

**Koncepcja funkcjonalno – techniczna Medycznego
Centrum Baz Danych (Medical Data Center) wraz z
infrastrukturą dla potrzeb przyszłego Klastra „e-
Zdrowie”**

Spis treści

1. Obszary zastosowań – rynek CMPD.
 - 1.1. Przykłady funkcjonowania i działania CMPD.
 - 1.2. Specyfika CMPD.
 2. Usługi telemedyczne – skala i wolumetria.
 - 2.1. Usługi e-learningu.
 - 2.2. Usługi telekomunikacyjne.
 - 2.3. Usługi telemonitoringu.
 3. Aplikacja ASP dla e-Zdrowia.
 - 3.1. Aplikacje klasy ERP i EHR dla szpitali.
 - 3.2. Aplikacja dla administracji, statystyki publicznej i ewidencji zasobów e- Zdrowie.
 4. Analiza konkurencji.
 - 4.1. Cennik usług.
 - 4.2. Czy warto budować CMPD i dlaczego?
-

Wprowadzenie

Przedkładane opracowanie, jest materiałem analitycznym powstałym na potrzeby związane z budową Medycznego Centrum Przetwarzania Danych (MCPD), jako elementu strategii e-Zdrowia Regionu Dolnośląskiego. Ze względu na cechy użytkowe MCPD oraz oddziaływanie na model świadczeń zdrowotnych, należy widzieć tego typu inwestycje jako przedsięwzięcie wykraczające poza obszar regionu. Celem tego opracowania jest zatem przedstawienie opinii odnośnie pytania „Czy warto budować MCPD i dlaczego”.

Streszczenie

Globalizacja usług powoduje ich lokalizację w wielu krajach i regionach, przy angażowaniu scentralizowanych zasobów najczęściej w miejscu, gdzie są sprzyjające warunki pozwalające na konkuruwanie. Wymaga to od współczesnych przedsiębiorstw coraz większej sprawności działania. Dynamika usług rynku ochrony zdrowia powiększa się poprzez możliwości korzystania z zasobów wiedzy czy konsultacji w oparciu o powszechnie stosowane cyfrowe metody przetwarzania danych. Użytkownicy narzędzi teleinformatycznych oczekują stałego skracania czasu od identyfikacji nowych potrzeb do ich zaspokojenia. Stawia to nowe wyzwania zarówno przed integratorami systemów teleinformatycznych, jak też przed operatorami usług telekomunikacyjnych. Pewny i wydajny dostęp do Internetu, wirtualne sieci korporacyjne czy usługi VoIP — to już nie tylko narzędzia codziennej pracy, ale elementy stymulujące rozwój. Taki model usług zagwarantuje Medyczne Centrum Przetwarzania Danych. CMPD i podobne firmy łatwiej kształcą i utrzymują potrzebnych specjalistów, a także szybciej realizują uzupełniające inwestycje w urządzenia, które spełniają wybrane funkcje przy wykorzystaniu istniejącej infrastruktury podstawowej. Również historia rozwoju gospodarki wykazuje, że zróżnicowane potrzeby klientów sprawniej i wydajniej zaspokajane są przez niewielkie, wyspecjalizowane firmy, które dzięki skupieniu się na wybranym wycinku działalności mogą elastycznie dostosowywać się do dynamicznie zachodzących zmian. Jako naturalna konsekwencja rozwoju potrzeb gospodarki pojawia się zatem na rynku telekomunikacyjnym nowa generacja usług, oferujących kompleksową obsługę klientów w tak zwanym modelu „usług

zarządzanych”. Zgodnie z potrzebami takiego konkretnego zastosowania, Centrum jest odpowiedzialne za zbudowanie systemu transmisyjnego opartego na infrastrukturze różnych operatorów telekomunikacyjnych. Ponosi również odpowiedzialność za zarządzanie całym rozwiązaniem, zapewnia gwarancję stałego spełniania zakontraktowanych parametrów technicznych i jakościowych oraz jednolite procedury obsługi użytkowników.

W zakresie integracji usług związanych z przechowywaniem, udostępnianiem, zabezpieczaniem, przetwarzaniem danych medycznych oraz udostępnianiem aplikacji dziedzinowych np. do wspomagania procesów zarządczych w szpitalu, organizacji sieci powiązań i monitorowania przesyłu danych telemedycznych pomiędzy pacjentami objętymi monitorowaniem a centrum medycznej opieki sprawuje Centrum Medycznego Przetwarzania Danych (CMPD), które niesie ze sobą korzyści dla wszystkich zainteresowanych stron. Daje on możliwość lepszego dostosowania do specyfiki wymagań wszystkich klientów, optymalizację kosztów korzystania z infrastruktury oraz — co może najważniejsze — elastyczność wprowadzania zmian.

Obszary zastosowań – rynek CPD

Migracja i przeniesienie danych z rozproszonych systemów stosowanych w szpitalach do zintegrowanego systemu. Migracja danych systemu kadrowo-płacowego zawierającego dane bieżące i archiwalne pracowników szpitali. Zadanie to musi być zrealizowane przez producenta oprogramowania kadrowo-płacowego lub w przypadku systemów otwartych przez zatrudnionych tam informatyków. Ten obszar kosztów powinien być finansowany z zewnętrznych środków, gdyż ZOZ nie stać obecnie na tak kosztowne przedsięwzięcia.

Migracja wymaga napisania programu migrującego dane ze starego systemu do np. pliku tekstowego w formacie akceptowanym przez wybrany system. Orientacyjne koszty takiej usługi winny być przedmiotem kalkulacji i analizy. Wielkość danych w tym systemie nie wpłynie na czas migracji.

