Szpital Powiatowy w Rykach spółka z o. o. wdraża Politykę Bezpieczeństwa Informacji w skład której wchodzi Instrukcja Zarządzania Systemami Informatycznymi.

System zarządzania bezpieczeństwem informacji składa się z : polityk, procedur, instrukcji, wytycznych, których celem jest ochrona danych osobowych i aktywów informacyjnych. System zarządzania informacją ma charakter systematyczny, co oznacza, że poza ustanowieniem i wdrożeniem zasad i rozwiązań podlegają one monitorowaniu i okresowej ocenie w celu ich poprawy i doskonaleniu bezpieczeństwa.

Szpital wdrożył i wykorzystuje system zarządzania bezpieczeństwem informacji w oparciu o wymagania przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, przepisów krajowych oraz dobrych praktyk i standardów, celem wyeliminowania zagrożeń mogących mieć niekorzystny wpływ na proces świadczenia usług przez szpital na rzecz pacjentów i kontrahentów.

Podstawowym dokumentem jest Polityka Bezpieczeństwa Informacji, która zawiera opis obowiązków nałożonych na Administratora Danych, którego podstawowym obowiązkiem jest dołożenie wszelkiej staranności w celu ochrony interesów osób, których dane przetwarza, a także dopełnienie obowiązku informacyjnego wynikającego z art. 13 RODO.

Każda osoba mająca dostęp do informacji zobowiązana, jest zgodnie z posiadanymi kompetencjami i uprawnieniami do zapoznania się z Polityką Bezpieczeństwa Informacyjnego – przeszkolenia na danym stanowisku, złożenia stosownego oświadczenia dot. zachowania tajemnicy.

Szpital zobowiązany jest do szacowania ryzyka dla swoich usług kluczowych, zbierania informacji o zagrożeniach i podatnościach, stosowania środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego oraz zgłaszania incydentów.

Reakcja na niepożądane zdarzenia (incydenty) lub podatności:

Każdy pacjent, osoba odwiedzająca pacjentów, pracownik, współpracownik Szpitala w przypadku zauważenia:

- ✓ próby wpłynięcia na system zabezpieczeń, których celem jest ich przełamanie, próby nieautoryzowanego wejścia do obszaru podlegającego ochronie;
- ✓ powzięcia wątpliwości co do stanu technicznego urządzeń służących do przetwarzania danych osobowych;
- ✓ innych budzących wątpliwości w zakresie przestrzegania bezpieczeństwa informacji, a mogących wpłynąć na świadczenie usług,

proszony jest o zgłoszenia niezwłocznie zaobserwowanej sytuacji na adres e-mail: iod@rykiszpital.pl

Każdy użytkownik (pracownik lub osoba z firmy zewnętrznej współpracującej ze Szpitalem) ma obowiązek zgłaszania zauważonych przez siebie incydentów i nieprawidłowości oraz notować wszystkie szczegóły związane z incydentem.

Ponadto dostrzegający zdarzenie, incydent bezpieczeństwa informacji, nieprawidłowe działanie systemów w aspekcie bezpieczeństwa informacji, próby podszywania się pod pacjenta, nieautoryzowane próby podłączeń do infrastruktury Szpitala, fałszywe wiadomości mailowe wysyłane do personelu Szpitala, inne zdarzenie mogące mieć wpływ na bezpieczeństwo informacji,

jest zobowiązany zaobserwowaną sytuację niezwłocznie zgłosić na adres e-mail: iod@rykiszpital.pl

Osoba zgłaszająca problem lub naruszenie ma obowiązek powstrzymania się od wykonywania czynności naprawczych lub rozwiązujących problem bez zgody i wiedzy zarządu szpitala, za wyjątkiem działań niezbędnych dla zapewnienia bezpieczeństwa osobom i mieniu szpitala. Działania te mogą być także związane z zabezpieczeniem materiału dowodowego, w celu ograniczenia możliwości ich wystąpienia w przyszłości oraz ocenie dlaczego doszło do incydentu.

Pamiętaj o najpopularniejszych zagrożeniach w sieci: (ataki z użyciem szkodliwego oprogramowania)

- ✓ kradzieże tożsamości,
- ✓ ataki mające na celu wyłudzenie lub zniszczenie danych,
- ✓ blokada dostępu do usług,
- ✓ niechciana poczta (SPAM),
- ✓ socjotechnika,
- ✓ phishing.

W celu ochrony przed zagrożeniami należy stosować zabezpieczenia:

- ✓ używaj aktualnego oprogramowania antywirusowego – stosuj ochronę w czasie rzeczywistym, włącz aktualizacje automatyczne,
- ✓ skanuj oprogramowaniem antywirusowym wszystkie urządzenia podłączane do komputera – pendrivy, płyty, karty pamięci,
- ✓ aktualizuj system operacyjny i posiadane oprogramowanie,
- ✓ nie otwieraj plików nieznanego pochodzenia,
- ✓ wszystkie pobrane pliki skanuj programem antywirusowym,
- ✓ nie korzystaj ze stron banków, poczty elektronicznej, które nie mają ważnego certyfikatu bezpieczeństwa,
- ✓ cyklicznie skanuj komputer oprogramowaniem antywirusowym i sprawdzaj procesy sieciowe,
- ✓ nie odwiedzaj stron oferujących darmowe filmy, muzykę albo łatwe pieniądze – najczęściej na takich stronach znajduje się złośliwe oprogramowanie,
- ✓ nie podawaj swoich danych osobowych na stronach internetowych, co do których nie masz pewności, że nie są one widoczne dla osób trzecich,
- ✓ zawsze weryfikuj adres nadawcy wiadomości e-mail,
- ✓ zawsze zabezpieczaj hasłem lub szyfruj wiadomości e-mail zawierające poufne dane – hasło przekazuj innym sposobem komunikacji,
- ✓ cyklicznie wykonuj kopie zapasowe ważnych danych,
- ✓ zawsze miej włączoną – zaporę sieciową „firewall”
- ✓ zwracaj uwagę na komunikaty wyświetlane na ekranie komputera.