## Zestawienie zdarzeń najczęściej występujących w podmiotach medycznych kwalifikowanych, jako naruszenie ochrony danych osobowych.

Przykłady zdarzeń, kwalifikowanych, jako naruszenie ochrony danych osobowych występujące w realiach służby zdrowia, w podmiotach medycznych. Zachęcam do zapoznania się z niniejszą listą, albowiem przedstawione przykłady pokazują dobitnie, iż zdarzenia będące naruszeniem ochrony danych osobowych, to nie zawsze tylko efekt działań atakujących, hakerów, ale to również pokaźna grupa zdarzeń, które powstają w związku z działaniami albo zaniechaniami personelu jednostki.

- **[Kradzieże sprzętu komputerowego**] W realiach podmiotów medycznych spotkać możemy się ze zjawiskiem kradzieży sprzętu komputerowego, w tym komputerów przenośnych (laptopów), na których zapisane zostały dane – jednak ich nośniki nie zostały zaszyfrowane, bądź które zawierają zapamiętane hasła dostępowe do poszczególnych elementów systemu teleinformatycznego podmiotu. W realiach medycznych kradzieży nie należy ograniczać tylko do zdarzeń polegających na włamaniu się do danego pomieszczenia pod nieobecność personelu. Kradzieże zdarzają się także w tych jednostkach które udzielają świadczeń całodobowo, gdzie praktycznie przez cały czas personel w nich zatrudniony przebywa na miejscu, pomimo jednak tego, do takich zdarzeń dochodzi. Nie należy wykluczać także ewentualności, w której sprawcą kradzieży może okazać się sam pacjent, bądź osoby odwiedzające. Warto także zwrócić uwagę na możliwość wystąpienia tego zjawiska kradzież, w odniesieniu do sprzętu, jaki przekazany został pracownikowi w związku z wykonywaniem przez niego pracy zdalnej w uzgodnionym miejscu. W takiej sytuacji, kiedy dochodzi do kradzieży np. laptopa z mieszkania pracownika, również mamy do czynienia ze zdarzeniem, które należy ocenić pod kątem możliwości wystąpienia naruszenia ochrony danych osobowych u administratora danych osobowych.
- **[Udostępnianie dokumentacji medycznej]** Niestety to grupa zdarzeń, która tworzy najliczniejszy katalog naruszeń ochrony danych w służbie zdrowia. Na skutek braku znajomości przepisów, błędów, braku wiedzy na temat obowiązujących procedur w jednostce, a nawet na skutek braku takich wewnętrznych regulacji, dochodzi do zdarzeń polegających na udostępnianiu danych zawartych w dokumentacji medycznej pacjentów innym osobom nieuprawnionym. Uwaga jednak do tej kategorii naruszeń zaliczymy także udostępnienia zrealizowane w sposób nieuprawniony na rzecz innych podmiotów. Nie należy także zapominać o tym, iż pomyłka, błąd również potrafi doprowadzić do tego rodzaju zdarzenia.
- **[Udostępnianie wyników badań osobom nieuprawnionym]** Świadomy jestem tego, iż ten przypadek można byłoby przypisać do grupy zdarzeń z poprzedniego przykładu, jednak z uwagi na fakt, iż odnosi się on do tej części dokumentacji medycznej, która często zawiera kluczowe informacje dla pacjentów, informacje, które często posiadają status kluczowych dla życia i zdrowia pacjenta, mają miejsce zdarzenia, w których to udostępnienie realizowane może być pod presją czasu, czy presją osób. Należy mieć bowiem świadomość, iż po taką dokumentację mogą zwrócić się nie tylko osoby upoważnione przez pacjenta, czy jego przedstawiciele ustawowi, ale mogą to być także osoby bliskie, lub nawet osoby trzecie zainteresowane wynikiem takiego badania. Tego rodzaju presja generować może skłonności do popełniania błędów przez personel udostępniający dokumentację medyczną w postaci wyników. Naturalnie dodatkowe zagrożenie generowane jest w związku z wykorzystywaniem kanałów komunikacji elektronicznej.
- **[Błąd w adresowaniu korespondencji]** Tego typu zdarzenia występują najczęściej w pionach administracyjnych, odpowiedzialnych za przygotowywanie korespondencji do wysyłki. Należy jednak pamiętać, iż w przypadku korespondencji email tego typu zdarzenie również może