Przykłady funkcjonowania i działania CMPD

Firmy międzynarodowe w Polsce

Na rynku europejskim i w Polsce z powodzeniem funkcjonują już Centra Przetwarzania Danych. Świadczą one określone usługi (omówione w innej części opracowania) ale żadne z nich nie świadczy usług dla branży medycznej. Taki stan wynika zapewne z ograniczeń

prawnych dotyczących przechowywania danych a terenie ZOZ. Inną przyczyną może być konieczność prowadzenia (do tego roku) dokumentacji medycznej w formie papierowej.

W Piasecznie pod Warszawą znajduje się wybudowane przez GTS Energis Centrum Danych. Data Center (<http://www.gtsenergis.pl>) posiada wysokiej jakości dostęp do sieci GTS Energis, oraz wysoki stopień bezpieczeństwa. Tam, gdzie jest to fizycznie możliwe, wszystkie najważniejsze elementy są dublowane, dzięki czemu nie ma pojedynczego punktu, w którym rozwiązania GTS Energis mogłyby okazać się zawodne. Centrum zajmuje powierzchnię 5.000 m², z czego 1.250m² (z możliwością rozbudowy o kolejne 1.500m²) przystosowane jest do podłączania serwerów dla Klientów. Cały obszar utrzymywany jest w stałej temperaturze. Firma oferuje hosting dedykowany, WWW, E-mail, kolokację oraz Zapasowe Centrum Danych

W ramach usług outsourcingowych Itelligence (<http://pl.itelligence.de/>) świadczy usługi wsparcia dla użytkowników systemu mySAP, usługi hostingu IT, usługi zdalnej administracji oraz usługi w ramach Application Services Provider. Firma świadczy usługi wsparcia dla technologii i procesów biznesowych w dedykowanych centrach w pięciu lokalizacjach: w Poznaniu, w Bielefeld, w Walldorf, w Bautzen, i w Cincinnati.

Własne Centrum Danych posiada również firma HP Data Center (<http://www.hp.com.pl>), która świadczy usługi na skalę międzynarodową. Obecnie firma HP dysponuje ośrodkiem outsourcingowym o łącznej powierzchni 2000 m², składającym się z Data Center, pomieszczeń operatorskich i powierzchni biurowych dla ponad 100 użytkowników. W Data Center zapewnione jest stałe zasilanie gwarantujące ciągłą łączność telekomunikacyjną. Niezawodny system zasilania zapewnia dedykowana stacja transformatorowa zabezpieczona zespołem zasilaczy awaryjnych UPS oraz agregatem prądotwórczym,

Firma ta posiada dostęp do większości rodzajów usług telekomunikacyjnych, począwszy od ciemnych światłowodów, poprzez łącza szerokopasmowe (SDH, ATM), skończywszy na łączach dostępowych 2mb/s - wszystko z możliwością zabezpieczeń łączami backupowymi. Utrzymanie optymalnych warunków pracy (temperatura, wilgotność) dla znajdującego się w Data Center sprzętu komputerowego i warunków środowiskowych zapewniono poprzez zastosowane jednostki klimatyzacji precyzyjnej, Zastosowano również dodatkowe środki bezpieczeństwa takie jak system gaszenia gazowego przestrzeni Data Center oraz ściany Data Center wykonano w technologii zapewniającej 90 minut odporności ogniowej. Restrykcyjny dostęp do samego obszaru Data Center zrealizowano poprzez wprowadzenie kart magnetycznych, PIN-code oraz czytników biometrycznych. Pomieszczenie dedykowane na nośniki z danymi Klientów wyposażono w ogniodoporne sejfy. Całodobowy monitoring i

ochrona fizyczna obiektu oraz restrykcyjne procedury związane z dostępem do ośrodka gwarantują zapewnienie bezpieczeństwa. Kluczowe elementy infrastruktury tj. UPS, klimatyzatory pracują w układach redundancyjnych zapewniających odpowiedni poziom nadmiarowości. Awaria jednego z elementów nie powoduje przestoju w pracy urządzeń znajdujących się w Data Center.

Często utrzymanie własnego ośrodka zapasowego jest zbyt kosztowne, a skorzystanie z ośrodka zapasowego HP podczas wystąpienia awarii jest utrudnione, np. z uwagi na duże odległości lub uwarunkowania techniczne. Na potrzeby tych Klientów HP w ramach usług BRS udostępnia ruchome Data Center - HP Mobile Data Center. Jest to 12-metrowej długości kontener wyposażony w klimatyzację, sieć komputerową oraz własne zasilanie (UPS, agregat), pozwalające na pracę bez zewnętrznego źródła zasilania. Kontener może pomieścić do 6 szaf rackowych ze sprzętem i jest wyposażony w dodatkowe pomieszczenie dla administratorów. Po podłączeniu do zewnętrznej sieci telekomunikacyjnej kontener stanowi w pełni funkcjonalne Data Center.

Duże firmy krajowe

Firma WASKO S.A. (<http://www.wasko.pl>) oferuje outsourcing pamięci masowych - umożliwi Klientom korzystanie z bezpiecznych i sprawdzonych rozwiązań sprzętowych i programowych bez konieczności ich zakupu. Usługi te obejmują archiwizację - zapisywanie danych określonych przez Klienta na trwałych nośnikach danych, backup - możliwość tworzenia kopii zapasowych danych przy wykorzystaniu najlepszych rozwiązań renomowanych firm światowych (np. Exodus Communications, Verio Co.).

Poza tym przechowywanie danych - udostępnia przestrzeń dyskową na administrowanych przez nas macierzach dyskowych oraz ASP - usługa pozwala klientom korzystać z nowoczesnych systemów informatycznych bez konieczności ich nabywania.

