; кроме того, проверяющие могут рекомендовать прохождение отраслевых программ сертификации, таких как ISO 27001 или ISO 27701[35].

Рекомендуемые действия

- Создать систему управления рисками для защиты данных, которая будет охватывать различные категории рисков, в т. ч. финансовые и репутационные.
- Обеспечить поддержку со стороны высшего руководства учреждения.
- Регулярно информировать высшее руководство и регулярно (раз в год или в схожие сроки) составлять отчеты о деятельности по защите данных.
- Сформировать средне- и долгосрочные планы финансирования ресурсов в области защиты данных.
- Соблюдать признанные на международном уровне стандарты, например ISO 27001, и проводить аудит соответствия этим стандартам.
- Проводить ОВЗД для сопряженной с высокими рисками деятельности.
- Если в учреждении отсутствует всесторонняя целостная система защиты данных, начать с малого и разработать концепцию для одной группы или отдела.

6.2 Просвещение и расширение прав и возможностей

Защита данных является важным компонентом ориентированного на соблюдение интересов человека подхода к технологиям и ориентиром для использования технологий в условиях перехода экономики и процессов разработки политики на цифровые рельсы. В системе общественного здравоохранения, где обработке персональных данных уделяется все больше внимания, описанные выше правовые гарантии становятся важным инструментом, позволяющим людям более эффективно контролировать свои персональные данные, а соответствующим учреждениям и организациям – осуществлять их обработку в законных целях, правовым, справедливым и прозрачным образом. Так как меры по защите данных должны быть интегрированы в разработку и осуществление программ в области охраны общественного здоровья, необходимо соответствующее просвещение и расширение прав и возможностей как граждан, так и специалистов общественного здравоохранения.

Грамотность в области работы с данными, подразумевающая в т. ч. грамотное управление обработкой данных и грамотную защиту персональных данных, должна стать неотъемлемой частью профессиональных знаний специалистов общественного здравоохранения, работающих с ИСЗ[36]. Просвещение в этой сфере должно опираться на описанные выше принципы и включать в себя применимую нормативную базу. Важным элементом просвещения является непрерывное повышение квалификации специалистов, уже прошедших курс академического образования. Для преодоления

35 Lachaud E. The General Data Protection Regulation and the rise of certification as a regulatory instrument; Comput Law Secur Rev. 2018;34(2):244–56.

36 О концептуальных вопросах интеграции защиты данных в учебные и образовательные программы см.: González Fuster G, Kloza D. The European handbook for teaching privacy and data protection at schools. Brussels: European Commission; 2016 (http://arcades-project.eu/index.php/deliverables).

барьеров, провоцирующих конфликт целей общественного здравоохранение и целей защиты данных, необходимы семинары, практические занятия и обучение решению конкретных проблем.

Непрерывное образование также чрезвычайно важно для того, чтобы обеспечить компетентность специалистов общественного здравоохранения в сфере новых технологий, таких как облачные вычисления или системы на основе блокчейна, внедряемых в секторе здравоохранения. Расширение прав и возможностей необходимо для правильного применения принципов защиты данных в постоянно меняющейся технологической среде.

Рекомендуемые действия

- Обеспечить включение вопросов защиты данных в комплекс просветительской деятельности в области общественного здравоохранения.
- Разработать предложения по непрерывному обучению в области защиты данных.
- Составить план профессиональной подготовки для учреждения.
- Разработать курсы повышения квалификации или методы обучения решению конкретных проблем, отвечающие особым потребностям учреждения.
- Поддерживать внедрение новых технологий или систем обработки данных с помощью соответствующих учебных программ.

6.3 Внешний надзор, внутренний контроль и меры по обеспечению соблюдения законодательства о защите данных

Защита данных, рассматриваемая как часть принципа подотчетности, требует от любого контролера данных нести ответственность за свою деятельность по обработке данных и за соблюдение принципов защиты данных. Чрезвычайно важно принимать соответствующие меры и иметь документы, подтверждающие соблюдение требований. Еще одним ключевым требованием является внутренний и внешний контроль; структура этого контроля может принимать различную форму или вид в зависимости от применимого законодательства. Различными законами о защите данных предусматривается наличие в штате специалиста по защите данных или соблюдению конфиденциальности. В организации он выполняет роль независимой стороны, которая консультирует контролера данных, ведет учет операций по обработке данных и служит контактным лицом для субъектов данных и органов власти[37].

