Załącznik do uchwały nr 83/VIII/2018 Okręgowej Rady Lekarskiej Beskidzkiej Izby Lekarskiej z dnia 8 maja 2018 roku w sprawie przyjęcia i zatwierdzenia procedury Zarządzania Ryzykiem w Beskidzkiej Izbie Lekarskiej w Bielsku-Białej.

Procedura Zarządzania Ryzykiem w Beskidzkiej Izbie Lekarskiej w Bielsku-Białej.

Spis treści

§1. Postanowienia ogólne.

1. Niniejsza procedura reguluje sposób zarządzania ryzykiem w Beskidzkiej Izbie Lekarskiej w Bielsku-Białej. Wskazuje na poszczególne procesy, osoby odpowiedzialne za dokonywanie oceny ryzyka, sposób postępowania z ryzykiem, zasady dokumentowania i komunikowania kwestii związanych z ryzykiem.
2. W zakresie zadań, zasad działania i organizacji Beskidzkiej Izby Lekarskiej stosuje się odpowiednio przepisy Ustawy z dnia 2 grudnia 2009 r. o izbach lekarskich (Dz.U. 2009 Nr 219 poz. 1708 ze zm., tj. Dz.U. 2018 poz.168).

§2. Definicje.

1. Izba - Beskidzka Izba Lekarska.
2. Prezes - Prezes Okręgowej Rady Lekarskiej.
3. Komórka organizacyjna - poszczególne działy podległe Kierownikowi Biura Izby bezpośrednio lub pośrednio, samodzielne stanowiska, konsultanci, zleceniobiorcy, Agencja Ubezpieczeniowa BIL.
4. Kierownik komórki organizacyjnej – Kierownik Biura Izby, osoba na samodzielnym stanowisku, konsultant, zleceniobiorca, Kierownik Agencji Ubezpieczeniowej BIL.
5. Ryzyko - wpływ niepewności na cele - możliwość wystąpienia zdarzenia (zagrożenia) mającego negatywny wpływ na realizację założonych celów lub uniemożliwiającego realizację celów lub możliwość wystąpienia szansy.
6. Zdarzenie - wystąpienie lub zmiana konkretnego zestawu okoliczności; może wystąpić raz lub wielokrotnie i może mieć wiele przyczyn. Może polegać na tym, że dane okoliczności nie wystąpiły.
7. Następstwo (Skutek) - rezultat zdarzenia mający wpływ na cele. Zdarzenie może prowadzić do wielu następstw.
8. Skutek kaskadowy - rezultat/rezultaty zdarzenia nasilające się w czasie i powodujące niespodziewane, silne zdarzenia wtórne.
9. Skutek skumulowany - wiele następstw (spiętrzenie) spowodowanych jednym zdarzeniem.
10. Prawdopodobieństwo - możliwość, szansa wystąpienia zdarzenia.
11. Zagrożenie - zjawisko potencjalnie szkodliwe.
12. Estymacja ryzyka - określenie przybliżonej wartości ryzyka, oszacowanie jego istotności
13. Interesariusz – osoba, organizacja lub inny podmiot która może wpływać na działalność BIL, na którą może wpływać działalność BIL lub która postrzega siebie jako zależną od podejmowanych w BIL decyzji lub działań (np. pracownicy, zleceniobiorcy, lekarze i lekarze dentyści).
14. Ryzyko nieakceptowalne – ryzyko przekraczające akceptowalny poziom ryzyka.
15. Akceptowalny poziom ryzyka – poziom narażenia na ryzyko, który jest akceptowany w razie jego wystąpienia.
16. Właściciel ryzyka – kierownik komórki organizacyjnej lub poszczególne organy BIL stosownie do zakresu wyznaczonych zadań ustawowych albo osoba wskazana pisemnie przez Prezesa BIL (wskazany pisemnie przez Prezesa zostaje również zakres ryzyka).
17. Zabezpieczenia (środki/mechanizmy ochrony) – wszystko to, co modyfikuje ryzyko. Obejmują one funkcjonowanie m.in. standardów, procedur, praktyk i fizycznych środków ochrony, których zadaniem jest minimalizacja negatywnego oddziaływania ryzyka na Beskidzką Izbę Lekarską. Zabezpieczenia wymagają regularnych sprawdzeń w celu identyfikacji np. zbyt

kosztownych, niepraktycznych i niepotrzebnych a także zbyt słabych i wymagających poprawy.