Proponowane przez Incenti (<http://www.incenti.pl>) usługi zapewnienia ciągłości działania i odtwarzania mają za zadanie zminimalizować straty finansowe klienta spowodowane nieciągłością pracy operacyjnej jego systemów informatycznych. Obejmują one trzy główne grupy:

Disaster Recovery - przywrócenie poprawnego działania firmy na poziomie technicznym i biznesowym po wystąpieniu zdarzenia kryzysowego

Business Continuity Planning - plan działań gwarantujących m.in. ciągłość realizacji działań

prowadzonych przez firmę oraz minimalizację zagrożeń w przypadku wystąpienia sytuacji kryzysowej.

Disaster Recovery Planning - plan działań gwarantujących: podjęcie szybkich działań odtwarzających (w przypadku wystąpienia sytuacji kryzysowej) oraz minimalizację skutków kryzysu.

Wykonywanie kopii zapasowych (Backup) umożliwiających odtworzenie danych aplikacji, systemu operacyjnego lub poszczególnych plików/katalogów w wypadku awarii lub incydentalnego usunięcia/modyfikacji,

Archiwizacja - przenoszenie i przyrostowe gromadzenie danych nie wymagających już przetwarzania bądź tworzenie kopii migawkowych (snapshot, point-in-time copy) umożliwiających odtworzenie stanu systemu z konkretnego punktu w czasie.

Firma posiada własną infrastrukturę techniczną i biurową, którą może udostępniać dla klienta jako zastępcze centrum przetwarzania danych.

Centrum Ochrony Danych ATM S.A. (<http://www.atm.com.pl>) zostało utworzone aby służyć instytucjom, dla których szczególne znaczenie ma ciągłość pracy i bezpieczeństwo kluczowych systemów informatycznych oraz zapewnienie zapasowego środowiska pracy dla kluczowych zespołów pracowników. Dzięki usługom COD możliwe jest ograniczenie ryzyka operacyjnego oraz kosztów w związanych z niedostępnością systemów teleinformatycznych i/lub strat związanych z przerwami w działalności systemów operacyjnych. Utrzymywanie i obsługa techniczna zapasowych centrów operacyjnych oparta jest na podłączeniu do systemów przetwarzania i składowania danych Klienta. Jest to realizowane poprzez sieci telekomunikacyjne, takie jak telefonia, sieć korporacyjna Klienta, Internet, sieci usługowe (np. Reuters, Bloomberg). Zalety wynikające z podłączenia do Centrum Ochrony Danych wiążą się z wdrożeniem procedur operacyjnych, bezpieczeństwem fizycznym (teren całodobowo chroniony i monitorowany) oraz z zapewnieniem nadmiarowych łączy telekomunikacyjnych. Zasoby telekomunikacyjne decydujące o atrakcyjności to własna sieć światłowodowa na terenie Warszawy (ponad 200 km tras), w tym trzy niezależne przeprawy przez Wisłę a także łącza innych operatorów. Centrum gwarantuje także zasilanie w energię elektryczną, pomieszczenia biurowe o wymaganym standardzie i z odpowiednim wyposażeniem oraz gwarantowane są czasy wznowienia działalności. Na miejscu jest też dostępna fachowa obsługa techniczna, świadczona przez kadrę doświadczonego integratora systemowego. Dla uprawnionych pracowników Klienta zapewniony jest dostęp gwarantujący wysoki poziom ochrony poufności danych.

CPD BOT Elektrownia Bełchatów S.A (<http://www.zoi.elb.pl>) zapewnia wysoką dostępność systemów oraz pełne bezpieczeństwo baz danych realizowane przez niezawodne zasilanie z dwóch transformatorów wysokiego napięcia, dwóch rozdzielni, podwójnego układu zasilania bezprzerwowego UPS. Możliwość podłączenia urządzeń z niezawodnym pojedynczym zasilaczem do „static switch-a”, oraz podwójny układ klimatyzacji precyzyjnej STULZ zapewnią pełną moc chłodniczą w przypadku awarii jednego klimatyzatora. Z kolei technologia „ROOM IN ROOM” zabezpiecza przed pożarem zewnętrznym, zalaniem w trakcie akcji gaśniczej, niepowołanym dostępem. Wczesne wykrywanie wody wewnątrz pomieszczenia serwerów, wraz z automatyczną wewnętrzną instalacją gaśniczą opartą o gaz FM200 i system wczesnego wykrywania dymu VESDA to kolejne wsparcie bezpieczeństwa CPD.

Poza tym Centrum dysponuje okablowaniem miedzianym w standardzie kat 6, podwójne łącza internetowe od niezależnych ISP a także separacją galwaniczną CPD od zewnętrznych sieci komputerowych i telekomunikacyjnych. Ponad to firma oferuje udostępnianie sprzętu na czas potrzebny do realizacji zadań partnera, udostępnianie baz danych oraz instalację i udostępnianie serwerów baz danych. Kolejna usługa to dzierżawienie "mocy obliczeniowych" serwerów, składowania danych oraz korzystania z aplikacji zainstalowanych na serwerach ELB wraz z wynajmem oprogramowania za pośrednictwem sieci - Internetu lub łączy dedykowanych. Możliwe jest również umieszczenie własnego serwera w zasobach CPD, oraz archiwizacja i przechowywanie cyfrowych zasobów systemowych partnera.

Małe firmy krajowe

Serwerownie firmy Hector S.A. (<http://www.hector.com.pl>) posiadają wielostopniowy system kontroli dostępu, całodobową ochronę, system alarmów strefowych oraz system monitoringu wizyjnego. Zakres usług obejmuje możliwość wynajęcia biura zapasowego dostępnego w ciągu 24 godzin od momentu zgłoszenia. Warunki techniczne dla tego Data Center to dwie niezależne lokalizacje w oddalonych od siebie budynkach z trójstopniowym systemem zasilania. Zasilanie dwustronne z systemem przełączania na kierunek zapasowy obejmuje urządzenia UPS oraz agregaty prądotwórcze (start automatyczny, praca ciągła). Poza tym istnieje redundantna klimatyzacja i system gaszenia gazowego. Nad bezpieczeństwem danych czuwa również system kontroli dostępu i system monitoringu wizyjnego oraz całodobowy dyżur operatorów i ochrony. Kompleks biurowy Hector S.A. składający się z dwóch

niezależnych budynków dysponuje specjalnie przygotowanymi pomieszczeniami na potrzeby biura zapasowego dla klientów wyposażonymi w biurka, krzesła, telefony i dedykowaną sieć logiczną. Biura są dostępne w ciągu 24 godzin (lub szybciej) od momentu zgłoszenia takiej potrzeby.

