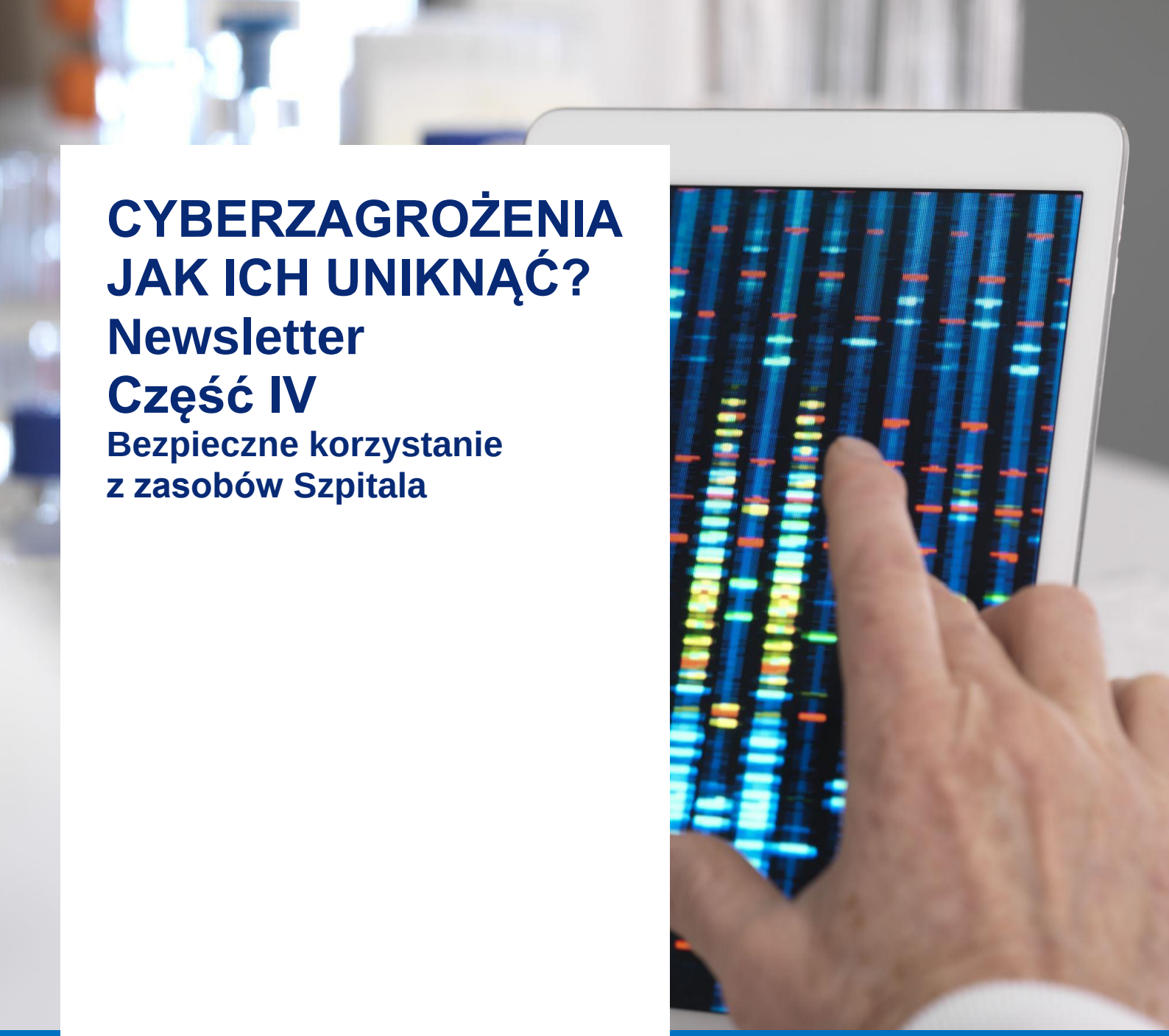


CYBERZAGROŻENIA JAK ICH UNIKNĄĆ?
Newsletter
Część IV
Bezpieczne korzystanie z zasobów Szpitala

