Polityka ochrony danych osobowych „w pigułce”

**Instytut „Centrum Zdrowia Matki Polki”
w Łodzi**

LISTOPAD 2020

ODO Consulting

Wstęp

Polityka Ochrona danych osobowych „w pigułce” **stanowi wyciąg najistotniejszych zapisów zawartych w Polityce Ochrony Danych Osobowych oraz innych procedurach z zakresu danych osobowych obowiązujących u Administratora.**

Zakres podmiotowy stosowania niniejszego dokumentu obejmuje wszystkich pracowników lub współpracowników mających dostęp do danych osobowych. Polityka dotyczy również osób, które odbywają praktykę, staż lub wolontariat u Administratora.

Kwestię bezpieczengo korzystania z zasobów Instytutu można rozważać z dwóch punktów widzenia. Z punktu widzenia osoby, której dane mogą być przetwarzane, zwracamy przede wszystkim uwagę na konieczność zapewnienia tym danym bezpieczeństwa. Wyciek danych osobowych szczególnej kategorii dotyczących stanu zdrowia może prowadzić do poważnych konsekwencji. W takiej sytuacji w poważny i dotkliwy sposób może zostać naruszone nasze prawo do prywatności.

Z punktu widzenia Instytutu, który dane osobowe przetwarza, warto pamiętać o konsekwencjach związanych z przetwarzaniem danych osobowych w sposób niezgodny z prawem. RODO przewiduje dotkliwe kary pieniężne w przypadku naruszenia przepisów o ochronie danych osobowych oraz możliwość dochodzenia odszkodowania przez osoby, których dane zostały naruszone.

Najsłabszym ogniwem jest człowiek – nawet najlepsze systemy nie uchronią nas przed zagrożeniami, jeżeli nie będziemy przestrzegać podstawowych zasad bezpieczeństwa!

1. Postępowanie z dokumentacją papierową

1. Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe odpowiedzialne są osobowy upoważnione do przetwarzania danych osobowych oraz kierownicy właściwych komórek organizacyjnych.

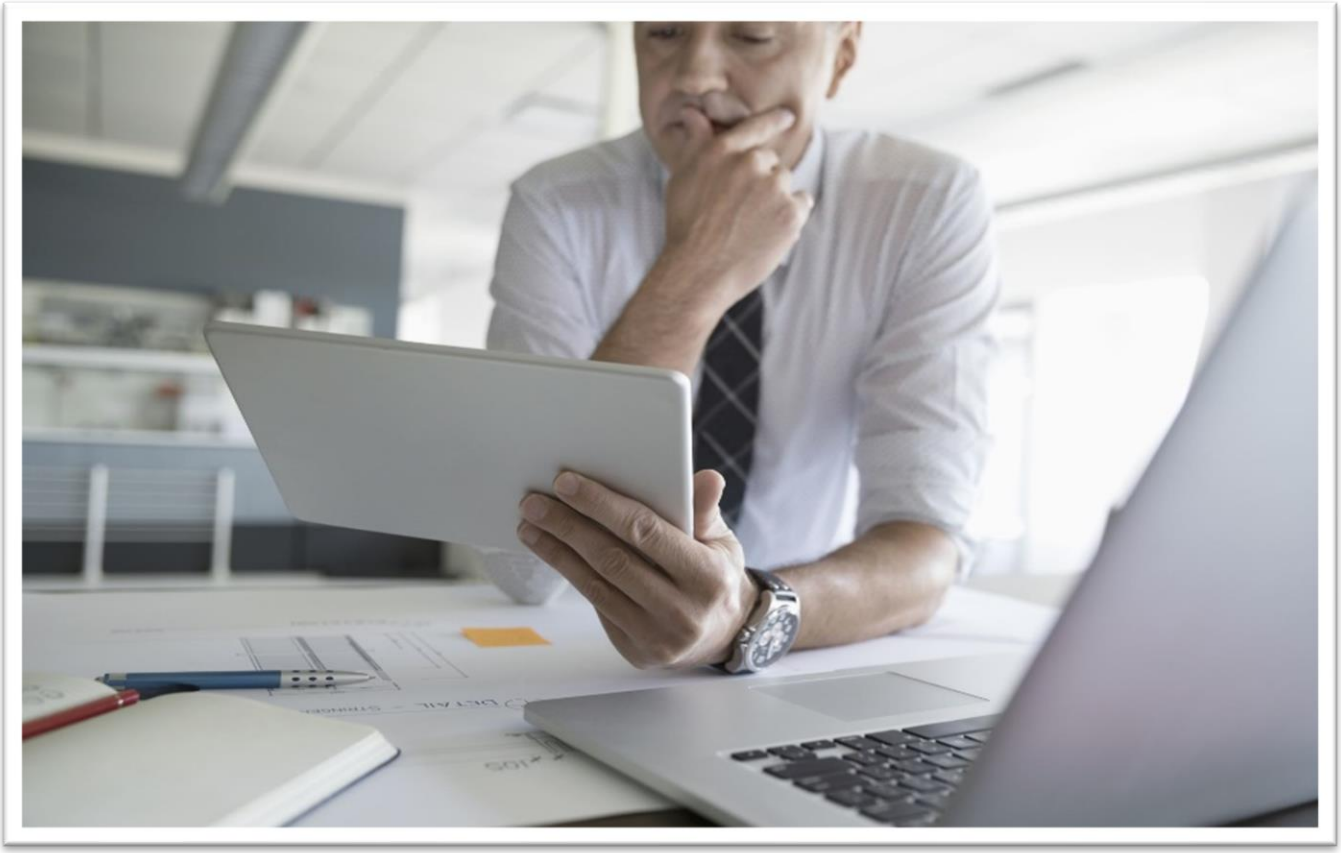
2. W przypadku konieczności przechowywania wydruków zawierających dane osobowe, należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.
3. Dokumenty z danymi osobowymi przechowuje się w archiwum lub w zabezpieczonych fizycznie pomieszczeniach, biurkach i szafach.
4. Pracownicy są zobowiązani do zabezpieczania dokumentów (np. zamykaniu dokumentów na klucz w szafach, biurkach, pomieszczeniach) przed dostępem osób nieuprawnionych podczas swojej nieobecności w pomieszczeniach lub po zakończeniu pracy, przed kradzieżą lub wglądem osób nieuprawnionych.
5. Zabrania się pozostawiania wydruków oraz ksero na drukarkach, skanerach i kserokopiarkach bez nadzoru.
6. Pracownicy zobowiązani są do przewożenia dokumentów w sposób zapobiegający ich kradzieży, zagubieniu lub utracie.
7. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie (w niszczarce).