ComputerLand S.A. (<http://www.computerland.pl>) Udostępnianie budynku, platformy sprzętowej, usług przetwarzania danych, archiwizacji i składowania danych lub operowanie systemami informatycznymi w siedzibie Klienta. Usługodawca odpowiada za bezpieczeństwo danych niezbędnych do prowadzenia działalności biznesowej Klienta. Usługę przechowania i przetwarzania danych w grupie kapitałowej Computerland realizuje firma WebInn S.A.

Usługi Centrum Danych Unizeto Technologies S.A. (<http://www.unizeto.pl>) obejmują przetwarzanie danych, udostępnianie aplikacji (ASP), backup i archiwizację danych, archiwizację dokumentów papierowych, obsługę korespondencji masowej, digitalizację i skanowanie dokumentów, hosting i kolokację, prowadzenie zapasowych centrów danych, outsourcingowe centrum certyfikacji, usługi Elektronicznego Urzędu Podawczego (EUP); oraz obsługę systemu e-faktur.

Talex S.A. (<http://www.talex.pl>) oferuje wynajem oprogramowania w systemie ASP, możliwość instalacji własnych serwerów w Centrum Danych, zaawansowany hosting. Dodatkowo firma oferuje usługi bezpiecznego transportu nośników oraz możliwość uruchomienia biura zapasowego w siedzibie usługodawcy. Powierzchnia centrum danych wynosi 1300 m². Usługa kolokacji polegająca na umieszczeniu własnego serwera fizycznego w wyspecjalizowanym ośrodku firmy TALEX S.A. zapewniającym optymalne warunki dla funkcjonowania serwerów.

Oferta Centrum Komputerowe Zeto S.A. (<http://www.ckzeto.com.pl>) obejmuje outsourcing aplikacji (ASP) na komputerach o wielkiej mocy obliczeniowej (mainframe), zdalny backup i archiwizację danych, zapasowe Centra Danych oraz wydruk i kopertowanie personalizowanych dokumentów masowych. Firma ITCS Sp. z o.o. (<http://www.itscs.pl>) posiada nowoczesne centrum przetwarzania danych, spełniające standardy bezpieczeństwa oraz ciągłości pracy centrum (niezależne zasilanie, system przeciwpożarowy, klimatyzacja, redundancja łączy internetowych i urządzeń dostępowych itd.). Oferuje również dodatkowe usługi, np.: regularna archiwizacja danych zgromadzonych na serwerach klienta.

Infrastruktura i wymagania dla CPD w kontekście wymogów formalno prawnych.

Nowoczesne technologie w zasadzie wykluczają wydzielenie dla potrzeb serwerowni pomieszczenia biurowego o odpowiedniej powierzchni. Nowoczesny obiekt Data Center

powinien umożliwiać rozbudowę swoich zasobów oraz spełniać zaawansowane wymogi bezpieczeństwa danych. Specyfika danych medycznych nakazuje uwzględnienie ochrony danych osobowych w tym konieczne jest ich oddzielenia od danych medycznych przechowywanych w Data Center. Dlatego też lokalizacja musi spełniać pewne wymagania. Centrum danych medycznych nie może leżeć na terenach, które by mogły być w zasięgu klęski żywiołowej, takiej jak podtopienie czy zalanie. Centrum powinno być zlokalizowana z dala od składowisk lub fabryk produkujących materiały toksyczne, radioaktywne, wybuchowe, żrące, łatwopalne itp. oraz z dala od instytucji i baz wojskowych. Powinien to być obiekt wolnostojący i całkowicie kontrolowany przez personel centrum, aby w ten sposób zapewnić całkowity nadzór nad ruchem osobowo-materiałowym w centrum oraz na obszarach bezpośrednio przyległych do pomieszczeń obiektu. Usytuowanie z dala od źródeł powodujących zakłócenia elektromagnetyczne (transformatory, radiotelefony itp.) to kolejny wymóg odnośnie lokalizacji. Wysokość technologiczna pomieszczenia serwerowni mierzona od podłogi technicznej do sufitu powinna wynosić minimum 3 m. Ściany powinny być ognioodporne, co najmniej klasy EI120 oraz pomalowane niepalnymi farbami. Z uwagi na modułową strukturę najnowszych rozwiązań serwerowni powinna istnieć możliwość dołożenia kolejnych szaf technicznych. Innym wymogiem jest nośność stropu, która powinna mieścić się w minimalnych granicach przewidzianych dla pomieszczeń biurowych: 500 kg/m² Zalecana jest jednak posadzka wysokiej nośności z wykończeniem niepalącym. Podłoga technologiczna z ramami do ustawienia ciężkich urządzeń. Przewiduje się też minimalną odporność ogniową - klasa EI30 (30 min) - tak jak dla pomieszczeń biurowych. Pomieszczenie to powinno być podzielone wzdłużnie podestem a stolarka budowlana powinna spełniać wymogi klasy EI 60 (60 minut) odporności ogniowej. W trosce o bezpieczeństwo należy ograniczyć ilość okien i zastosować okna antywłamaniowe. W celu zapewnienia szczelności pomieszczenia konieczne jest założenie czujników otwarcia okna podłączonych do lokalnego systemu alarmowego. Sufit serwerowni powinien być podwieszany i wykonany z materiału niepalnego i niepalącego. Ponadto konieczny jest podjazd umożliwiający wwiezienie ciężkich urządzeń. Zgodnie z wymogami konieczne jest też zapewnienie wydzielonego systemu kontroli dostępu. Wyposażenie serwerowni w przeszklone drzwi zagwarantuje kontrolę dostępu i możliwość monitorowania pomieszczenia przez nadzór administracyjny. Ograniczenie ruchu osobowego nastąpić powinno poprzez czytniki kart zbliżeniowych, klawiatury i biometrikę w dowolnej kombinacji. Można też, przewidzieć kolejne drzwi i rozbudować system kontroli dostępu. Drzwi transportowe powinny mieć minimalne wymiary 120x200 z odpornością ogniową, co