Newsletter nr IV

stillsec

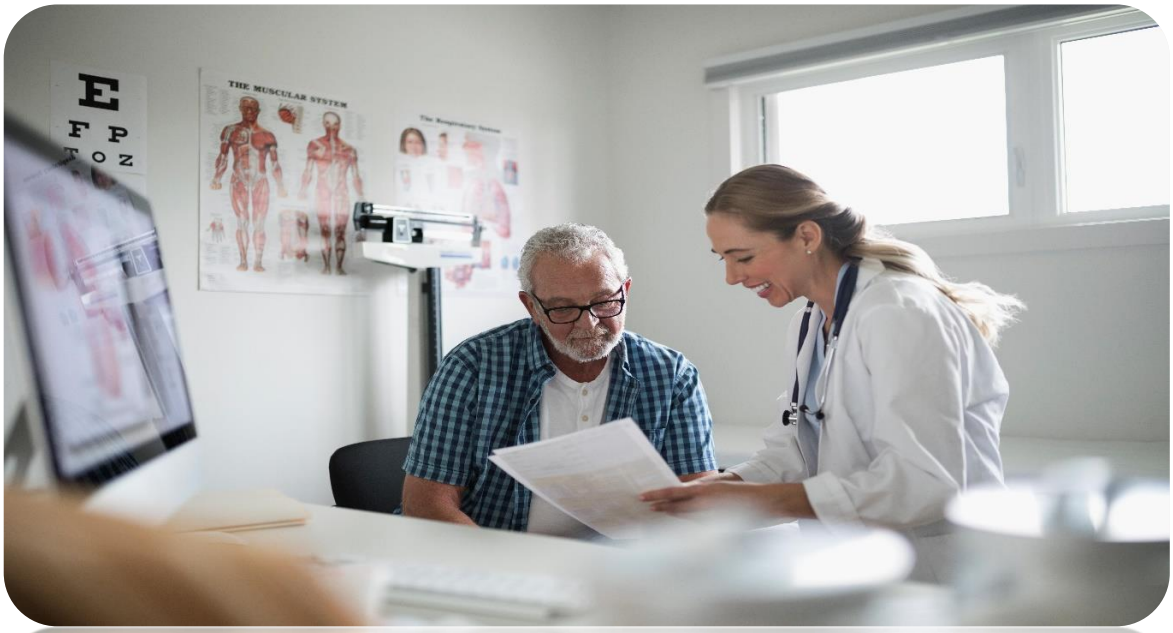
Wojewódzki Szpital Specjalistyczny nr 5 im. Św. Barbary w Sosnowcu

Centrum Urazowe

DLACZEGO BEZPIECZENE KORZYSTANIE Z ZASOBÓW SZPITALA JEST TAK WAŻNE?

Kwestię tego, dlaczego bezpieczne korzystanie z zasobów Szpitala jest tak ważne 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 Szpitala, 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.



Zasady bezpieczengo korzystania z zasobów teleinformatycznych

Rozpoczęcie pracy:

- Po włączeniu stacji roboczej użytkownik podaje własny login i hasło
- Dostęp do danych możliwy jest jedynie po dokonaniu uwierzytelnienia użytkownika
- W przypadku niemożności zalogowania się do systemu pracownik powinien niezwłocznie powiadomić o tym fakcie **pracownika Obszaru Zarządzania Informacją lub Inspektora Ochrony Danych**
- W przypadku zablokowania konta lub utraty hasła pracownik powinien osobiście zgłosić się do **Obszaru Zarządzania Informacją celem otrzymania nowego jednorazowego hasła do systemu**

Zawieszenie pracy:

- Niedopuszczalne jest pozostawienie odblokowanego komputera w miejscu dostępnym dla osób postronnych
- W przypadku braku aktywności użytkownika na komputerze przez czas dłuższy niż 10 minut następuję automatyczne włączenie wygaszacza ekranu oraz zablokowanie komputera
- Jeżeli pozostawienie włączonego komputera jest konieczne ze względu na specyfikę przetwarzanych danych, **pracownik jest zobowiązany do jego zablokowania**
- **Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane osobowe, jest dopuszczalne tylko w obecności i pod nadzorem osoby upoważnionej do ich przetwarzania**

Zakończenie pracy:

- 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 nieumożliwiający dostęp osobom nieupoważnionym (np. szafka zamykana na klucz)**

Dopuszczalne jest użytkowanie jedynie autoryzowanych przez Inspektora Ochrony Danych i przypisanych do użytkownika przenośnych nośników danych (dysków, pendrive'ów, kart pamięci itp.).

Na czym polega zasada czystego biurka i czystego ekranu?

Jest to lista dobrych nawyków zwiększających bezpieczeństwo nośników i danych wykorzystywanych w miejscu pracy. Najważniejszą i najbardziej podstawową zasadą jest obowiązek schowania wszystkich wykorzystywanych dokumentów przed wyjściem z biura/ gabinetu – nawet, jeśli będą potrzebne pracownikowi również kolejnego dnia. **Powinny one zostać umieszczone w szafce zamykanej na klucz**, który osoba zatrudniona zabierze ze sobą do domu, zda na recepcji lub przekaże innemu pracownikowi. Najlepiej w ogóle nie zostawiać na biurku żadnych dokumentów lub innych nośników danych (takich jak np. pendrive'y) oraz kluczy do szafek, kiedy się od niego oddalamy.

- Dokumenty, które **nie są już potrzebne**, **należy jak najszybciej zniszczyć** (w sposób, który uniemożliwi odczytanie zawartych w nich informacji, np. za pomocą niszczarki) lub **przekazać do archiwum**
- Przenosząc dokumenty pomiędzy poszczególnymi pomieszczeniami lub budynkami, należy je zabezpieczyć np. poprzez włożenie do koperty lub teczki
- Podczas używania faksów, kopiarek lub drukarek, **trzeba odbierać wydruki niezwłocznie po wykonaniu zadania przez urządzenie, należy cały czas nadzorować urządzenie**
- Należy pamiętać o wycieraniu tablicy po spotkaniach, na których omawiane są istotne kwestie
- **Monitor należy ustawić w taki sposób, by nikt nieupoważniony nie mógł odczytać wyświetlanych na nim informacji**
- Pamiętaj, aby ZAWSZE wylogować się z systemu przed opuszczeniem stanowiska pracy