2. Zasady korzystania ze sprzętu i oprogramowania

1. Pracownik ma obowiązek natychmiastowego zgłoszenia zagubienia, utraty lub zniszczenia powierzonego mu sprzętu.
2. Użytkownicy nie mają prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez osoby upoważnione.
3. Pracownik jest zobowiązany do:
   a. niekorzystania z oprogramowania komputerowego innego niż oprogramowanie zainstalowane przez Dział IT, w tym niedokonywania samodzielnej instalacji innego oprogramowania bez wiedzy Działu IT;
   b. niekorzystania ze sprzętu i oprogramowania w celach prywatnych, w szczególności poprzez prowadzenie korespondencji e-mail niezwiązanej ze świadczeniem pracy, poprzez korzystanie z komunikatorów, portali społecznościowych, witryn www, innych niż konieczne do wykonywania obowiązków pracowniczych;
   c. niekorzystania z oprogramowania w sposób mogący naruszyć prawa osób trzecich, w tym niekopiowania i nierozpowszechniania oprogramowania;
   d. niezwłocznego udostępniania administratorowi, na każde żądanie, sprzętu i oprogramowania celem umożliwienia wykonania kontroli przez Administratora.
4. Bezwzględnie zabronione jest wykorzystywanie sprzętu lub oprogramowania w celach niezgodnych z prawem lub zasadami obowiązującymi u administratora, a w szczególności w celach:
   a. korzystania z treści pornograficznych;
   b. naruszania praw autorskich (nielegalnego pobierania bądź udostępniania plików);
   c. infekowania sieci komputerowej wirusami pobieranymi z plikami z Internetu;
   d. korzystania ze służbowej poczty elektronicznej w sprawach prywatnych.

Pracownik może korzystać ze sprzętu i oprogramowania wyłącznie w celu wykonywania powierzonych obowiązków!

3. Zasady użytkowania przenośnego sprzętu IT



1. Zabrania się pozostawiania urządzeń przenośnych w miejscach ogólnodostępnych bez opieki.
2. Należy blokować dostęp do systemu przy każdorazowym oddaleniu się od niego.
3. Należy ustawiać ekran w sposób uniemożliwiający odczyt przez osoby postronne lub stosować nakładki prywatyzujące.
4. Nie należy dokonywać samodzielnych napraw i modernizacji sprzętu komputerowego, a także ingerować w oprogramowanie i ustawienia systemu operacyjnego bez zgody pracowników Działu IT.
5. Użytkownik przed wyłączeniem stacji roboczej i opuszczeniem stanowiska pracy powinien wylogować się z systemu informatycznego oraz sprawdzić, czy nie zostały pozostawione niezabezpieczone elektroniczne nośniki zawierające dane osobowe.
6. Dane osobowe w postaci elektronicznej – zapisywane na dyskietkach, dyskach magnetooptycznych czy dyskach twardych nie są wynoszone poza siedzibę administratora. Nie dotyczy to komputerów przenośnych, które mogą być wynoszone poza siedzibę administratora.