najmniej klasy EI60. Dodatkowym elementem systemu są zainstalowane kamery przemysłowe z możliwością cyfrowej rejestracji i archiwizacji zdarzeń. Powinny one umożliwić również monitorowanie pozostawionego otwartego okna. Za wykrywanie nieupoważnionego wtargnięcia na teren Data Center i ew. obszary sąsiadujące, transmisja alarmów do SMA Agencji Ochrony odpowiedzialny jest System Sygnalizacji Włamania i Napadu (SSWiN). Pełną kontrolę nad obiegiem kluczy do ważnych pomieszczeń w obiekcie może zapewnić System Elektronicznej Ewidencji Kluczy (np. produkt ATM). Jednak najlepszym systemem pozwalającym na zapewnienie optymalnych warunków temperatury i wilgotności jest centralny system klimatyzacji ogólnobudynkowej zapewniający około 1-2 wymian powietrza na godzinę. Taki system klimatyzacji powinien posiadać możliwości precyzyjnej regulacji temperatury i wilgotności oraz zdalne monitorowanie parametrów pracy urządzeń. Redundancja dla elementów systemu klimatyzacji powinna wynosić co najmniej N+1. Często jest też używany dodatkowy zewnętrzny klimatyzator ze ściennym układem nawiewu z możliwością zamknięcia dopływu świeżego powietrza na wypadek pożaru. Nadmuchiwanie powietrza powinien być umiejscowiony pod podłogą technologiczną a powrót sponad sufitu podwieszanego. Regulowane kratki podłogowe zapewnią lokalnie precyzyjny dobór ilości schłodzonego powietrza. Poza tym konieczny jest monitoring obecności wody na podłodze. Z uwagi na sezonową pracę takich urządzeń można też zamontować niezależny klimatyzator ścienny lub sufitowy wyposażony w klapy odcinające dopływ powietrza w kratce nawiewnej istniejącej klimatyzacji. Założenie takich klap ppoż. w istniejących anemostatach powinno być zintegrowane z centralną ppoż. lub systemem gaszenia. Dodatkowym zabezpieczeniem przeciwpożarowym jest centralne wykrywanie pożaru np. montując centralę IGNIS 1520 sterującą wyzwoleniem gazu obojętnego (gaz typu FM-200-bezpieczny dla ludzi i urządzeń) na wypadek pożaru i zintegrowanie systemu gaszenia z centralą budynkową. Ponadto system wykrywania i gaszenia pożaru powinien być wyposażony w czujki autonomicznego systemu gaszenia będącego niezależnym układem sterowania gaszeniem z własną centralą systemu wykrywania pożaru. Ważnym elementem bezpieczeństwa przeciwpożarowego są tabliczki informacyjne i ostrzegawcze oraz instrukcja postępowania na wypadek pożaru. Integracja wszystkich systemów technicznych zainstalowanych w obiekcie powinna być zaimplementowana na jednym, lub kilku stanowiskach komputerowych. Innym ważnym elementem tego systemu są interfejsy wykrywania i sygnalizacji pożaru budynku (SAP), systemu zarządzania budynkiem (SZB, BMS) oraz sterowania klimatyzacją i wentylacją. Zarówno zdalna (poprzez interfejs) jak i lokalna sygnalizacja optyczna i akustyczna powinny posiadać przyciski ręcznego zatrzymania

akcji gaśniczej i ręcznego wyzwolenia gazu. System gaszenia powinien zapewnić trzy fazy wykrywania z możliwością zatrzymania lub natychmiastowego rozpoczęcia akcji gaśniczej na każdym etapie. Powinien też być gotowy do ponownego użycia maksymalnie w ciągu 24 godzin od zadziałania. Innym zagadnieniem związanym z ochroną danych jest zapewnienie podtrzymania pracy wszystkich urządzeń Data Center, włącznie z klimatyzacją i oświetleniem. Konieczne jest zasilenie serwerowni w prąd z dwóch niezależnych źródeł zewnętrznych. Powinno to być zrealizowane poprzez zastosowanie zasilaczy UPS o redundancji co najmniej n+1 oraz agregatu prądotwórczego z co najmniej 8-godzinną autonomią i układem tankowania w biegu. Takie rozwiązanie zapewni kontynuację pracy Centrum w przypadku braku podtrzymania zasilania. System zasilania powinien zapewnić możliwość monitorowania, na stanowisku administratora, obciążenia poszczególnych faz zasilaczy UPS oraz awarii w rejonie. Wymagane są co najmniej po dwa obwody z każdego źródła na szafę zakończone listwami zasilającymi a szynoprzewody dla dużych gęstości upakowania mocy. Wszystkie elementy metalowe powinny być podłączone do wysokiej, jakości uziemienia. Zastosowanie zabezpieczeń odgromowych i przeciwprzepięciowych jest ważnym elementem bezpieczeństwa danych a zastosowanie opraw kierunkowych i ewakuacyjnych z podtrzymaniem zapewni bezpieczeństwo personelu.

