Руководство по обеспечению безопасности использования пациентом логина и пароля от личного кабинета в программном продукте «ТОНУС ONLINE».

Термины и определения

Программный продукт «ТОНУС ONLINE» - это информационная система для оказания медицинской помощи с применением телемедицинских (информационных) технологий специалистами сети медицинских клиник «Тонус» (под сетью клиник понимаются медицинские клиники, содержащие в своем наименовании слово «ТОНУС» и в составе единоличного исполнительного органа и/или учредителей то же лицо, что и у Оператора информационной системы).

Оператор информационной системы - Общество с ограниченной ответственностью «Центр лучевой диагностики «ТОНУС ПРЕМИУМ», 603000, г. Нижний Новгород, ул. Большая Покровская, д. 62/5, тел./факс: (831) 411-13-13, info@tonus.nnov.ru.

Личный кабинет Пациента в программном продукте «ТОНУС ONLINE» - это персональная страница Пациента в программном продукте «ТОНУС ONLINE» (https://tonusnn.ru/), доступ к которой есть только у Пациента и/или его Законного представителя. Вход возможен с помощью авторизации.

Авторизация – это проведение процедуры подтверждения данных при входе в личный кабинет в программном продукте «ТОНУС ONLINE». Авторизация происходит по логину и паролю.

Логин – это имя пользователя, которое используется для авторизации в программном продукте «ТОНУС ONLINE».

Пароль – это уникальны набор букв и/или цифр, который необходим для доступа к личному кабинету в программном продукте «ТОНУС ONLINE».

Носитель логина и/или пароля - физический носитель определенной структуры (бумага, записная книжка, мобильный телефон, компьютер и т.п.), предназначенный для размещения на нем логина и/или пароля.

Компрометация логина и/или пароля - утрата доверия к тому, что используемые логин и/или пароль недоступны посторонним лицам или подозрение, что логин и/или пароль были временно доступны посторонним лицам. К событиям, связанным с компрометацией логина и/или пароля относятся (включая, но не ограничиваясь):

- физическая утрата носителя логина и/или пароля;
- потеря носителя логина и/или пароля с его последующим обнаружением;
- передача логина и/или пароля по открытым каналам связи;
- перехват логина и/или пароля вредоносным программным обеспечением;
- несанкционированный доступ постороннего лица к носителю логина и/или пароля;
- случаи, когда невозможно достоверно установить, что произошло с носителем логина и/или пароля (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);
- сознательная передача логина и/или пароля постороннему лицу;
- сознательная передача носителя логина и/или пароля постороннему лицу.

Несанкционированный доступ к информации - доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

1. Риски, связанные с использованием логина и пароля от личного кабинета Пациента в программном продукте «ТОНУС ONLINE»

К основным рискам относятся:

1.1. Несанкционированная авторизация в личном кабинете в программном продукте «ТОНУС ONLINE», которое может быть произведено в результате:

- компрометации логина и/или пароля;
- работы на техническом устройстве вредоносного программного обеспечения.

1.2. Негативные последствия, вызванные невозможностью использования логина и/или пароля в личном кабинете в программном продукте «ТОНУС ONLINE», обусловленной следующими событиями:

- уничтожение носителя логина и/или пароля;
- неисправность носителя логина и/или пароля;
- блокировка носителя логина и/или пароля;
- физическая утрата носителя логина и/или пароля.

2. Организация работ по обеспечению безопасности использования логина и пароля от личного кабинета Пациента в программном продукте «ТОНУС ONLINE»

Правом доступа к носителю логина и/или пароля должен обладать только Пациент или его Законный представитель.

3. Требования по размещению носителей логина и/или пароля.

При размещении носителей логина и/или пароля должны быть приняты меры по исключению несанкционированного доступа посторонних лиц.

4. Требования по защите от несанкционированного доступа к логину и/или паролю.

4.1. Запрещается:

- разглашать логин и/или пароль;
- оставлять без контроля носитель логина и/или пароля;
- разглашать логин и/или пароль с носителей логина и/или пароля или передавать сами носители логина и/или пароля лицам, к ним не допущенным, выводить логин и/или пароль с носителей логина и/или пароля на дисплей, принтер и т.п. иные средства отображения информации;

4.2. Необходимо регулярно устанавливать пакеты обновления безопасности операционной системы (Service Packs, Hot fix и т.п.), обновлять антивирусные базы.

4.3. Необходимо организовать и использовать комплекс мероприятий антивирусной защиты.

5. Действия при компрометации логина и/или пароля.

5.1. Пациент самостоятельно должен определить факт компрометации логина и/или пароля, оценить значение этого события.

5.2. При компрометации логина и/или пароля Пациент должен немедленно сообщить оператору информационной системы (программного продукта «ТОНУС ONLINE») о факте компрометации.

5.3. Информация о компрометации должна передаваться оператору информационной системы (программного продукта «ТОНУС ONLINE») способом, определенным в Дополнительном соглашении к Договору на оказание платных медицинских услуг.

5.4. По получении информации о компрометации логина и/или пароля оператор информационной системы (программного продукта «ТОНУС ONLINE») приостанавливает (блокирует) доступ к личном кабинету в программном продукте «ТОНУС ONLINE» до выяснения обстоятельств на личном визите Пациента в медицинскую клинику Оператора информационной системы.