7. Po zakończeniu pracy przez użytkowników systemu wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych.

4. Zasady bezpieczengo korzystania z Internetu

1. Bezwzględnie zabronione jest wykorzystywanie sprzętu lub oprogramowania w celach niezgodnych z prawem lub zasadami obowiązującymi u administratora, a w szczególności w celach:
   a. korzystania z treści pornograficznych;
   b. naruszania praw autorskich (nielegalnego pobierania bądź udostępniania plików);
   c. infekowania sieci komputerowej wirusami pobieranymi z plikami z Internetu;

d. korzystania ze służbowej poczty elektronicznej w sprawach prywatnych.

2. Zabrania się pobierania z Internetu plików nieznanego pochodzenia.
3. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym.
4. **Użytkownik jest obowiązany zawiadomić Dział IT o pojawiających się komunikatach wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.**
5. Nie należy w opcjach przeglądarki włączać autouzupełniania formularzy oraz zapamiętywania haseł.

5. Zasady korzystania z poczty elektronicznej

1. Zabronione jest:
   a. Wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu).
   b. Otwieranie załączników od nieznanych nadawców, w szczególności z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.
   c. Czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika (nie udostępniaj swojego loginu i hasła innym pracownikom).

   d. Posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych.
   e. Wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej, niż wynikającej z potrzeb Instytutu lub do poszukiwania dodatkowego zatrudnienia.
2. W przypadku konieczności dokonania wysyłki korespondencji masowej poza Instytut, wysyłający powinien ukryć listę odbiorców (pole BCC lub UDW).
3. Dokonując wysyłki korespondencji z załącznikiem zawierającym w swojej treści dane osobowe, poufne informacje lub informacje mogące stanowić tajemnicę przedsiębiorstwa należy opatrzyć takie dokument hasłem autoryzacyjnym. Hasło do pliku powinno zostać przesłane za pomocą innej formy komunikacji np. krótkiej wiadomości tekstowej SMS.

PAMIĘTAJMY!

Administrator **NIGDY** nie prosi o potwierdzenie naszych poufnych danych w e-mailach, smsach czy w trakcie rozmów telefonicznych. W szczególności nigdy nie zażąda od nas podania hasła do konta **– hasło jest znane tylko i wyłącznie nam**.

Administrator nie wysyła także: e-maili z linkami kierującymi do strony do zalogowania się na konto internetowe, smsów z odsyłaczami do logowania, aplikacji lub certyfikatów bezpieczeństwa. Jeżeli otrzymałeś taką wiadomość, to znaczy, że ktoś – z pewnością **NIE** administrator – próbuje zainfekować Twoje urządzenie złośliwym oprogramowaniem.

6. Polityka haseł

Niebezpieczeństwa, jakie może nieść wyciek haseł do danego systemu, to m.in. możliwość uzyskania nieautoryzowanego dostępu do naszego systemu, co może skutkować dokonaniem nieautoryzowanej zmiany w dokumentacji (np. medycznej, kadrowej, płacowej) co może nieść duże zagrożenie dla zdrowia i życia naszych pacjentów, nieautoryzowany dostęp może również skutkować kradzieżą danych – co także wiąże się możliwością wystąpienia wielu negatywnych daleko idących skutków. Poniżej przedstawiamy podstawowe zasady polityki haseł.

1. Zabronione jest udostępnianie przez użytkownika swojego identyfikatora i hasła innym osobom, a także korzystanie z identyfikatora i hasła innego użytkownika. Zabrania się również przechowywania haseł w miejscach dostępnych innym osobom, np. pod klawiaturą, na monitorze lub w niezabezpieczonej szafce.
2. Hasło należy wprowadzać do systemu informatycznego w sposób, który uniemożliwia innym osobom jego poznanie.
3. W sytuacji, gdy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do samodzielnej zmiany hasła i powiadomienia o tym incydencie Działu IT.
4. Hasło powinno składać się z zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę itp.), ani jego imieniem lub nazwiskiem.
5. Hasło użytkownika powinno być zmienianie nie rzadziej niż co 30 dni.
6. Niedozwolone jest stosowanie haseł, którymi użytkownik posługiwał się uprzednio w okresie minionego roku.
7. Kombinacja hasła **nie powinna zwierać ogólnie dostępnych informacji o użytkowniku**, np. imienia i nazwiska, numeru telefonu, numeru rejestracyjnego samochodu, marki samochodu lub przewidywanych sekwencji z klawiatury (np.: „QWERTY” i „12345” itp.).

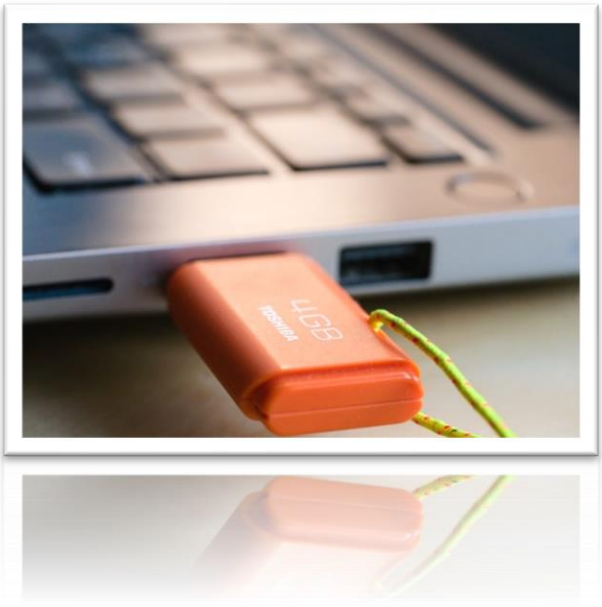
7. Rozpoczęcie, zawieszenie i zakończenie pracy