Połączenia pomiędzy użytkownikami a pomieszczeniem serwerowni wykonane zostanie przy pomocy łączy światłowodowych, dwoma w pełni niezależnymi, co umożliwi bezprzerwowe przesyłanie danych z wykorzystaniem protokołów wszystkich np. Gigabit Ethernet i Fibre Chanel.

Okablowanie strukturalne to połączenie sieci komputerowych lub telefonów i urządzeń pracujących w tej sieci. Powinno być umieszczone w niezależnej od instalacji energetycznej sieci koryt pod podłogą technologiczną na pionowych wspornikach i zabezpieczone przed zalaniem. Zwykle do okablowania używa się skrętki 4-parowej, kabla koncentrycznego o impedancji 75Ω a obecnie coraz częściej światłowodów. Transmisja strumienia danych poprzez okablowanie kategorii 6 (1000BASE-TX - "skrętka") pozwala na uproszczenie urządzeń gdyż każde jest wyposażone tylko w dwa moduły nadawcze i dwa moduły odbiorcze. Dwie pary przesyłają dane z przepustowością 1 Gbit/s w jedną stronę, pozostałe dwie w przeciwną. Rzędy szaf powinny być niezależnie połączone światłowodami a okablowanie kat. 6 do szaf rozszyte na panelach krosowych używając poziomych i pionowych organizatorów kabli zachowując maksymalną odległość krosowania do 3m.

Wymogi systemu zarządzania Data Center

Polska norma (PN-ISO/IEC 27001) została przygotowana w celu przedstawienia modelu oraz ustanawiania, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji (ISMS). Wprowadzenie ISMS powinno być dla organizacji takiej jak MCPD decyzją strategiczną. Na projektowanie i wdrażanie ISMS w organizacji mają wpływ jej potrzeby i cele biznesowe, wymagania bezpieczeństwa, realizowane procesy oraz wielkość i struktura organizacji. Zarówno organizacje jak i systemy ją wspomagające zmieniają się w czasie. Przyjmuje się, że wdrożenie ISMS będzie dostosowane do potrzeb organizacji, np. prosta sytuacja wymaga prostego rozwiązania ISMS.

Niniejsza norma stosuje podejście procesowe w celu ustanawiania, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia ISMS w organizacji. Aby efektywnie funkcjonować, organizacja musi zidentyfikować i wykonać wiele działań. Działanie wykorzystujące zasoby i zarządzane w celu przekształcenia wejść w wyjścia może być rozpatrywane, jako proces. Często wyjście jednego procesu stanowi wejście kolejnego procesu. Zastosowanie systemu procesów w organizacji wraz z identyfikacją i interakcją tych procesów, a także zarządzanie nimi może być określone, jako „podejście procesowe”.

Podejście procesowe do zagadnienia zarządzania bezpieczeństwem informacji, przedstawione w niniejszej normie, zwraca uwagę jej użytkowników na szczególne zrozumienie wymagań bezpieczeństwa informacji w organizacji oraz ustanowienia zasad i celów bezpieczeństwa informacji, wdrożenie i eksploatację zabezpieczeń w celu zarządzania ryzykiem bezpieczeństwa informacji w kontekście całkowitego ryzyka biznesowego organizacji, monitorowanie i przegląd wydajności oraz skuteczności ISMS oraz ciągłe doskonalenia w oparciu o obiektywny pomiar. MCPD powinno ustanowić, wdrożyć, eksploatować, monitorować, przeglądać, utrzymywać i stale doskonalić system zarządzania bezpieczeństwem informacji ISMS (Information Security Management System) w kontekście prowadzonej działalności i ryzyka występującego w organizacji. MCPD powinno zdefiniować zakres i granice ISMS uwzględniając charakterystykę prowadzonej działalności, organizacją, jej lokalizację, aktywa i technologie, i dołączając dokładny opis i uzasadnienie dla każdego wyłączenia z zakresu.

Polityka ISMS powinna:

- uwzględniać charakterystykę prowadzonej działalności, organizacji, jej lokalizacji, aktywów i technologii, która zawiera ramy i ustalenia celów polityki oraz wyznacza ogólny kierunek i zasady działania w odniesieniu do bezpieczeństwa informacji,
- brać pod uwagę wymagania biznesowe oraz prawne lub o charakterze regulacyjnym, a także zobowiązania związane z bezpieczeństwem wynikające z umów,
- określać kryteria, według których ma być oceniane ryzyko,
- definiować podejście do szacowania ryzyka w organizacji,
- wskazywać metodę szacowania ryzyka, odpowiednią, dla ISMS,
- określać bezpieczeństwo informacji w kontekście prowadzonej działalności, wymagania prawne i wymagania nadzoru.

By efektywnie realizować politykę ISMS należy uzyskać autoryzację kierownictwa do wdrażania i eksploatacji ISMS (deklaracja stosowania). Deklaracja stosowania powinna zawierać, cele stosowania zabezpieczeń i wybrane zabezpieczenia oraz uzasadnienie ich wyboru a także zabezpieczenia już wdrożone oraz informację o wykluczeniu jakiegokolwiek celu stosowania zabezpieczeń.