18. Istotność ryzyka - iloczyn prawdopodobieństwa i oddziaływania ryzyka.
19. Rejestr ryzyk – lista ryzyk prowadzona przez Właścicieli ryzyk w formie papierowej i elektronicznej, zwana dalej rejestrem. Wzór rejestru stanowi załącznik nr 1 do niniejszej procedury.

§3. Zakres zadań objętych zarządzaniem ryzykiem.

1. Procedurą zarządzania ryzykiem objęte są:
   1) Wybrane zadania samorządu lekarzy wymienione w art. 5 ust. 1-23 Ustawy o izbach lekarskich z dnia 2 grudnia 2009 r. (Dz.U. 2009 Nr 219 poz. 1708 ze zm., tekst jednolity: Dz.U. 2018 poz. 168),
   2) Inne zadania samorządu lekarzy określone w przepisach odrębnych,
   3) Wszystkie zadania i procesy związane z pracą Biura Beskidzkiej Izby Lekarskiej w zakresie obsługi organizacyjno-administracyjnej, finansowej i prawnej organów Beskidzkiej Izby Lekarskiej.
2. Procedura zarządzania ryzykiem służy także w szczególności właściwemu zabezpieczeniu i ochronie danych osobowych przetwarzanych przez Beskidzką Izbę Lekarską i jest częścią oceny skutków dla ochrony danych osobowych w BIL.

§4. Cel i elementy procedury zarządzania ryzykiem.

1. Zarządzanie ryzykiem to proces, który powinien być nieustannie doskonalony.
2. Zarządzanie ryzykiem ma służyć skutecznemu realizowaniu zadań samorządu lekarzy oraz optymalizacji procesów zarządzania i wykonywania zadań w Biurze BIL.
3. Procedura zarządzania ryzykiem stanowi narzędzie pomocnicze w procesie zarządzania ryzykiem.
4. Procedura obejmuje metodykę oceny ryzyka oraz proces modyfikacji ryzyka – postępowanie z ryzykiem.
5. Na ocenę ryzyka składa się:
   1) Identyfikacja ryzyka,
   2) Analiza ryzyka,
   3) Ewaluacja ryzyka.
6. Ocena ryzyka podlega bieżącemu dokumentowaniu.
7. Ocena ryzyka wykonywana jest:
   1) dla Biura Izby – raz w roku,
   2) dla danego Organu BIL - na polecenie Prezesa Beskidzkiej Izby Lekarskiej lub z inicjatywy własnej,
   3) każdorazowo w przypadku przeprowadzania oceny wpływu na ochronę danych osobowych, o której mowa w §3 ust.2, zgodnie z procedurą obowiązującą w tym zakresie w BIL.
8. Przegląd ryzyk zidentyfikowanych i umieszczonych w rejestrze ryzyk dokonywany jest przez Właścicieli ryzyk przynajmniej raz w roku.
9. Nadzór nad procedurą pełni Prezes Beskidzkiej Izby Lekarskiej a wykonywana jest:
   1) Przez Właścicieli ryzyk;

2) Dla Organów BIL – przez poszczególne organy (gdy działają jednoosobowo), lub przewodniczącego organu (gdy organy działają kolegialnie);
3) w przypadku przeprowadzania oceny wpływu na ochronę danych osobowych – przez Prezesa BIL lub wyznaczoną przez niego osobę/osoby.

§5. Identyfikacja ryzyka.