1. **Rozpoczęcie pracy**:
   a. Po włączeniu stacji roboczej użytkownik podaje własny login i hasło.
   b. Dostęp do danych możliwy jest jedynie po dokonaniu uwierzytelnienia użytkownika.
   c. W przypadku niemożności zalogowania się do systemu pracownik powinien niezwłocznie powiadomić o tym fakcie Dział IT.
   d. W przypadku zablokowania konta lub utraty hasła pracownik powinien zgłosić się do Działu IT celem otrzymania nowego jednorazowego hasła do systemu.
2. **Zawieszenie pracy:**
   a. Niedopuszczalne jest pozostawienie odblokowanego komputera w miejscu dostępnym dla osób postronnych.
   b. W przypadku braku aktywności użytkownika na komputerze przez czas dłuższy niż 10 minut następuję automatyczne włączenie wygaszacza ekranu oraz zablokowanie komputera.

c. Jeżeli pozostawienie włączonego komputera jest konieczne ze względu na specyfikę przetwarzanych danych, pracownik jest zobowiązany do jego zablokowania.

3. **Zakończenie pracy:**
   a. Po zakończeniu pracy należy wylogować się z systemu lub wyłączyć komputer kończąc pracę pracownik zobowiązany jest zabezpieczyć stanowisko pracy, wszelką dokumentację oraz inne nośniki danych, na których znajdują się dane, należy przechowywać w sposób uniemożliwiający dostęp osobom nieupoważnionym (np. szafka zamykana na klucz).

8. Postępowanie z elektroniczymi nośnikami zawierającymi dane osobowe



1. Elektroniczne nośniki danych (np. pendrive, płyty CD/DVD/BR, dyski twarde) są przechowywane w sposób uniemożliwiający dostęp do nich osób nieuprawnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).
2. Dane osobowe w postaci elektronicznej – zapisywane na dyskietkach, dyskach magnetooptycznych czy dyskach twardych nie są wynoszone poza siedzibę administratora. Nie dotyczy to komputerów przenośnych, które mogą być wynoszone poza siedzibę administratora.
3. Po zakończeniu pracy przez użytkowników systemu wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych.
4. Użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania danych osobowych z nośników informacji po ustaniu powodu ich przechowywania.
5. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób mechaniczny uniemożliwiający ich odczytanie.

6. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych.
7. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych.

W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego, użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na swoim komputerze.

9. Zapewnienie poufności danych osobowych

1. Pracownik zobowiązany jest do zachowania w tajemnicy danych osobowych, do których ma lub będzie miał dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych lub zadań zleconych przez pracodawcę.
2. Pracownik zobowiązany jest do niewykorzystywania danych osobowych w celach pozasłużbowych bądź niezgodnych ze zleceniem.
3. Pracownik zobowiązany jest do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych.

Pamiętajmy!

Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieuprawnionym.

10. Udzielanie informacji dotyczących stanu zdrowia

1. Osoby udzielające świadczeń zdrowotnych oraz osoby uczestniczące w procesie udzielania świadczeń zdrowotnych są zobowiązane do zachowania w tajemnicy wszelkich informacji związanych z pacjentem, w szczególności informacji dotyczących stanu zdrowia pacjenta. Obowiązek zachowania w tajemnicy informacji związanych z pacjentem obowiązuje również po śmierci pacjenta.
2. **Obowiązku zachowania w tajemnicy nie stosuje się gdy:**
   a. pacjent lub jego przedstawiciel ustawowy wyraża zgodę na ujawnienie tajemnicy;
   b. zachodzi potrzeba przekazania niezbędnych informacji o pacjencie związanych z udzielaniem świadczeń zdrowotnych innym osobom wykonującym zawód medyczny, uczestniczącym w udzielaniu tych świadczeń,
   c. o zwolnieniu z tajemnicy stanowią przepisy rangi ustawowej.

   Obowiązku zachowania w tajemnicy nie stosuje się również do postępowania przed wojewódzką komisją do spraw orzekania o zdarzeniach medycznych.
3. Tożsamość osoby żądającej udzielenia informacji związanej z pacjentem należy ustalić na podstawie dokumentu potwierdzającego tożsamość, np. dowód osobisty lub paszport.
4. Osoba wykonująca zawód medyczny ma obowiązek udzielania pacjentowi, w tym pacjentowi małoletniemu, który ukończył 16 lat przystępnej informacji o stanie zdrowia, rozpoznaniu, proponowanych oraz możliwych metodach diagnostycznych, leczniczych, dających się przewidzieć następstwach ich zastosowania albo zaniechania, wynikach leczenia oraz rokowaniu, w zakresie udzielanych przez tę osobę świadczeń zdrowotnych oraz zgodnie z posiadanymi przez nią uprawnieniami. Proces diagnostyczny lub leczniczy, w miarę uzyskiwania nowych danych lub badań, może być modyfikowany.