Кроме того, специалист по защите данных управляет аудиторской деятельностью как внутри компании, так и в отношении третьих сторон, которые обрабатывают данные по поручению контролера данных. При выполнении аудиторских функций специалист по

37 Подробнее см.: Guidelines on data protection officers ('DPOs'). Brussels: European Commission; 2017 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048).

защите данных регулярно прибегает к помощи внутренних или внешних ресурсов ИТ-аудита. Важно отметить, что специалист по защите данных не должен иметь каких-либо конфликтующих интересов и подчиняется высшему руководству организации.

В большинстве стран Европейского региона ВОЗ были созданы специальные органы по защите данных, а в некоторых странах надзор за государственными и частными учреждениями в этой сфере осуществляют два разных органа. Используя установленные законом полномочия, орган по защите данных рассматривает жалобы субъектов данных в связи с потенциальными нарушениями закона о защите данных, делает запросы и проводит расследования нарушений законодательства о защите данных и в случае необходимости принимает меры по обеспечению его соблюдения, а также содействует повышению осведомленности субъектов данных об их правах на защиту персональной информации в соответствии с применимыми законами о защите данных.

Органы общественного здравоохранения должны помнить о разнообразии рисков, связанных с нарушениями в области защиты данных, главным из которых является репутационный ущерб. Кроме того, орган по защите данных может подвергнуть органы общественного здравоохранения и научно-исследовательские институты денежному штрафу (до 20 млн евро в случае нарушения GDPR), наложить судебный запрет или обязать принять меры для исправления ситуации[38]. Очевидно, что в связи с этим в любом крупном учреждении общественного здравоохранения должен существовать надежный механизм управления рисками в области защиты данных, а следовательно, необходимы специальные знания на стыке сфер обеспечения соответствия, ИТ и защиты данных.

Одним из важных способов борьбы с такими рисками является соблюдение общепризнанных стандартов и сертификатов, например стандарта ISO 27701 для систем управления защитой данных. Поскольку получение подобных сертификатов может быть связано с трудностями и требует выделения надлежащих ресурсов, всем контролерам данных следует создать внутреннюю систему контроля защиты данных, функции которой будут соразмерны рискам организации в сфере защиты данных.

Рекомендуемые действия

- Назначить независимого и компетентного специалиста по защите данных.
- Создать в рамках компании институт внутреннего аудита для обеспечения ИТ-безопасности и защиты данных.
- Активно взаимодействовать с органами по защите данных и гражданским обществом.
- Сотрудничать с национальными и зарубежными партнерами для обмена передовым опытом.
- Надлежащим образом документировать все действия для соблюдения принципа подотчетности.

38 Voigt P, von dem Bussche A. Enforcement and fines under the GDPR. In: The EU General Data Protection Regulation (GDPR). Cham: Springer; 2017: 201–17.

7. Выводы

Соблюдение требований к защите данных представляет собой сложную задачу для всей сферы общественного здравоохранения и в особой степени – для всех учреждений, активно участвующих в ведении ИСЗ. Следует отметить, что постепенно ужесточающиеся на протяжении последних десятилетий нормативные требования вынуждают сектор общественного здравоохранения корректировать свою политику и практику в отношении обработки персональных данных. Необходимо сделать тему защиты данных понятной для каждого, и предоставить руководящие указания относительно внедрения мер по охране общественного здоровья, которые будут полностью соответствовать требованиям и служить на пользу общества. Обеспечение защиты данных в сфере общественного здравоохранения сопряжено с решением новых и важных задач, возникающих по мере того, как технический прогресс расширяет границы эпиднадзора, больших данных, облачного хранения данных и других составляющих систем здравоохранения. Вследствие этого чрезвычайно важно, чтобы учреждения общественного здравоохранения имели возможность поддерживать равновесие между затрагиваемыми основополагающими правами и применять принципы защиты данных.

Эффективная защита данных не представляет собой нечто недостижимое: она требует правового и технического профессионализма, выделения достаточных ресурсов и подготовки всех специалистов, вовлеченных в процесс обработки персональных данных. Защита данных представляет собой не единичное мероприятие, а непрерывную деятельность, определяемую организационной стратегией, концепцией управления и готовностью нести ответственность. Эта ответственность, основанная на тщательной оценке рисков, опирается на документирование всех действий в области защиты данных, а также постоянный внутренний контроль и внешний надзор.