1. Identyfikacja ryzyka to proces wykrywania, rozpoznawania i opisywania ryzyka, który obejmuje:
   1) Określenie źródeł ryzyka, zdarzeń, ich przyczyn i potencjalnych następstw – w tym celu można wykorzystywać np. dane historyczne (informacje o zdarzeniach dokonanych), analizy teoretyczne, opinie ekspertów, potrzeby i wymagania interesariuszy (konieczna wcześniejsza identyfikacja grup interesariuszy), a następnie utworzenie listy wstępnie zidentyfikowanych ryzyk;
   2) Identyfikację ryzyk bez znajomości lub pewności źródeł ryzyka;
   3) Określenie przyczyn i scenariuszy możliwych następstw (skutków).
2. Przy identyfikacji ryzyka możliwe jest stosowanie podejścia zarówno szerszego - „od zdarzenia" (np. zniszczenie budynku) lub węższego - „od zagrożenia" (np. pożar budynku), a także stosowanie różnych metod wspomagających identyfikację (np. analiza SWOT, burza mózgów, lista pytań kontrolnych, what-if, analiza scenariuszy) a następnie analizę ryzyka.
3. Identyfikacja ryzyka uwzględnia badania efektów ubocznych następstw łącznie ze skutkiem kaskadowym i skumulowanym.
4. Identyfikacja ryzyka dokonywana jest przez poszczególne komórki organizacyjne i organy Beskidzkiej Izby Lekarskiej, stosownie do swojego zakresu działania.
5. Wszystkie zidentyfikowane dla Biura BIL ryzyka zgłaszane są do Kierownika Biura i umieszczane w prowadzonym przez niego rejestrze ryzyk.
6. Kierownik Biura, jeżeli jest to możliwe, przypisuje zidentyfikowane ryzyka do jednej z następujących kategorii:
   1) finansowego – związanego z zagrożeniem zasad planowania, wydatkowania i kontroli budżetu Izby,
   2) prawno–organizacyjnego –związanego z zagrożeniem naruszenia przepisów prawa, w tym naruszenia obowiązujących procedur, z wyłączeniem przypadków objętych kategorią ryzyka finansowego,
   3) bezpieczeństwa zasobów– związanego z zagrożeniem bezpieczeństwa:
      a) zasobów ludzkich (np. wystąpienia wypadków, nieprawidłowego prowadzenia rekrutacji, absencją pracowników),
      b) zasobów majątkowych (np. pożaru, kradzieży),
      c) zasobów technologicznych lub informacyjnych (np. bezpieczeństwa systemów informatycznych, danych osobowych),
      d) technicznej lub środowiska naturalnego (np. awarii infrastruktury, przerwach w dostępie do mediów, klęski ekologicznej).
7. Każdy pracownik lub osoba współpracująca z Beskidzką Izbą Lekarską, bez względu na formę prawną i zakres współpracy, ma prawo zgłaszać Kierownikowi BIL zidentyfikowane ryzyka związane z wykonywanymi przez siebie obowiązkami.

§6. Analiza ryzyka.

