Институт за онкологију и радиологију Србије
Пастерова 14, Београд, Србија
+381 11 2067 100
iors@ncrc.ac.rs www.ncrc.ac.rs

РЕПУБЛИКА СРБ
ИНСТИТУТ ЗА ОНКОЛОГИЈУ И РАДИОЛОГИ
Бр. 01-1/2023/3494-7
26 DEC 2023
БЕОГРАД, Пастерова 1

ПРОЦЕДУРА ЗА ПОСТУПАЊЕ, ОБРАДУ, СКЛАДИШТЕЊЕ И ПРЕНОС ПОДАТАКА

Ознака процедуре	**П.ДТЦ.08**
Верзија	01
Датум усвајања	08.03.2018./15.12.2023.
Аутор процедуре	Душица Гавриловић, маст мат Зорана Бизетић, маст мат
Посилац процедуре	Др сци. мед. др Ана Јовићевић
Процедуру одобрио	Доц. др Милан Жегарац

1.0 ДЕФИНИЦИЈЕ И СКРАЋЕНИЦЕ

ИОРС је Институт за онкологију и радиологију Србије;
ОЈ је Организациона јединица ИОРС-а;
ДЦ је Дата Центар ИОРС-а;

ИКТ систем је информационо-комуникациони систем ИОРС-а у смислу технолошко-организационе целине која обухвата:

1. електронске комуникационе мреже у смислу закона који уређује електронске комуникације;
2. уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада електронских података коришћењем рачунарског програма;
3. електронске податке који се похрањују, обрађују, претражују или преносе помоћу средстава из подтач. (1.) и (2.) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;
4. организациону структуру путем које се управља ИКТ системом;

ИС (информациони систем) је део ИКТ система ИОРС-а који је формализован и намењен планском прикупљању, складиштењу, обради, размени и испоруци информација од значаја за рад, тако да су информације доступне и употребљиве свима који су овлашћени да их користе;

Информациона безбедност представља скуп мера које омогућавају да електронски подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити тајност, интегритет, расположивост, аутентичност и непорецивост тих података, да би ИКТ систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;

Администратор ДЦ је запослени Дата центра коме је дозвољено администрирање ИКТ и/или ИС система.

Инжињер за ИТ безбедност је запослени Дата центра који се бави пословима информационе безбедности;

Корисник је запослени ИОРС-а који има приступ ИКТ систему ради обављања својих пословних активности;

Пословни подаци су подаци на које се односи Закон о заштити пословне тајне ("сл. Гласник рс", бр. 72/2011)

Интерни подаци су подаци медицинске документације пацијената ИОРС-а као и подаци на које се односи Закон о заштити података о личности ("сл. Гласник рс", бр. 97/2008, 104/2009 - др. Закон, 68/2012 - одлука ус и 107/2012);

Кориснички креденцијали су идентификатори Корисника помоћу којег је Кориснику омогућен приступ ИКТ или ИС системима ИОРС-а који садрже пословне и/или интерне податке (напр име и лозинка; картица; ПИН-код и сл.) Они служе за додељивање, ограничавање, измену или укидање права приступа ИКТ и ИС системима;

Захтев ДЦ - Захтев за услугом ДЦ;

База ИКТ ресурса и услуга ДЦ - електронска база евиденција ИКТ ресурса и услуга које Дата центар пружа у ИОРС-у;

Анонимизација података представља поступак конверзија података о личности у облик који онемогућава идентификацију личности;

Анонимизирани подаци су подаци о личности на основу којих се не може идентификовати о којој особи је реч;

Агрегарни подаци су подаци који нису изворни (подаци на којима је спроведена обрада података) и из којих се не може идентификовати особа/личност (напр сумарне табеле, графикони).

2.0 ПРЕДМЕТ

Овом процедуром утврђују се активности, носиоци активности и одговорности приликом поступања, обраде, преноса и складиштења пословних, интерних и јавних података ИКТ и ИС система ИОРС-а.

3.0 ПОДРУЧЈЕ ПРИМЕНЕ

Примењује се на све запослене у ИОРС-у.

4.0 ОДГОВОРНОСТИ

Сваки запослени је дужан да се понаша у складу са процедуром и у складу са својим задужењима ће сносити одговорност.

