



# **Moduł eKopia+**

Instrukcja użytkownika

---

# Spis treści

<b>Rozdział 1</b>	<b>Rozpoczęcie pracy z modułem</b> .....	2
<b>Rozdział 2</b>	<b>Konfiguracja modułu</b> .....	3
<b>Rozdział 3</b>	<b>Praca z modułem eKopia+</b> .....	5
<b>Rozdział 4</b>	<b>Składowanie kopii zapasowych szyfrowanych za pomocą modułu eKopia+</b> .....	8

---

## Wstęp

Moduł **eKopia+** stanowi funkcjonalność pozwalającą na dodatkowe zabezpieczenie kopii zapasowych w celu zminimalizowania wszelkich potencjalnych zagrożeń bezpieczeństwa danych szczególnie wrażliwych, jakimi są dane medyczne.

Zabezpieczenie pliku fizycznego kopii zapasowej bazy danych odbywa się poprzez zastosowanie dodatkowych algorytmów szyfrowania.

---

Ilustracje i „zrzuty” ekranowe zamieszczone w niniejszej publikacji mają charakter instruktażowy i mogą odbiegać od rzeczywistego wyglądu ekranów. Rzeczywisty wygląd ekranów zależy od posiadanej wersji aplikacji, aktywnych modułów dodatkowych oraz numeru wydania. Większość zrzutów ekranowych zamieszczonych w niniejszej instrukcji została wykonana przy pomocy wersji Standard+ z aktywnymi wszystkimi modułami dodatkowymi.

# Rozdział

# 1

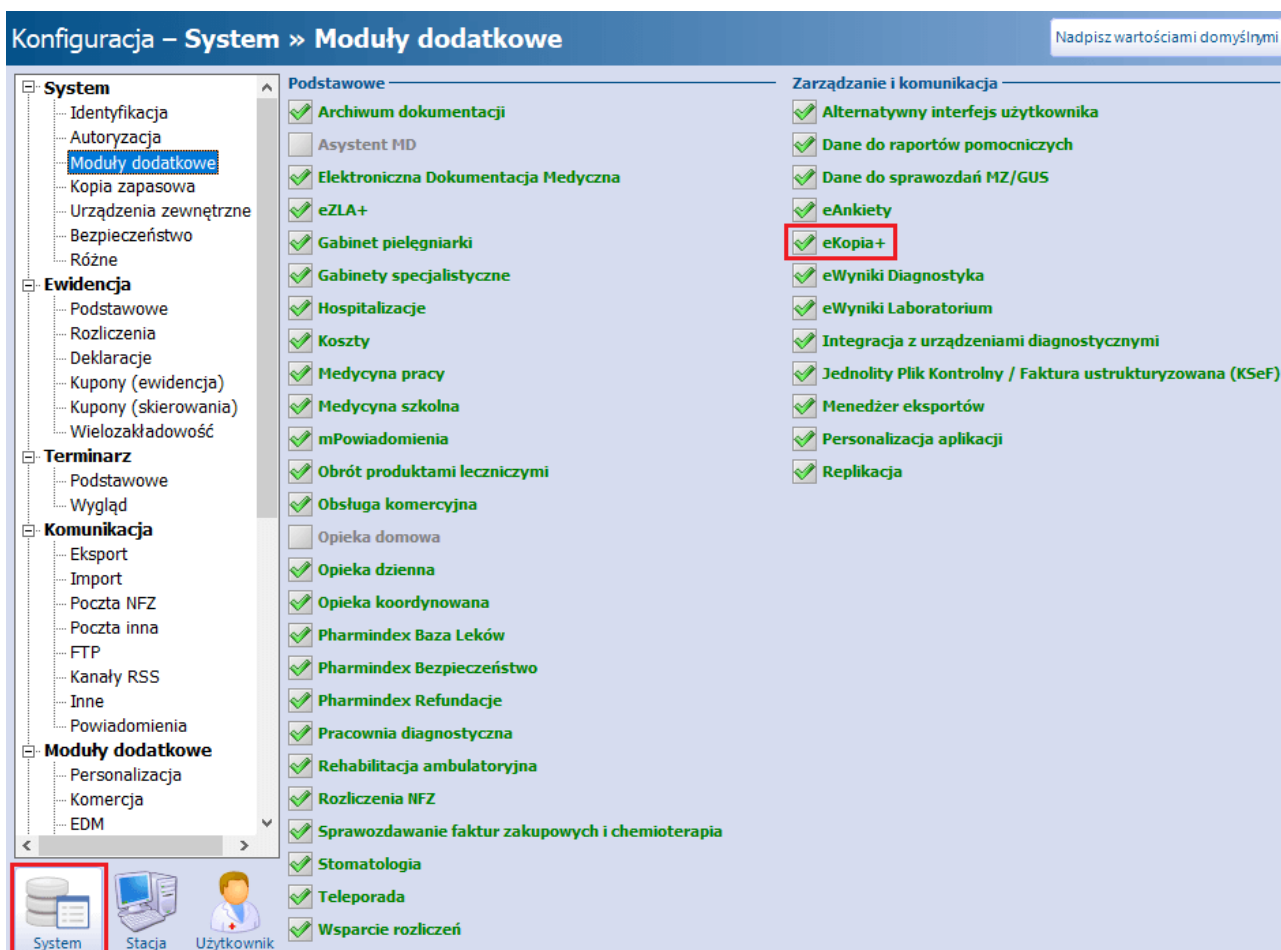
## Rozpoczęcie pracy z modulem

Aby rozpocząć pracę z modulem **eKopia+** należy:

- dokonać zakupu modułu na stronie Centrum Zarządzania Licencjami
- pobrać nowy klucz licencyjny i wczytać go do programu mMedica w [Zarządzanie > Operacje techniczne > Aktywacja systemu mMedica](#)
- włączyć moduł w [Zarządzanie > Konfiguracja > Konfigurator](#), pozycja: [System > Moduły dodatkowe](#).

Szczegółowa instrukcja włączenia modułu:

1. Przejść do: [Zarządzanie > Konfiguracja > Konfigurator](#), pozycja: [System > Moduły dodatkowe](#).
2. Włączyć parametr **eKopia+** (możliwość zaznaczenia tylko w kontekście systemu).
3. Zapisać zmiany przyciskiem **Zatwierdź (F9)**.
4. Zaakceptować komunikat o konieczności restartu aplikacji i ponownie zalogować się do programu.



## Rozdział

## 2

## Konfiguracja modułu

Konfiguracja modułu obejmuje następujące czynności:

- **nadanie wybranym użytkownikom aplikacji uprawnienia pozwalającego na zarządzanie modułem**

Ścieżka: [Zarządzanie](#) > [Konfiguracja](#) > [Użytkownicy systemu](#) > zakładka: [Uprawnienia funkcjonalne](#) > uprawnienie: "Szyfrowanie kopii bazy danych"

3. Autoryzacja 4. Uprawnienia do danych 5. Uprawnienia funkcjonalne

Nadane uprawnienia:

Grupa użytkowników: Pełne uprawnienia

Uprawnienia

- Administracja systemem
  - Definicja ustawień domyślnych personelu
  - Dopisanie użytkownika systemu
  - Dostępność opcji pilna wiadomość w poczcie wewnętrznej
  - Migracja dokumentów z repozytoriów zewnętrznych
  - Modyfikacja rejestru użytkowników systemu
  - Modyfikacja rejestru zgód eRepozytorium w chmurze
  - Prawo administrowania systemem
  - Przegląd rejestru zgód eRepozytorium w chmurze
  - Przegląd rejestru przechowywanych kart uodpornienia
  - Przegląd rejestru sprzeciwów
  - Przegląd rejestru udostępnień
  - Przegląd rejestru wniosków
  - Rejestr wysłanych powiadomień
  - Reczne wykonanie kopii zapasowej
  - Szyfrowanie kopii bazy danych**
  - Zarządzanie globalnymi schematami danych
  - Zarządzanie kontem Chmury dla zdrowia
  - Zarządzanie pulami recept

- **nadanie dodatkowego hasła, służącego do szyfrowania wykonywanej kopii bazy danych, poprzez jego wpisanie lub generację za pomocą przycisku "Generuj hasło"**

Ścieżka: [Zarządzanie](#) > [Konfiguracja](#) > [Konfigurator](#) > pozycja: [System](#) > [Kopia zapasowa](#)

Konfiguracja – System » Kopia zapasowa Nadpisz wartościami domyślnymi

<b>System</b> <ul style="list-style-type: none"><li>Identyfikacja</li><li>Autoryzacja</li><li>Moduły dodatkowe</li><li><b>Kopia zapasowa</b></li><li>Urządzenia zewnętrzne</li><li>Różne</li></ul> <b>Ewidencja</b> <ul style="list-style-type: none"><li>Podstawowe</li><li>Rozliczenia</li><li>Deklaracje</li><li>Kupony (ewidencja)</li><li>Kupony (skierowania)</li><li>Wielozakładowość</li></ul>	<b>Folder na pliki kopii:</b>	C:\Kopia	...
	Folder z plikami dodatkowymi:		...
	Zawartość folderu zostanie dołączona do pliku kopii.		
	Folder na pliki tymczasowe:		...
	<b>Hasło do szyfrowania bazy danych:</b>	*****	<input type="button" value="Generuj hasło"/> <input type="button" value="Pokaż hasło"/>
	Częstotliwość wykonywania:		(dni)
	<b>Godzina wykonania:</b>		
	Liczba zapamiętywanych plików:	5	
	<input checked="" type="checkbox"/> <b>Bez bazy leków Pharmindex</b>		
	<input type="checkbox"/> Bez załączników		

W celu ukrycia hasła należy skorzystać z przycisku "**Ukryj hasło**". Po tej czynności nazwa przycisku zmienia się na "**Pokaż hasło**" i będzie on służył do wyświetlenia hasła.