5. Pacjent małoletni, który nie ukończył 16 lat, ma prawo do uzyskania od osoby wykonującej zawód medyczny informacji w zakresie i formie potrzebnej do prawidłowego przebiegu procesu diagnostycznego lub terapeutycznego.

6. W sytuacjach wyjątkowych, jeżeli rokowanie jest niepomyślne dla pacjenta, lekarz może ograniczyć informację o stanie zdrowia i o rokowaniu, jeżeli według oceny lekarza przemawia za tym dobro pacjenta. W takich przypadkach lekarz informuje przedstawiciela ustawowego pacjenta lub osobę upoważnioną przez pacjenta. Na żądanie pacjenta lekarz ma jednak obowiązek udzielić mu żądanej informacji.
7. Upoważnienie do uzyskiwania informacji o stanie pacjenta dla osoby wskazanej przez pacjenta ważne jest do chwili jego odwołania. Jeżeli upoważnienie nie zostało odwołane, upoważnienie obowiązuje również po śmierci pacjenta. Upoważnienie uprawnia do pozyskiwania informacji związanej z pacjentem tylko osobie upoważnionej przez pacjenta i nie uprawnia osoby upoważnionej do wydawania dalszych pełnomocnictw w zakresie udzielania informacji o pacjencie innym osobom.

Udzielanie informacji telefonicznie, jak identyfikować rozmówcę?

1. Personel medyczny **nie jest uprawniony do udzielania informacji związanych z pacjentem telefonicznie, chyba że jest w stanie zidentyfikować rozmówcę.**
2. Sposoby identyfikacji rozmówcy:
    a. Zadanie pytań dot. pacjenta, na które personel powinien otrzymać prawidłowe odpowiedzi. Przykłady pytań:
        i. Jaki jest numer PESEL pacjenta lub jaka jest data urodzenia pacjenta,
        ii. Jaki jest dokładny adres zamieszkania pacjenta,
        iii. Jakie są imiona rodziców pacjenta.
    b. Wykonanie połączenia na numer wskazany w treści zgody na udzielanie informacji o stanie zdrowia pacjenta.
    c. Podanie, wcześniej ustalonego pomiędzy rozmówcą a personelem, hasła.

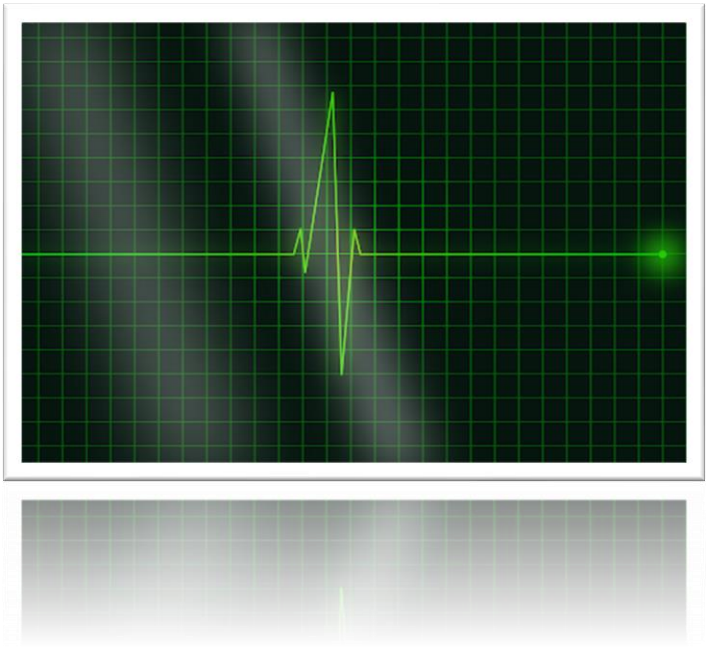
d. W przypadku osób pytających o dostępność wyników badań, personel może udzielić informacji czy badania są dostępne po podaniu przez rozmówcę co najmniej:
    i. imienia i nazwiska,
    ii. numeru PESEL,
    iii. rodzaju badania lub daty wykonania badania.

Udzielanie informacji o pacjencie małoletnim

1. Osobą uprawnioną do uzyskania informacji o stanie zdrowia pacjenta małoletniego jest pacjent, przedstawiciel ustawowy pacjenta, lub osoba wskazana przez przedstawiciela ustawowego pacjenta.
2. Rodzice są przedstawicielami ustawowymi dziecka pozostającego pod ich władzą rodzicielską. Jeżeli dziecko pozostaje pod władzą rodzicielską obojga rodziców, każde z nich może samodzielnie żądać udzielenia informacji związanej z małoletnim pacjentem.