Обавеза руководиоца сваке организационе јединице ИОРС-а је да све запослене упозна са процедуром и све новозапослене, било да су у сталном или радном односу на одређено време.

За контролу спровођења процедуре одговорни су одговарајући руководиоци организационих јединица.

5.0 ОПИС ПРОЦЕДУРЕ

Сви подаци који се генеришу, складиште, преносе или обрађују у оквиру ИКТ система ИОРС-а представљају власништво ИОРСа и не смеју бити саопштени или на други начин учињени доступним трећим лицима (1) од стране Корисника без одговарајућих одобрења (у складу са изјавом о поверљивости и интерним актима); (2) од стране вендора, у складу са одговарајућим уговором.

5.1 Присуп пословним и/или интерним подацима

Приступ ИКТ или ИС који садрже пословне и/или интерне податке је омогућен запосленима помоћу корисничких налога, а у складу са радним задацима дефинисаним у Правилнику о организацији и систематизацији радних места ИОРС-а.

Додељивање права приступа се спроводи у складу са *Процедуром о правима приступа ИКТ сиситему*.

- ***Приступ подацима који су унутар ИС система***

Процедура приступа и обраде пословних и/или интерних података који се чувају у ИС системима ИОРС-а подразумева:

- пријављивање Корисника на ИС систем помоћу његових креденцијала за тај ИС;
- евиденцију пословних и/или интерних података у складу са процедурама ИОРС-а које се односе на рад Корисника;
- одјава Корисника из ИС система у случају било каквог напуштања радног места;
- одјава Корисника из ИС система и искључивање рачунара, по завршетку радног периода.

За едукацију из области познавања рада на рачунару одговоран је Корисник, док је за едукацију из области коришћења ИС одговоран непосредни руководилац ОЈ у којој запослени ради.

За тачност и безбедност унетих пословних и/или интерних података је одговоран Корисник.

- ***Приступ подацима који су ван ИС система***

Процедура приступа пословним и/или интерним подацима који се не чувају унутар ИС система, али се чувају у ИКТ систему ИОРС-а подразумева:

- пријављивање Корисника на ИКТ систем помоћу његових креденцијала;
- евиденцију пословних и/или интерних података у складу са процедурама ИОРС-а које се односе на рад Корисника;
- одјава из ИКТ система и искључивање рачунара по завршетку радног периода.

За едукацију из области познавања рада на рачунару као и за тачност и безбедност унетих пословних и/или интерних података је одговоран Корисник.

5.2 Измена пословних и/или интерних података и/или електронских докумената

Уколико постоји потреба за изменом пословних и/или интерних података и/или електронских документа ИС и Корисников налог дозвољава ту измену тада је он спроводи у складу са процедурама рада своје ОЈ.

Уколико Корисник нема право да мења пословне и/или интерне податке и/или електронска документа, тада он подноси захтев ДЦ у електронској и/или папирној форми, уз обавезну сагласност непосредног руководиоца ОЈ. У ДЦ се захтев ДЦ анализира и уколико измена утиче на рад више Корисника, тада тај захтев ДЦ мора имати и сагласност руководиоца који је надлежан за све Кориснике на чији рад може да утиче измена. Спроведена измена се евидентира у *Бази ИКТ ресурса и услуга ДЦ,* а Корисник се обавести да је захтев ДЦ реализован.

За измену пословних и/или интерних података и/или електронских документа који нису унутар ИС, надлежан је Корисник.

5.3 Обрада пословних и/или интерних података

- ***Стандардна обрада пословних и/или интерних података***

Стандардна обрада података подразумева употребу стандардних извештаја који су дефинисани у информационом систему. Стандардна обрада података је дозвољена правима дефинисаним у оквиру корисничког налога који је у складу са радним задацима Корисника, дефинисаним у Правилнику о организацији и систематизацији радних места ИОРС-а и са процедурама рада ОЈ.

- ***Нестандардна обрада пословних и/или интерних података***

У случају потребе за нестандардном обрадом пословних и/или интерних података, најпре се у ДЦ процењује да ли су потребни подаци из ИС.

Уколико је потребна обрада података који нису из ИС, у ДЦ се спроводи услуга, са евентуалном анонимизацијом. Спроведена обрада података се евидентира у *Бази ИКТ ресурса и услуга ДЦ,* а Корисник се обавести да је захтев ДЦ реализован.