Specyfika CMPD - Realizacja – strategia i cele biznesowe

Centrum Medyczne Przetwarzanie Danych może świadczyć swoje usługi w sektorze służby zdrowia. W początkowej fazie działalności sprowadzać się to będzie do outsourcingu zasobów informatycznych (hardware i software). Centrum zaprojektowane zgodnie z zasadami nadmiarowości będzie głównym dostawcą usług dla tego sektora. Projekt budowy CMPD zakłada zaproszenie do współpracy od kilku do kilkunastu wybranych szpitali w Województwie Dolnośląskim i sąsiednich aby wzorem innych państw skorzystali z doświadczeń UE i USA w zakresie wykorzystania informatyki w placówkach medycznych poprzez wykorzystanie technologii ASP (Application Server Provider) i Internetu. Obsługa informatyczna poszczególnych procesów w placówce medycznej powinna odbywać się na podstawie kontraktowania usług informatycznych. z wybranym w wyniku oferty i przetargu jaki będzie z udziałem Medical Data Center (MCPD). W MCPD winny być zainstalowane kompleksowe rozwiązania informatyczne wspomagające część administracyjną (tzw. systemy szare) oraz leczniczą (tzw. systemy białe). W okresie przejściowym może być w MCPD „wstawiane” oprogramowanie dotychczas eksploatowane w poszczególnych szpitalach. MCPD w tym okresie może zabezpieczać i archiwizować dane szpitali. Taka usługa ma za

zadanie poprawę bezpieczeństwa danych medycznych (beckapy), aż do stopniowego przejścia na jednolite dla wszystkich szpitali rozwiązania np. SAP for Healthcare, które będzie podstawą Zdalnodostępowego Systemu Informatycznego dla ZOZ. Po uruchomieniu projektu i wdrożeniu w okresie jego eksploatacji, koszty będą współdzielone przez beneficjentów projektu. Każdy ze szpitali będzie ponosił tylko część kosztów utrzymania systemu. Projekt takiego rozwiązania zakłada uzyskanie tzw. efektu skali co znacznie zmniejsza koszty jednostkowe korzystania z oprogramowania.

Usługi telemedyczne – skala i wolumetria

Potrzeby Szpitali wymuszają działania toczące się w innych sektorach biznesowych polegających na poprawie efektywności. Gwałtowne zwiększanie się dostępności komputerów powoduje, że są one wykorzystywane w rozmaitych zastosowaniach także w służbie zdrowia (w szpitalach oraz w prywatnych gabinetach POZ). Takie działania mają na celu poprawę efektywności i produktywności. Wkomponowują się one także w zapewnienie kompatybilności różnych systemów i informacji, a także w kwestie bezpieczeństwa i przestrzegania zasad polityki prywatności. W celu modernizacji infrastruktury informatycznej, elektronicznego obiegu dokumentów, archiwizacji dokumentów i rozwoju elektronicznych usług dla ludności, z zachowaniem bezpieczeństwa i prywatności. W tych działaniach Szpitale definiują swoje działania w obszarze poprawy jakości świadczeń zdrowotnych przekazując w outsourcing swoją działalność IT. Informatyzacja nie ominęła także środowiska medycznego, przejawiając się w m.in. w zakupach nowoczesnego cyfrowego sprzętu diagnostycznego oraz komputeryzacji usług i obsługi pacjentów w jednostkach służby zdrowia. Dostęp do informacji medycznej z wykorzystaniem telemedycyny (e-health) może bardzo istotnie wpłynąć na wzrost innowacyjności i konkurencyjności Regionu. Używanie sieci bezprzewodowych zostało już wdrożone z powodzeniem w kilku ośrodkach. Zatem dostęp do danych medycznych mogą mieć obecne technologie sieciowe oraz dostępne urządzenia przenośne klasy PDA.

Informatyzacja przejawia się również w intensywnym rozwoju infrastruktury sieci komputerowych, zarówno lokalnych, jak i sieci globalnej i zwiększania jej popularności powodując, że coraz więcej informacji z różnych dziedzin życia jest udostępnianych użytkownikom Internetu. Korzyści stąd płynące mogą i powinny dotyczyć także służby zdrowia, co wymaga jednak wdrażania właściwie zaprojektowanych systemów telemedycznych.

Należy zdawać sobie sprawę z tego, że specyfika danych medycznych stawia przed tymi systemami ogromne Wymagania. Polegają one, podobnie jak w systemach bankowych, na konieczności zapewnienia najwyższej poufności i integralności danych. Dodatkowo dane medyczne (jak graficzne wyniki badań pacjentów) są zazwyczaj dużej wielkości i wymagają do ich obróbki wydajnego sprzętu. Dodatkową komplikacją jest ich dostępność z wielu miejsc. Technologiczne zaawansowanie zarówno sprzętu mobilnego jak i możliwości sieci wydają się już na tyle duże, że pozwalają na efektywne ich wykorzystanie w telemedycynie. Skomputeryzowane systemy kliniczne oferowane przez Centrum Medyczne Przetwarzania Danych zagwarantują swoją strukturą świadczenie zaawansowanych usług telemedycznych. Mogą w ten sposób udzielać wsparcia osobom zawodowo zajmującym się zdrowiem i zapewnić ciągłość opieki. Takie inteligentne systemy pozwalają obywatelom na przejęcie większego uczestnictwa i odpowiedzialności za swoje własne zdrowie.

Jeśli chodzi o zawodową służbę zdrowia to systemy te zwiększają umiejętności osób zawodowo pracujących w służbie zdrowia odnośnie zapobiegania i diagnostyki. Telemedycyna stosowana z powodzeniem w innych państwach UE pozwoliła uprawnia do wniosków polegających między innymi na gwarancji odpowiedniego poziomu opieki i wspomagania rehabilitacji. Inteligentne systemy nieinwazyjnej diagnozy i terapii a także pomoce medyczne są podstawowym narzędziem telemedycyny. Stosowane w nich zaawansowane metody obrazowania medycznego pozwalają na dostęp do danych medycznych wymagających wizualizacji. Zaawansowane zastosowania telemedycyny to na przykład „wirtualne zakłady opieki zdrowotnej” oferujące dostęp do usług przy pomocy jednego punktu dostępu. w nagłych wypadkach do łączenia usług pomocy konieczne są szybkie zabezpieczone sieci gwarantujące dostęp do aplikacji szpitali, laboratoriów oraz aptek. Systemy zarządzania przepływem informacji w służbie zdrowia powinny być łatwe w stosowaniu i o przystępnej cenie. Elektroniczne rejestry zdrowia nowej generacji oraz karty dla nowoczesnych obiektów danych zdrowotnych; osobiste systemy zdrowotne muszą być dostępne oraz przyjazne dla użytkownika. Podobnym warunkom muszą również odpowiadać systemy monitorowania zdrowia osobistego oraz stałe lub przenośne systemy zapobiegania obejmujące zaawansowane i dostępne czujniki, przetworniki i mikro systemy. Telesystemy i aplikacje do wspierania opieki we wszystkich kontekstach muszą być przyjazne użytkownikowi. Z kolei wspomaganie edukacji zdrowotnej i świadomości zdrowotnej obywateli musi być zapewnione przez kwalifikowane systemy informacyjne. Wraz z