wystąpić, co oznacza, na każdym stanowisku prowadzącym komunikację elektroniczną, może ono wystąpić. Należy sobie uświadomić także fakt, iż dostarczenie korespondencji do osoby nieuprawnionej, może stanowić następstwo, za które jednostka nie ponosi do końca odpowiedzialności np. pacjent podał błędny adres email, bądź nie zaktualizował swoich danych korespondencyjnych. Niestety nie zwalnia to podmiotu medycznego, jako administratora danych osobowych z obowiązku podejmowania stosownych działań na gruncie RODO. Aby zapobiegać tego typu zdarzeniom, warto wprowadzić obowiązkowe szyfrowanie korespondencji email wraz z przekazywaniem hasła dostępowego do archiwum drogą alternatywną np. przez SMS.

- **[Błąd przy załączaniu dokumentacji do wysyłki]** Ponownie błąd, presja czasu, ale najczęściej niedbałość, stanowią przyczyny takiego stanu rzeczy, w którym do właściwego adresata kierowana jest większa ilość dokumentów niż wymagane. Uwaga takie zjawisko wystąpić może nie tylko w przypadku wysyłki tradycyjnej za pośrednictwem operatora pocztowego, czy firmy kurierskiej, takie zjawisko może wystąpić także przy prowadzeniu korespondencji email. Co więcej, takie zdarzenie może wystąpić nie tylko w sytuacji, kiedy dokumentacja przesyłana jest do pacjenta wnioskującego, bądź do osoby przez niego upoważnionej, albo do jego przedstawiciela ustawowego, często takie zdarzenia mają miejsce w przypadku wysyłek realizowanych do innych organów i podmiotów np. sąd, prokuratura, ZUS.
- **[Wykorzystywanie bezy pacjentów do innych celów]** Niestety również i tego typu zdarzenia mają miejsce. Chodzi o sytuacje, w których pracownicy posiadający dostęp do zasobów bazodanowych podmiotu medycznego, wykorzystują go do innych celów, aniżeli cele określone przez administratora danych osobowych np. na podstawie tak pozyskanych danych zawierają fikcyjne umowy ubezpieczenia, jako agenci ubezpieczeniowi, przekazują informacje do podmiotów ubezpieczeniowych, bądź do podmiotów medycznych zaopatrujących w wyroby medyczne.
- **[Zbyt szerokie uprawnienia użytkowników systemu informatycznego]** Należy zwracać szczególną uwagę pry przyznawaniu uprawnień poszczególnym użytkownikom, aby były one adekwatne do upoważnień im udzielonych oraz zgodne z poleceniami wydanymi.
- **[Utrata dostępu do danych, jako następstwo ataku]** Niestety realnym zagrożeniem są także skuteczne ataki hackerskie w wyniku, których dochodzi do utraty dostępu do danych przechowywanych na komputerze, laptopie, telefonie, serwerze. Niestety takie zjawisko może również wystąpić u dostawcy aplikacji gabinetowej działającej w systemie online, aplikacji wykorzystywanej przez jednostkę.
- **[Kradzież dokumentacji medycznej]** Niestety tego typu zdarzenia również maja miejsce w realiach podmiotów medycznych. Praktyka przekazywania pacjentom dokumentacji celem jej zaniesienia do gabinetu lekarskiego, jest praktyka która podnosi znacznie ryzyko wystąpienia takiego zdarzenia. Należy uświadomić sobie fakt, iż pacjent może pozostawać w błędnym przekonaniu, że skoro to jego dokumentacja medyczne, jego osoby dotycząca, to ma prawo zrobić z nią wszystko. Pozostawianie dokumentacji bez nadzoru również sprzyja powstawaniu tego rodzaju zjawisk np. na parapetach, przy okienkach rejestracji.
- **[Błędne wpisy w dokumentacji medyczne]** Elementem, który najczęściej doprowadza do powstania tego rodzaju zdarzeń, jest błędna identyfikacja tożsamości pacjenta, zarówno może mieć to miejsce na etapie jego rejestracji, jak i bezpośrednio już w gabinecie lekarskim. W konsekwencji wpis dokonywany jest w dokumentacji medycznej innego pacjenta, aniżeli ten jakiemu zostało udzielone świadczenie medyczne. Należy mieć na względzie nie tyko przepisy o ochronie danych osobowych, ale także przepisy dotyczące zasad prowadzenia dokumentacji medycznej. Bezwzględnie i bezzwłocznie należy podejmować działania ukierunkowane na usunięcie tego rodzaju uchybienia. Pamiętać należy o tym, iż Platforma P1 na której gromadzone są dane, odnotuje fakt błędnego wpisu, o czym pacjent zostanie poinformowany. Tego rodzaju błędy mogą również nieść za sobą daleko idące konsekwencje dla pacjentów, którzy nie będą mogli skorzystać np. skorzystać z możliwości wystawienia recepty w związku z kontynuacją leczenia, albowiem brak będzie wpisu potwierdzającego w ogóle jego