Ако су потребни подаци из ИС, тада Корисник подноси захтев ДЦ у електронској и/или папирној форми са сагласношћу непосредног руководиоца ОЈ. Захтев ДЦ се анализира и ако је за његову реализацију потребно тада се: ангажује одговарајући вендор; спроводи се трансформација и се анонимизација података.

Спроведена измена се евидентира у *Бази ИКТ ресурса и услуга ДЦ,* а Корисник се обавести да је захтев ДЦ реализован.

5.3 Складиштење пословних и/или интерних података

Ако се подаци налазе на радним станицама, мобилним уређајима или преносним носачима података који су власништву ИОРС-а, за њихову обраду, складиштење и безбедност је задужен Корисник.

ИС системи врше аутоматско складиштење података и за њихову безбедност је задужен Инжињер за ИТ безбедност и/или одговарајући вендор.

5.4 Пренос пословних и/или интерних података

Пренос интерних и/или пословних података подлеже прописима о заштити података о личности и о пословној тајни те он може бити само за потребе обављања редовних радних задатака:

- аутоматски, путем рачунарске мреже и ИС ИОРС-а, за податке који су унутар ИС система;
- путем преносних носача података у складу са *Процедуром за управљање преносним носачима података;*
- путем службене електронске поште у складу са *Процедуром о безбедности у размени електронских порука;*
- путем WEB сајта ИОРС-а у складу са *Процедуром за ажурирање и администрирање WEB сајта* (за потребе: обавештавања пацијената и јавности о листама чекања; о финансијском извештају; јавним набавкама; конкурсима и др.)
- аутоматски, путем ВПН-а за потребе државних институција (Министарство здравља, РФЗО, трезор Народне банке, ...).

Уколико постоји потреба за преносом пословних и/или интерних података путем преносних носача података или службене електронске поште тада се она спроводи уз сагласност непосредног руководиоца ОЈ. Уколико је потребно податке послати (путем мејла) или их предати трећим лицима (предати преносни носач података на коме се подаци налазе), тада је потребно да:

- ИОРС има уговор са трећим лицима који у себи има клаузулу о поверљивости података.
- Подаци буду агрегарни или бар анонимизирани. Уколико би се анонимизацијом онемогућило прибављање важних података (нпр. ако се траже подаци о смрти) тада се спроводи нека од других методе заштите (нпр. шифровано отварање документа у прилогу) или размена података са криптозаштитом. У вези са тим, корисници се могу обратити Администратору ДЦ.

Уколико постоји потреба за преносом пословних и/или интерних података путем путем WEB сајта ИОРС-а тада се пре објављивања подаци анонимизирају.

5.5 Приступ, обрада, складиштење и пренос јавних података

Приступ јавним подацима имају сви запослени ИОРС-а. Обрада, складиштење и пренос јавних података је дозвољена.

Пренос осталих јавних података који се односе на ИОРС се спроводи у складу са *Процедуром за односе са јавношћу.*

Складиштење и пренос јавних података је дозвољена и на преносним носачима података под условом да су носачима података претходно прошли безбедоносну проверу од стране Инжењера за ИТ безбедност.

6.0 ВЕЗА СА ДРУГИМ ДОКУМЕНТИМА

Процедура је у вези са документима:

1. *Правилник о безбедности информационо-комуникационог система Института за онкологију и радиологију Србије*
2. *Процедуром о правима приступа ИКТ сиситему*
3. *Процедуром за управљање преносним носацима података*
4. *Процедуром о размени елетронских порука*
5. *Процедуром за односе са јавношћу*
6. *Процедуром за администрирање WEB сајта*
7. *Процедура за рад Дата центра*

7.0 ПРАВНИ ОСНОВ

- *Закон о информационој безбедности ("Сл. Гласник РС", бр. 6/2016)*
- *Закон о здравственој документацији и евиденцијама у области здравства ("Службени гласник РС", број 123 од 10. новембра 2014)*
- *Закон о заштити података о личности ("Сл. гласник РС", бр. 97/2008, 104/2009 - др. закон, 68/2012 - одлука УС и 107/2012)*
- *Правилник о анонимизацији података о личности (Број: 110-00-00011/2013 -01 од 15. 11. 2013; доступно на: https://www.poverenik.rs/sr/актуелни-акти/1706-правилник-о-анонимизацији-података-о-личности.html)*