1. Analiza ryzyka to proces dążący do poznania charakteru ryzyka oraz określenia poziomu ryzyka.

2. W analizie ryzyka zidentyfikowane zdarzenia i zagrożenia (patrz §5 ust.2) należy rozważyć pod kątem istniejących w BIL zabezpieczeń, ich skuteczności i efektywności oraz wpływu na cele.
3. Przykładowe środki/mechanizmy ochrony:
   1) Środki organizacyjne:
      a) Instrukcje
      b) Procedury
      c) Wytyczne
      d) Standardy i Normy
      e) Wzory dokumentów
      f) Sprawdzenia okresowe/audyty
      g) Punkty kontrolne w obiegu dokumentów (zatwierdzenia)
      h) Ubezpieczenia
      i) Szkolenia
      j) Oświadczenia, np. o zachowaniu poufności
      k) Upoważnienia dostępu/przetwarzania informacji
   2) Środki ochrony fizycznej:
      a) Strefy ograniczonego dostępu,
      b) Plomby
      c) Dozór ochrony
      d) Kontrola dostępu (zamki, szyfratory, kłódki, urządzenia biometryczne),
      e) Zabezpieczenia dokumentów (kasy, sejfy, szafy zamykane na akta),
      f) Systemy alarmowe, antywłamaniowe, CCTV (monitoring), sygnalizacja (pożar, włamanie, zalanie), systemy kontroli i nadzoru pracy (RCP)
   3) Środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej:
      a) Routery, switch, sprzętowe szyfratory do szyfrowania dysków, modemy,
      b) Urządzenia eliminujące zakłócenia i przepięcia w sieci zasilającej oraz urządzenia podtrzymujące zasilanie w przypadku jego zaniku – UPS-y,
      c) System operacyjny i sieć komputerowa oraz ich konfiguracja, zapewniająca odpowiednie restrykcje w zakresie dostępu do danych;
      d) Zabezpieczenie teletransmisji (np. wykorzystanie poufnych protokołów, stosowanie procedury oddzwonienia - „callback”);
   4) Środki ochrony w ramach systemowych narzędzi programowych i baz danych:
      a) Zabezpieczenie teletransmisji (np. ograniczenie identyfikatorem i hasłem dostępu do urządzeń teletransmisji, szyfrowanie przesyłanych danych,);
      b) Środki w ramach systemu operacyjnego serwera ograniczające dostęp użytkownika jedynie do konkretnych zasobów (np. system użytkowników i haseł, ograniczenie dostępu do poziomu poleceń systemowych lub zakaz wykonywania poleceń systemowych - restricted shell, rejestracja nieudanych logowań do systemu), w ramach dostępu do Internetu – programy antywirusowe,
      c) Szyfrowania bazy danych;
      d) Automatyczna blokada dostępu do nieużywanego komputera.
4. Analiza ryzyka zawiera estymację ryzyka, która pozwala określić poziom ryzyka.
5. Estymacja polega na określeniu wagi następstwa (N) w skali od 1 do 5 i określeniu prawdopodobieństwa (P) jego wystąpienia w skali od 1 do 5.
6. Do określenia wartości następstwa (skutku) stosuje się następujące definicje i punktację:
   1) 1 pkt - nieznaczne; rozwiązanie problemu wymagało będzie nieznacznego nakładu czasu/zasobów, lecz problem nie spowoduje trwałej szkody i nie wywrze wpływu na wyniki finansowe. Może spowodować krótkotrwałe zakłócenia w działalności;

2) 2 pkt - małe; rozwiązanie problemu będzie wymagało pewnego nakładu czasu/zasobów. Usunięcie skutków (powstałych strat) będzie wymagało czasu. Może mieć mały wpływ na wyniki finansowe, których ranga będzie wymagała ujawnienia. Może spowodować niewielkie zakłócenia w działalności;
3) 3 pkt – średnie; rozwiązanie problemu będzie wymagało umiarkowanego nakładu czasu/zasobów – w tym kierownictwa wyższego szczebla. Usunięcie skutków (strat) będzie trudne. Wywrze wpływ na wyniki finansowe i może stać się ważnym wydarzeniem publicznym. Może doprowadzić do niezrealizowania zadania;
4) 4 pkt – Poważne; rozwiązanie problemu będzie wymagało dużego nakładu czasu/zasobów – w tym kierownictwa wyższego szczebla. Usunięcie skutków (strat) będzie bardzo trudne lub niemożliwe. Wywrze istotny wpływ na wyniki finansowe i stanie się istotnym wydarzeniem publicznym. Może doprowadzić do niezrealizowania kluczowego celu;
5) 5 pkt – Katastrofalne; rozwiązanie problemu będzie wymagało bardzo dużego nakładu czasu/zasobów – w tym kierownictwa wyższego szczebla. Usunięcie skutków (strat) będzie bardzo trudne lub niemożliwe. Wywrze istotny wpływ na wyniki finansowe i stanie się ważnym wydarzeniem publicznym. Doprowadzi do niezrealizowania kluczowego celu.