W przypadku, gdy jedno z rodziców przedstawi postanowienie sądu, z którego wynika, że drugi z rodziców jest pozbawiony władzy rodzicielskiej, należy odnotować ten fakt w dokumentacji medycznej oraz systemie informatycznym HIS (zaleca się odnotowanie sygnatury decyzji sądu, zabrania się włączania do dokumentacji medycznej postanowienia sądu o pozbawieniu władzy rodzicielskiej). Osobie pozbawionej władzy rodzicielskiej nie udziela się żadnych informacji związanej z małoletnim pacjentem.

Udzielanie informacji po zgonie pacjenta



1. Osoba wykonująca zawód medyczny, jest zobowiązana do zachowania w tajemnicy informacji związanych z pacjentem również po śmierci pacjenta, chyba że zgodę na ujawnienie tajemnicy wyrazi osoba bliska i nie sprzeciwi się temu inna osoba bliska. Osoba bliska wyrażająca zgodę na ujawnienie tajemnicy może określić zakres jej ujawnienia. W tym celu osoba bliska zobowiązana jest złożyć oświadczenie dotyczące ujawnienia informacji związanej z pacjentem. Oświadczenie należy załączyć do dokumentacji medycznej pacjenta.
2. Zwolnienia z tajemnicy nie stosuje się, jeżeli ujawnieniu tajemnicy po śmierci sprzeciwił się pacjent za życia. Przed wyrażeniem sprzeciwu pracownik jest zobowiązany do udzielenia pacjentowi informacji o skutkach złożenia sprzeciwu. Sprzeciw dołącza się do dokumentacji medycznej pacjenta.
3. W przypadku uzasadnionych wątpliwości, czy osoba występująca o ujawnienie tajemnicy lub sprzeciwiająca się jej ujawnieniu jest osobą bliską, osoba wykonująca zawód medyczny może wystąpić z wnioskiem do sądu. Sąd, wyrażając zgodę na ujawnienie tajemnicy może określić zakres jej ujawnienia.

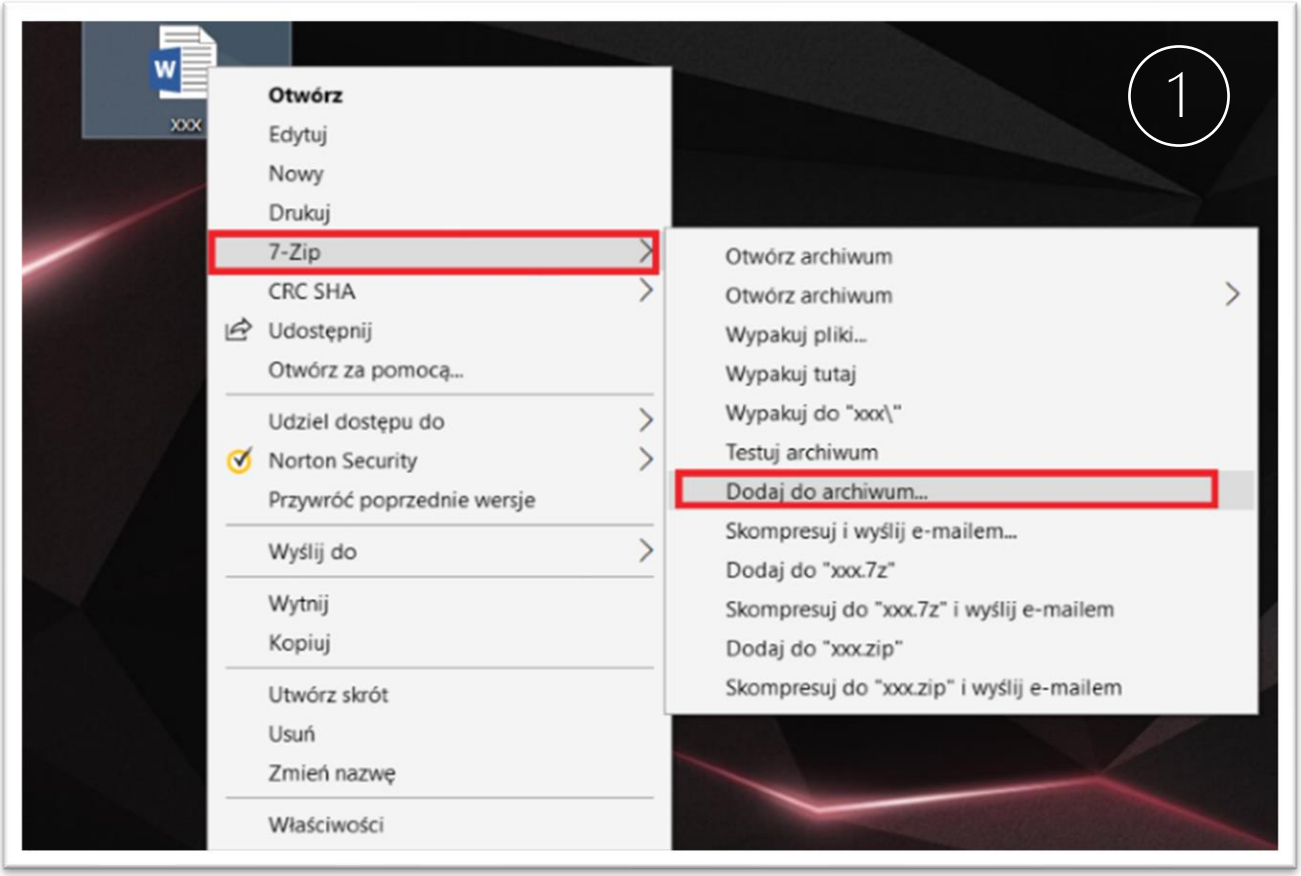
11. Przesyłanie wyników badań drogą elektroniczną. Co należy wiedzieć?