### **Uwagi dodatkowe**

1. Tylko użytkownicy, którzy posiadają uprawnienie do szyfrowania kopii bazy danych, mają możliwość nadawania hasła.
2. Hasło do szyfrowania kopii bazy danych musi spełniać następujące kryteria:
  - a. Musi składać się z co najmniej 12 znaków.
  - b. Musi zawierać co najmniej jedną dużą literę, cyfry i znaki specjalne.
3. Spełnienie warunków minimalnej długości oraz odpowiedniej składni zapewnia funkcjonalność przycisku "**Generuj hasło**". Skorzystanie z funkcji przycisku pozwoli utworzyć losowy ciąg znaków - przykład: ak#92KxkaEf

## Rozdział

## 3

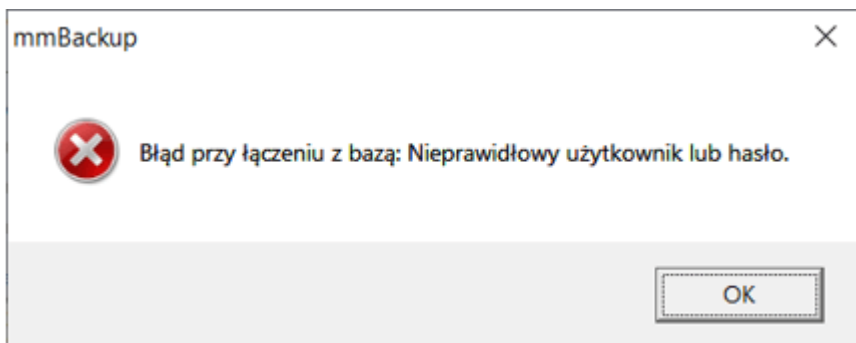
## Praca z modułem eKopia+

Od momentu uruchomienia modułu eKopia+ i jego konfiguracji wszystkie kopie są domyślnie zabezpieczone dodatkowo hasłem i szyfrowane. Przed odtworzeniem kopii bazy danych, zaszyfrowanej przy pomocy modułu eKopia+, użytkownik jest proszony o wprowadzenie hasła, ustawionego przy [konfiguracji modułu](#), w celu odszyfrowania przed dalszym rozpakowaniem kopii zapasowej.

**Uwaga!**

**Nadane przy konfiguracji modułu hasło (utworzone automatycznie przez system lub wpisane przez użytkownika) należy zapamiętać lub zapisać w bezpiecznym miejscu.** Jeżeli zdarzy się, że po nadaniu hasła zostanie utworzona dowolna kopia i po jej wykonaniu hasło zostanie zmienione, a następnie

wygenerowana zostanie kolejna kopia, to w przypadku ewentualnej awarii i utraty drugiej spośród przykładowo omawianych tu kopii – odtworzenie pierwszej z nich należy przeprowadzić z wykorzystaniem pierwszego z użytych haseł. W innym wypadku komunikat zwrotny, zamieszczony poniżej, uniemożliwi dalsze odtwarzanie bazy.



### Przykład:

1. Zapisujemy w systemie mMedica hasło: ak#92KxkaeEf.
2. Wykonujemy kopię ręcznie lub wykonana jest ona automatycznie z harmonogramu – powstaje plik wynikowy o nazwie: 2022-09-30-0015-MMEDICA(a).zip.
3. Zmieniamy w systemie mMedica hasło na: BL#92KxkaeEf.
4. Wykonujemy ponownie kopię bazy – powstaje plik wynikowy o nazwie: 2022-09-30-0030-MMEDICA(b).zip.

Odtworzenie kopii z pliku: 2022-09-30-0015-MMEDICA(a).zip należy wykonać, korzystając z hasła utworzonego w punkcie 1.

W wersji 9.0.0 aplikacji mMedica w oknie wykonywania kopii zapasowej został dodany parametr **"Wykonanie kopii bez dodatkowego szyfrowania"** (zdj. poniżej).

mMedica – kopia zapasowa

**Parametry**

Użytkownik:       Hasło:

Folder na pliki kopii zapasowych:  ...

Folder z plikami dodatkowymi:  ...

Pliki te zostaną dołączone do archiwum z bazą danych.

Sprawdź spójność danych

Nie uwzględniaj w kopii słownika leków Pharmindex

Nie uwzględniaj w kopii zawartości załączników

Wykonanie kopii bez dodatkowego szyfrowania

**Informacje**

Należy go zaznaczyć, jeżeli kopia ma zostać wykonana z pominięciem dodatkowego szyfrowania za pomocą modułu eKopia+.

## Rozdział

# 4

## Składowanie kopii zapasowych szyfrowanych za pomocą modułu eKopia+

Moduł eKopia+ poprzez dodatkowe szyfrowanie i zabezpieczenie hasłem pozwala na bezpieczne przechowywanie kopii zapasowych w ramach lokalnych zasobów placówki medycznej, jak również w sprawdzonych i bezpiecznych zasobach chmurowych, oferowanych przez wielu dostawców tego rodzaju usług.

Sposób konfiguracji danej usługi przekazywany jest przez jej dostawcę.