7. Przy określaniu punktowej wartości następstwa bierze się pod uwagę następujące czynniki:
   1) wpływ na realizację działania,
   2) opóźnienia, wpływ na płynność realizacji działania,
   3) ciągłość pracy,
   4) dostęp do zasobów,
   5) naruszenia przepisów wewnętrznych lub przepisów prawa powszechnie obowiązującego,
   6) konsekwencje prawne, w tym karno-skarbowe,
   7) konsekwencje dyscyplinarne,
   8) utrata dobrego imienia (wizerunek),
   9) utrata szans,
   10) obniżenie jakości pracy,
   11) wpływ na bezpieczeństwo informacji/ochrony danych osobowych,
   12) zniszczenie lub utrata zasobów,
   13) trudność w usunięciu skutków,
   14) inne.
8. Do określenia prawdopodobieństwa wystąpienia ryzyka należy stosować następujące definicję i punktację:
   1) 1 pkt (szacunkowe prawdopodobieństwo procentowe: od 1 do 20%) - rzadkie; ryzyko raczej nierealne, nie powinno wystąpić w nadchodzącym roku;
   2) 2 pkt (szacunkowe prawdopodobieństwo procentowe: powyżej 20 % do 40%) – mało prawdopodobne; ryzyko mało realne, może wystąpić w nadchodzącym roku w wyniku zbiegu niezwykłych okoliczności;
   3) 3 pkt (szacunkowe prawdopodobieństwo procentowe: powyżej 40% do 60%) – średnie; ryzyko realne, ryzyko może wystąpić w nadchodzącym roku, istnieją sprzyjające okoliczności wystąpienia ryzyka;
   4) 4 pkt (szacunkowe prawdopodobieństwo procentowe: powyżej 60% do 75%) – prawdopodobne; ryzyko jest wysokie, ryzyko wystąpi w nadchodzącym roku, o ile nie zostanie zmniejszone;
   5) 5 pkt (szacunkowe prawdopodobieństwo procentowe: (powyżej 75%) – prawie pewne; ryzyko jest bardzo wysokie, ryzyko wystąpi w najbliższym roku.

9. Poziom ryzyka stanowi iloczyn wartości punktów następstwa i punktów prawdopodobieństwa jego wystąpienia. Matryca pozwalająca ustalić i zinterpretować poziom ryzyk stanowi załącznik nr 2 do niniejszej Procedury.

§7. Ewaluacja ryzyka.

1. Ewaluacja ryzyka to proces porównywania wyników analizy ryzyka (poziomu ryzyka) z kryteriami ryzyka w celu stwierdzenia czy ryzyko i/lub jego wielkość są akceptowalne lub tolerowane.
2. Kryteria ryzyka ustala się w odniesieniu do wielkości poszczególnych poziomów ryzyka w matrycy ryzyka i są one następujące:
   1) Ryzyko poważne (25 -12 pkt) – wymaga pilnej uwagi i dalszych decyzji i/lub analiz. Kolor czerwony na matrycy.
   2) Ryzyko umiarkowane (10-5 pkt) – wymaga omówienia i monitorowania. Należy podjąć dalsze działania pod warunkiem, że nakłady związane z podjęciem tych działań nie przewyższą korzyści z nich wynikających. Kolor niebieski na matrycy.
   3) Ryzyko nieznaczne (4 i mniej pkt) – akceptowalny poziom ryzyka. Kolor zielony na matrycy.

§8. Postępowanie z ryzykiem.