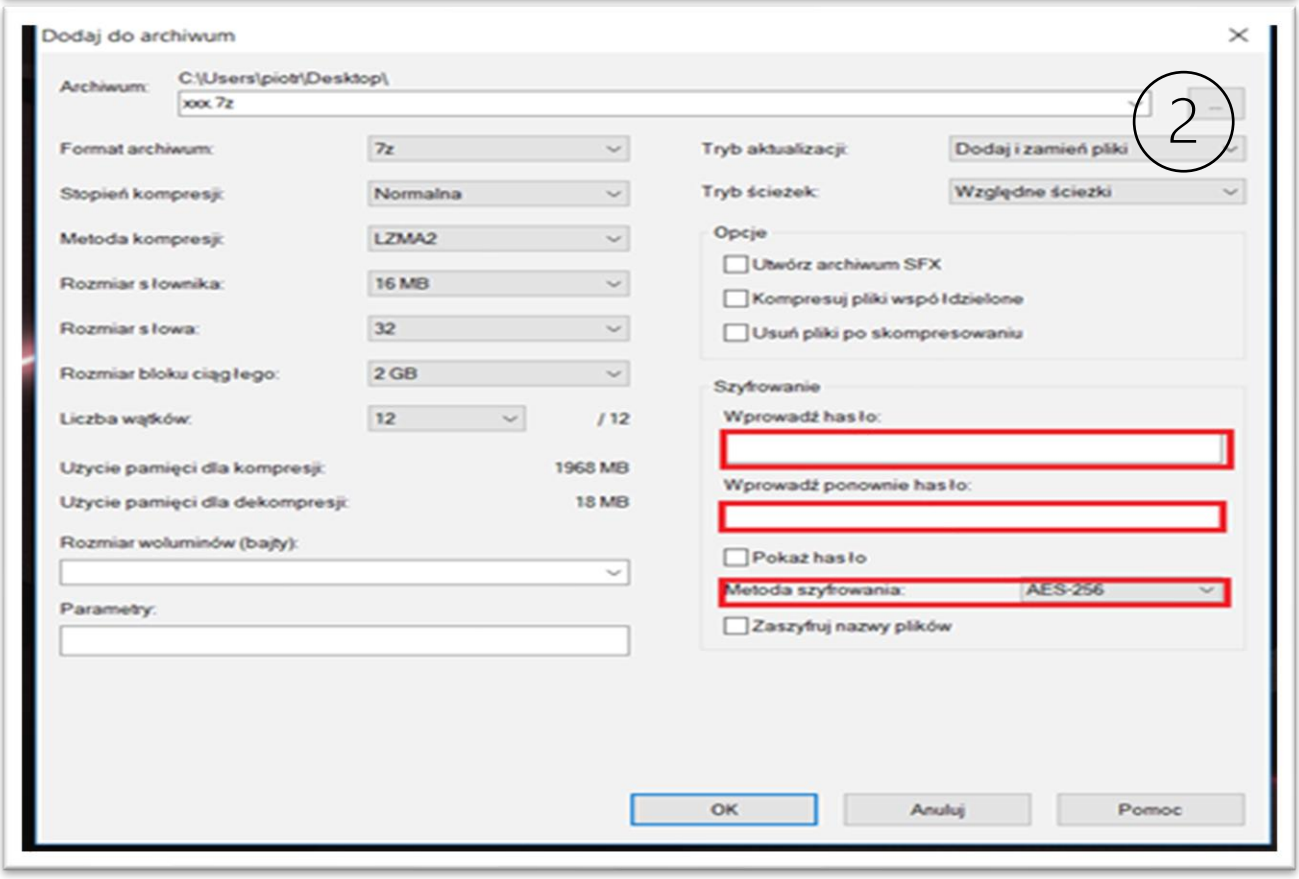
1. Należy zweryfikować czy pacjent wyraził zgodę na przesyłanie wyników badań/dokumentacji medycznej drogą elektroniczną.
2. W przypadku przesyłania wyników badań/dokumentacji medycznej drogą elektroniczną należy wysyłać pliki zaszyfrowane/spakowane (np. programem 7 zip, winzipem, winrarem) i zabezpieczone hasłem dostępu. Hasło powinno być przesłane do odbiorcy odrębnym kanałem komunikacji (np. SMS-em).
3. W przypadku zaistnienia przeszkód technicznych lub formalnych uniemożliwiających przesyłanie korespondencji drogą elektroniczną należy wysłać korespondencję w formie papierowej (przekazując dane drogą pocztową zaleca się, by wysyłać je spakowane w dwie koperty, listem poleconym za potwierdzeniem odbioru).

