

BIURO GIODO
Departament Inspekcji

Zestawienie wyników kontroli (sektorowych) zgodności przetwarzania danych z przepisami o ochronie danych osobowych przeprowadzonych w podmiotach leczniczych.

1. Wprowadzenie

Przedmiot kontroli: zbadanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, tj. ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135, z późn. zm.), zwaną dalej „ustawą” i rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), zwanym dalej „rozporządzeniem”.

Zakresem kontroli objęto przetwarzanie przez podmioty lecznicze danych osobowych pacjentów w elektronicznej dokumentacji medycznej, w systemie informatycznym Elektroniczna Weryfikacja Upnień Świadczeniobiorców (eWUŚ) oraz w innych systemach informatycznych, z wyjątkiem sterujących specjalistyczną aparaturą medyczną (firmware), poprzez ustalenie:

1. Podstawy prawnej przetwarzania danych osobowych.
2. Źródła pozyskiwania danych osobowych.
3. Zakresu, celu i rodzaju przetwarzanych danych osobowych.
4. Sposobu i trybu zbierania danych osobowych.
5. Sposobu dopełnienia obowiązków informacyjnych, wynikających z art. 24 i art. 25 ustawy.
6. Czy dane osobowe są adekwatne w stosunku do celów, w jakich są przetwarzane (art. 26 ust. 1 pkt 3 ustawy).
7. Czy dane osobowe udostępniane (przekazywane) są innym podmiotom, a jeżeli tak, to jakim podmiotom, na jakiej podstawie prawnej, w jakim celu, zakresie i w jaki sposób.
8. Czy dane osobowe podlegają zgłoszeniu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (art. 40 ustawy).

9. Czy zostały zastosowane przez administratora danych środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności, czy ww. administrator danych zabezpieczył dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem (art. 36 ust. 1 ustawy).
10. Czy administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w art. 36 ust. 1 ustawy (art. 36 ust. 2 ustawy).
11. Czy administrator danych powołał administratora bezpieczeństwa informacji (art. 36a ust. 1 ustawy).
12. Czy zostały nadane, przez administratora danych, upoważnienia osobom dopuszczonym do przetwarzania danych osobowych (art. 37 ustawy).
13. Sposobu sprawowania kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane (art. 38 ustawy).
14. Czy prowadzona jest ewidencja osób upoważnionych do przetwarzania danych zgodnie z art. 39 ustawy.
15. Kontrola systemów informatycznych w zakresie spełnienia wymogów określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

Celem przeprowadzonych kontroli było ustalenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przez podmioty lecznicze.

Czynności kontrolne przeprowadzono w okresie od dnia 6 października 2015 r. do dnia 11 grudnia 2015 r.

Kontrole zostały podjęte z inicjatywy własnej Generalnego Inspektora Ochrony Danych Osobowych na podstawie harmonogramu kontroli sektorowych na rok 2015.

Kontrole zostały przeprowadzone w siedmiu (7) podmiotach leczniczych.

2. Charakterystyka sposobu przetwarzania danych

2.1. Istotne ustalenia kontroli.

2.1.1. W toku kontroli ustalono, iż kontrolowane podmioty lecznicze przetwarzają dane osobowe pacjentów w postaci tradycyjnej (papierowej) oraz dodatkowo w systemach informatycznych. Systemy informatyczne użytkowane w kontrolowanych podmiotach leczniczych cechuje znaczna różnorodność, wynikająca z tego, iż pochodzą od różnych

producentów. Systemy informatyczne są wykorzystywane w ww. podmiotach przede wszystkim do: rejestrowania pacjentów, obsługi skierowań do poradni specjalistycznych, generowania recept, prowadzenia rozliczeń z Narodowym Funduszem Zdrowia (NFZ), przesyłania danych statystycznych dotyczących wykonanych badań, świadczeń. W toku jednej kontroli ustalono również, iż system informatyczny użytkowany jest przez podmiot leczniczy także do gromadzenia informacji związanych z przeprowadzanym przez lekarzy w trakcie wizyty lekarskiej wywiadem i badaniem (dane o stanie zdrowia pacjentów).

2.1.2. Podmioty kontrolowane korzystają również z systemów informatycznych Narodowego Funduszu Zdrowia, w szczególności z systemu o nazwie „Elektroniczna Weryfikacja Upoważnień Świadczeniobiorców” („eWUŚ”). Podstawą prawną wprowadzenia systemu Elektronicznej Weryfikacji Upoważnień Świadczeniobiorców jest art. 50 ust. 3 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2015 r. poz. 581, z późn. zm.), zgodnie z którym prawo do świadczeń opieki zdrowotnej może zostać potwierdzone na podstawie dokumentu elektronicznego, o którym mowa w art. 3 pkt 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne¹, sporządzonego na podstawie nr PESEL, przez Narodowy Fundusz Zdrowia (NFZ) dla świadczeniodawcy (podmiotu leczniczego) i przesłanego za pomocą środków komunikacji elektronicznej. Podmioty kontrolowane posiadają wydane przez NFZ upoważnienia do korzystania z systemu „eWUŚ”, na podstawie przepisów rozporządzenia Ministra Zdrowia z dnia 20 grudnia 2012 r. w sprawie warunków występowania o sporządzenie dokumentu elektronicznego potwierdzającego prawo do świadczeń opieki zdrowotnej (Dz. U. z 2012 r. poz. 1500)². Systemy informatyczne w podmiotach kontrolowanych z reguły posiadają funkcjonalność umożliwiającą kierowanie zapytania do systemu „eWUŚ”, czy osoby zapisane w danym dniu na wizytę posiadają prawo do świadczeń opieki zdrowotnej, tym samym wyjątkowo sprawdzenia dokonywane są przez