rozpoczęcie, bądź pozbawieni zostaną możliwości realizacji e-recepty, albowiem została ona wystawiona faktycznie z wykorzystaniem danych innego pacjenta. Takich wariantów w zależności od charakteru zdarzenia może być o wiele więcej.

- **[Pomieszczenia archiwum bez nadzoru]** Zdarza się także, iż pomieszczenia przeznaczone na przechowywanie dokumentacji archiwalnej są pomieszczeniami, które całkowicie są do tego celu nieprzystosowane bądź przez lata ich użytkowania nie były one remontowane, a instalacje współwystępujące nie podlegały przeglądom technicznym. Takie sytuacje istotnie podnoszą ryzyko wystąpienia zdarzenia polegającego na zniszczeniu dokumentacji medycznej przechowywanej poprzez jej zalanie bądź spalenie.
- **[Brakowanie dokumentacji]** Z pozoru czynność, która wydawać może się nieistotna z punktu widzenia ochrony danych osobowych, jednak przypomnę, iż niszczenie, brakowanie dokumentacji medycznej zawierającej dane osobowe, stanowi przykład przetwarzania, a jako takie podlega wszystkim reżymom ochronnym.

## Autor opracowania


**mgr Dominik Spałek** Inspektor ochrony danych, założyciel portalu www.prostetorodo.pl Absolwent Wydziału Prawa i Administracji Uniwersytetu Łódzkiego. Członek Zespołu merytorycznego Proste to RODO. Ekspert z wieloletnim doświadczeniem w obsłudze podmiotów medycznych w zakresie prawa pracy, zbiorowego prawa pracy oraz ochrony danych osobowych. Dominik Spałek, jako praktyk, realizuje zadania jako Inspektor Ochrony Danych w podmiotach wykonujących działalność leczniczą w Częstochowie i nie tylko. Wspiera administratorów danych osobowych w realizacji ich obowiązków w zakresie przede wszystkich ochrony danych medycznych, w tym danych osobowych. Dominik Spałek, jako praktyk od lat przygotowuje dokumentację z zakresu prawa pracy, zbiorowego prawa pracy. Wieloletnie doświadczenie w pracy w centrali związkowej, zaowocowało licznymi publikacjami tematycznymi z zakresu prawa pracy na łamach tygodników prasowych, jak również w formie audycji radiowych. Fakt uczestnictwa w zespołach roboczych, jak i negocjacyjnych, przełożył się na jego udział w tworzeniu zapisów zakładowych / ponadzakładowych układów zbiorowych pracy m.in. dla sektora medycznego oraz pomocy społecznej.

www.prostetorodo.pl | tel. 694 494 240