Instrukcja szyfrowania plików

1. Dokument, który chcemy zaszyfrować należy kliknąć prawym przyciskiem myszy.
2. Z menu należy wybrać kolejno opcję „7-zip”, a następnie „Dodaj do archiwum”. Po kliknięciu opcji „Dodaj do archiwum” pojawi się nowe okno.
3. W polu „Wprowadź hasło” należy wpisać ustalone hasło, a następnie ponowić jego wpisanie w polu „Wprowadź ponownie hasło”.
4. Następnie „Metoda Szyfrowania”. Należy upewnić się, że wybrana metoda to AES-256. Jeśli nie, to należy rozwinąć menu obok „Metody Szyfrowania” i wybrać metodę AES-256.
5. Należy kliknąć OK u dołu okna. Plik został zaszyfrowany.

Instrukcja graficzna





12. Zgłaszanie incydentów

1. Każdy pracownik, w przypadku stwierdzenia zagrożenia lub podejrzenia naruszenia zasad ochrony danych osobowych, zobowiązany jest do niezwłocznego zgłoszenia o ww. okolicznościach bezpośredniemu przełożonemu lub pracownikowi Działu IT. Bezpośredni przełożony lub pracownik Działu IT w przypadku powzięcia powyższej informacji zobowiązany jest do jej niezwłocznego przekazania Inspektorowi Ochrony Danych. Zgłoszenia można dokonać za pomocą formularza zgłoszenia zdarzenia, który stanowi załącznik do Polityki Ochrony Danych Osobowych.
2. W przypadku stwierdzenia poważnego incydentu lub powzięcia uzasadnionej informacji o podejrzeniu poważnego naruszenia zasad ochrony danych osobowych, Inspektor informuje Administratora o konieczności zgłoszenie naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
3. W przypadku stwierdzenia poważnego incydentu lub powzięcia uzasadnionej informacji o podejrzeniu poważnego naruszenia zasad ochrony danych osobowych Inspektor ma prawo przeprowadzić audyt doraźny.

Rodzaj najczęściej występujących zagrożeń bezpieczeństwa danych osobowych to :

a) niewłaściwe zabezpieczenie urządzeń, dokumentów oraz oprogramowania IT przed kradzieżą, zniszczeniem lub utratą danych osobowych;

b) wydanie osobie nieuprawnionej np. wyników badań, karty informacyjnej z leczenia szpitalnego, kopii dokumentacji medycznej;

c) nieprzestrzeganie przyjętych zasad ochrony danych osobowych przez upoważnione osoby.

13. Odpowiedzialność

Administrator za naruszenie ochrony danych osobowych może ponieść odpowiedzialność cywilną zgodnie z art. 82 RODO lub odpowiedzialność administracyjną na podstawie wskazanej w art. 83 lub 84 RODO.

- Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony może ponieść odpowiedzialność karną przewidzianą w art. 107 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.
- Podmiot przetwarzający za naruszenie ochrony danych osobowych może ponieść odpowiedzialność cywilną zgodnie z art. 82 RODO lub odpowiedzialność administracyjną na podstawie wskazanej w art. 83 i 84 RODO.
- Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony może ponieść odpowiedzialność karną przewidzianą w art. 107 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Odpowiedzialność pracownicza

Osoba upoważniona za naruszenie ochrony danych osobowych może ponieść odpowiednio odpowiedzialność wskazaną w art. 52 lub 108 kodeksu pracy albo odpowiedzialność kontraktową przewidzianą w art. 471 kodeksu cywilnego. Osoba upoważniona może także ponieść odpowiedzialność karną przewidzianą w art. 266 kodeksu karnego. **Przypadki nieuzasadnionego zaniechania obowiązków wynikających z Polityki ochrony danych osobowych potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.** Wobec osoby, która w przypadku wykrycia incydentu lub uzasadnionego podejrzenia powstania incydentu nie podjęła działania określonego w Polityce ochrony danych osobowych, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie udokumentowała takiego przypadku, możne zostać wszczęte postępowanie dyscyplinarne.

Kara dyscyplinarna nałożona na osobę uchylającą się od powiadomienia, o którym mowa powyżej, nie wyklucza odpowiedzialności karnej tej osoby oraz możliwości kierowania wobec takiej osoby roszczeń cywilnych przez administratora o zrekompensowanie poniesionych strat.