¹ Zgodnie z art. 3 pkt 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114), dokument elektroniczny to stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych.

² Stosownie do § 3 ust. 1 rozporządzenia Ministra Zdrowia z dnia 20 grudnia 2012 r. w sprawie warunków występowania o sporządzenie dokumentu elektronicznego potwierdzającego prawo do świadczeń opieki zdrowotnej, w celu uzyskania upoważnienia do korzystania z usługi Elektronicznej Weryfikacji Upoważnień Świadczeniobiorców, świadczeniodawca lub niebędąca świadczeniodawcą osoba uprawniona, składa wniosek o wydanie tego upoważnienia. Zgodnie z ust. 5 ww. przepisu, upoważnienie o którym mowa w ust. 1, zawiera: 1) dane identyfikujące świadczeniodawcę lub niebędącą świadczeniodawcą osobę uprawnioną, o których mowa w ust. 2 pkt 1; 2) zakres upoważnienia, obejmujący uprawnienie świadczeniodawcy lub niebędącej świadczeniodawcą osoby uprawnionej do: a) korzystania z usługi Elektronicznej Weryfikacji Upoważnień Świadczeniobiorców, b) upoważniania osób, którym powierza się wykonywanie zadania w zakresie występowania w jego lub jej imieniu do Funduszu o sporządzenie dokumentu potwierdzającego prawo do świadczeń.

pracowników podmiotów leczniczych poprzez stronę internetową NFZ o adresie <https://ewus.nfz.gov.pl>.

3. Podsumowanie wyników kontroli

3.1. Ogólna ocena kontrolowanej działalności

Oceniając wyniki przeprowadzonych kontroli stwierdzić należy, iż podmioty objęte kontrolą zapewniają należyte przetwarzanie danych osobowych pacjentów w systemach informatycznych przez siebie wdrożonych, w szczególności przedmiotowe systemy spełniają warunki określone w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

3.2. Synteza wyników kontroli

Uchybienia stwierdzone w toku kontroli w podmiotach leczniczych polegały na naruszeniu następujących obowiązków wynikających z przepisów o ochronie danych osobowych:

- 1) niezawarcie pisemnej umowy w przedmiocie przetwarzania danych osobowych pacjentów - w dwóch (2) podmiotach (art. 31 ust. 1 ustawy³);
- 2) niespełnieniu przez opracowany dokument odnoszący się do zasad ochrony danych osobowych wymogów przewidzianych dla polityki bezpieczeństwa – w jednym (1) podmiocie (§ 4 pkt 2 – 4 rozporządzenia⁴);
- 3) niezawarcie w ewidencji osób upoważnionych do przetwarzania danych osobowych zakresu upoważnienia do przetwarzania danych osobowych – w jednym (1) podmiocie (art. 39 ust. 1 pkt 2 ustawy).

Ponadto, w toku kontroli stwierdzono w procesie przetwarzania danych osobowych pacjentów nieprawidłowości polegające na:

- 4) niezastosowaniu środków technicznych zapewniających ochronę przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną – w jednym (1) podmiocie (art. 36 ust. 1 ustawy⁵);

³ Art. 31 ust. 1 ustawy, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.

⁴ Zgodnie z § 4 pkt 2 – 4 rozporządzenia, polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności: wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposób przepływu danych pomiędzy poszczególnymi systemami.

5) niecelowym pozyskiwaniu zgody na przetwarzanie danych osobowych od pacjentów w sytuacji przetwarzania ich danych na podstawie przepisów prawa, w związku z realizacją umowy, lub w oparciu o prawnie usprawiedliwiony cel administratora danych, tj. marketing własnych produktów i usług – w dwóch (2) podmiotach (art. 23 ust. 1 ustawy⁶).

4. Postępowanie kontrolne i działania podjęte po zakończeniu kontroli

Na podstawie wyników kontroli wszczęto postępowania administracyjne w zakresie stwierdzonych uchybień w celu przywrócenia stanu zgodnego z prawem.

⁵ Art. 36 ust. 1 ustawy, administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

⁶ Zgodnie z art. 23 ust. 1 ustawy, przetwarzanie danych jest dopuszczalne tylko wtedy, gdy: 1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych; 2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa; 3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą; 4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego; 5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.