Хотя с первого взгляда все вышеперечисленные аспекты и требования могут не без основания показаться трудновыполнимыми, самое главное – начать действовать, даже если это начало будет достаточно скромным и затронет отдельные компоненты, а не всю задачу в целом.

8. Глоссарий

Анонимные данные	Преамбула 26 GDPR определяет анонимную информацию как «информации, которая не относится к идентифицированному или идентифицируемому физическому лицу, а также в отношении персональных данных, предоставленных достаточно анонимно, чтобы субъект данных не мог быть идентифицированным».
Нарушение безопасности данных	Нарушение безопасности персональных данных означает нарушение безопасности, ведущее к случайному или незаконному уничтожению, потере, изменению, несанкционированному разглашению пересылаемых, хранимых или иным образом обрабатываемых персональных данных или к несанкционированному доступу к ним.
Контролер данных	Контролер данных – это любое физическое или юридическое лицо, государственный орган, учреждение или другой орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных; контролер или критерии для его определения могут быть установлены законодательством ЕС или государства-члена в случаях когда, цели и средства этой обработки определяются законодательством ЕС или государства-члена.
Обработка данных	Обработка данных означает любую операцию или совокупность операций, совершаемых с персональными данными с использованием средств автоматизации или без использования таких средств, включая сбор, запись, организацию, структурирование, накопление, хранение, адаптацию или изменение, загрузку, просмотр, использование, раскрытие посредством передачи, распространение или иной вид предоставления доступа, сопоставление или комбинирование, сокращение, удаление или уничтожение.

Процессор	Процессор – это физическое или юридическое лицо, государственный орган, учреждение или другой орган, который обрабатывает персональные данные от имени по поручению контролера.
Орган по защите данных	Орган по защите данных – это учрежденный правительством независимый государственный орган с соответствующими функциями и полномочиями.
Субъект данных	Субъект данных – это идентифицированное или идентифицируемое физическое лицо, к которому относятся персональные данные.
Персональные данные	Персональные данные – это любая информация, относящаяся к субъекту данных, то есть к идентифицированному или идентифицируемому физическому лицу; идентифицируемое физическое лицо – это лицо, которое можно прямо или косвенно идентифицировать, в частности, посредством ссылки на идентификатор, такой как имя, идентификационный номер, данные о местоположении, онлайновый идентификатор или один или несколько факторов, специфичных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности этого физического лица.
Псевдонимизация	Согласно пункту 3b статьи 4 GDPR псевдонимизация определяется как «обработка персональных данных таким образом, что персональные данные не могут быть больше отнесены к определенному субъекту данных без использования дополнительной информации, при условии, что такая дополнительная информация хранится отдельно и в отношении нее приняты технические и организационные меры, предотвращающие ее отнесение идентифицированному или идентифицируемому физическому лицу».

Всемирная организация здравоохранения

Европейское региональное бюро

Европейское региональное бюро ВОЗ

Всемирная организация здравоохранения (ВОЗ) – специализированное учреждение Организации Объединенных Наций, созданное в 1948 г., основная функция которого состоит в решении международных проблем здравоохранения и охраны здоровья населения. Европейское региональное бюро ВОЗ является одним из шести региональных бюро в различных частях земного шара, каждое из которых имеет свою собственную программу деятельности, направленную на решение конкретных проблем здравоохранения обслуживаемых ими стран.

Государства-члены

Австрия
Азербайджан
Албания
Андорра
Армения
Беларусь
Бельгия
Болгария
Босния и Герцеговина
Венгрия
Германия
Греция
Грузия
Дания
Израиль
Ирландия
Исландия
Испания
Италия
Казахстан
Кипр
Кыргызстан
Латвия
Литва
Люксембург
Мальта
Монако
Нидерланды
Норвегия
Польша
Португалия
Республика Молдова
Российская Федерация
Румыния
Сан-Марино
Северная Македония
Сербия
Словакия
Словения
Соединенное Королевство
Таджикистан
Туркменистан
Турция
Узбекистан
Украина
Финляндия
Франция
Хорватия
Черногория
Чехия
Швейцария
Швеция
Эстония

Всемирная организация здравоохранения
Европейское региональное бюро
UN City, Marmorvej 51
DK-2100 Copenhagen Ø, Denmark
Тел.: +45 45 33 70 00;
факс: +45 45 33 70 01
Эл. адрес: eurocontact@who.int
Веб-сайт: www.euro.who.int