1. W stosunku do ryzyk nieakceptowalnych (poważnych i umiarkowanych) ustala się następujące możliwe reakcje:
   1) Tolerowanie/akceptacja – przyjmuje się, iż można zaakceptować ryzyko w przypadku braku możliwości podjęcia działań ograniczających poziom danego ryzyka lub gdy koszt podjęcia jakiegokolwiek działania będzie niewspółmierny do potencjalnych korzyści, które można odnieść. W ramach tej reakcji można wdrożyć plany awaryjne w razie wystąpienia ryzyka.
   2) Przeniesienie – ograniczenie prawdopodobieństwa i efektu wystąpienia danego zdarzenia poprzez przekazanie ryzyka w całości lub częściowo innej stronie, np. outsourcing i ubezpieczenie.
   3) Wycofanie się – zaprzestanie działań ryzykownych, likwidacja ryzyka.
   4) Łagodzenie – podjęcie działań mających na celu minimalizację prawdopodobieństwa lub skutków wystąpienia ryzyka lub obu jednocześnie.
   5) Inne.

§9. Monitorowanie ryzyka.

1. Monitorowanie ryzyka w BIL stanowi proces, w ramach którego m.in:
   1) sprawdzane jest czy wdraża się reakcje na ryzyko zgodnie z planem,
   2) ocenia się czy działania podejmowane w ramach reakcji na ryzyko skutkują oczekiwanymi rezultatami,
   3) sprawdzana jest skuteczność dotychczasowych mechanizmów kontrolnych,
   4) sprawdzane jest czy poziom ryzyka nie uległ zmianie/wystąpiły nowe ryzyka,
   5) analizowane jest czy punktowa ocena ryzyka jest wciąż odpowiednia.
2. Właściciele ryzyk monitorują ryzyko w komórkach organizacyjnych, którymi zarządzają.

§10. Informowanie o ryzyku.

1. Kierownik Biura BIL, do 31 marca każdego roku zdaje Prezesowi ORL BIL raport o stanie zarządzania ryzykiem w Biurze BIL.

2. Raport może dotyczyć jedynie części lub wybranych zagadnień związanych z funkcjonowaniem Biura BIL, zawsze musi jednak zawierać informacje o wszystkich ryzykach poważnych.
3. Organy Izby, po dokonanej ocenie ryzyka składają raport o stanie ryzyka Prezesowi ORL BIL.
4. Organy Izby prowadzą wewnętrzne rejestry ryzyk, zgodnie ze wzorem, który stanowi załącznik nr 1 do niniejszej procedury.

§11. Postanowienia końcowe.

1. Procedura zarządzania ryzykiem podlega raz na rok przeglądowi przez Kierownika Biura BIL w celu jej aktualizacji.
2. Wszelkie zmiany w Procedurze zarządzania ryzykiem zatwierdzane są w drodze uchwały Okręgowej Rady Lekarskiej BIL.

Autor procedury: Agnieszka Witoszek, Administrator bezpieczeństwa informacji w Beskidzkiej Izbie Lekarskiej w Bielsku-Białej

Załącznik nr 1. Rejestr ryzyk.

ID ryzyka	Opis ryzyka	Ocena ryzyka			Postępowanie z ryzykiem 1.	Postępowanie z ryzykiem 2.	Działania planowane w ramach postępowania z ryzykiem	Terminy wykonania działań	Osoby odpowiedzialne za działania
		N	P	R					

Załącznik nr 2. Matryca ryzyka.

Następstwo					
Katastrofalne	**5**	**10**	**15**	**20**	**25**
Poważne	**4**	**8**	**12**	**16**	**20**
Średnie	**3**	**6**	**9**	**12**	**15**
Małe	**2**	**4**	**6**	**8**	**10**
Nieznaczne	**1**	**2**	**3**	**4**	**5**
Prawdo-podobieństwo	*Rzadkie*	*Mało prawdo-podobne*	*Średnie*	*Prawdo-podobne*	*Prawie pewne*

SEKRETARZ
OKRĘGOWEJ RADY LEKARSKIEJ

MACIEJ SKWARNA

PREZES
OKRĘGOWEJ RADY LEKARSKIEJ

KLAUDIUSZ KOMOR