działaniami pierwszych użytkowników i innymi inicjatywami najlepszej praktyki systemy powinny być aktualizowane przez podejmowanie działań obejmujących walidacje i oceny.

Usługi e-learningu

MCPD realizując swoje zadania statutowe powinno używać współczesnych metod szkolenia swoich pracowników i użytkowników. Zdalne nauczanie (e-learning) jest jednym z głównych kierunków rozwoju e-usług publicznych spełniających specyficzne wymagania obywateli poprzez użycie nowych technologii komunikacyjnych (ICT). Jest to dynamicznie rozwijająca się metodologia umożliwiająca udostępnianie informacji na dowolny temat w dowolnym czasie. E-learning jest jednym z najbardziej dynamicznie rozwijających się obszarów edukacji. Jego funkcjonowanie opiera się głównie na dwóch podstawowych technikach. Główna technika e-learningu wykorzystuje materiały nauczające o często złożonej strukturze, które udostępniane są poprzez serwery WWW. Nauczający tworzy dokumenty na określony temat, przewiduje ich podział na jednostki nauczające (lekcje), wzbogaca je poprzez ćwiczenia lub zadania i kontroluje postęp nauki formułując sprawdziany lub egzaminy. Takie materiały nauczające mogą mieć złożoną strukturę i wymagają odpowiednich standardów do zdefiniowania formatu plików, aby umożliwić ich wymianę i wykorzystanie. Rozpowszechnianie materiałów opiera się w tym przypadku na standardowych systemach WWW i protokołach komunikacyjnych, takich jak HTTP. Tradycyjny wykład prezentowany przez wykładowcę może być również nagrywany jako dokument audiowizualny i rozpowszechniany jednocześnie (online) lub z opóźnieniem (off-line) za pomocą strumieni multimedialnych do grupy uczących się. Obraz i dźwięk wykładowcy może być wzbogacony poprzez inne materiały nauczające, takie jak przeźrocza PowerPoint, tworząc złożoną strukturę multimedialną, w której każdy element zawartości jest zsynchronizowany w czasie tak, aby jego prezentacja wypadła w odpowiednim momencie. Technologie umożliwiające realizację takich funkcji (RealNetworks SMIL - W3C), \ definiują zsynchronizowane dokumenty multimedialne. Wraz z rozwojem technik multimedialnych usługa ta ma coraz szersze zastosowanie. Począwszy od funkcji informacyjnej po edukacyjną. Realizowana przez Centrum Medyczne może mieć ogromne znaczenie w nauczaniu i informowaniu użytkowników. Nowym narzędziem, które zyskuje coraz większe powodzenie w rozpowszechnianiu wykładów dźwiękowych jest podcast, dzięki któremu można otrzymać nagrania dźwiękowe w formacie MP3. Pomimo dynamicznego rozwoju, e-learning nie osiągnął jeszcze możliwej do uzyskania popularności i efektywności. Istnieje kilka przyczyn

takiego stanu rzeczy. Używane metody przedstawiają tradycyjny asymetryczny model nauczania. W wypadku nauczania typu online, wymagana jest jednoczesna obecność nauczającego i uczących się. Nauka odbywa się w izolacji i zwykle brak jest koordynacji i komunikacji pomiędzy nauczycielem i uczącym się. Aktualne rozwiązania wymagają stosunkowo dużych inwestycji (sprzęt do nagrywania, serwer WWW), nakładów operacyjnych (zarządzanie, uaktualnianie informacji) i specjalistycznej obsługi. Wykłady takie nie są szeroko rozpowszechnione z uwagi na potrzebę zastosowania wyspecjalizowanych narzędzi i potrzebną wiedzę techniczną do ich użytkowania. Zaletą techniki zdalnego nauczania jest pewnego stopnia niezależność uczącego się od nauczającego. Uczący się może korzystać z materiałów w dowolnej chwili. Nauka często wymaga jednak pomocy nauczającego, co może być realizowane poprzez narzędzia komunikacyjne, takie jak e-mail, forum, czat. Oznacza to, że nowe standardy zaczynają być używane do integrowania materiałów w tym typie zdalnego nauczania. Podstawowe rozwiązania e-learningu, jak już wspomniano, opierają się na wypróbowanych tradycyjnych technikach WWW lub na przesyłaniu strumieni multimedialnych. Jako element, który mógłby wzbogacić funkcjonalność systemów e-learningu, obecnie rozwarzane są techniki typu peer-to-peer (P2P)(http://www.e-mentor.edu.pl/artukul_v2.php?numer=17&id=353). Mogą one pozwolić na łatwe i szybkie rozpowszechnianie materiałów, tworzenie się grup współpracy uczących się i uczenie się poprzez współpracę. Możliwa jest również łatwa komunikacja pomiędzy wszystkimi uczestnikami (autor, nauczający, uczący się). Metoda ta będzie wymagać najprawdopodobniej równoczesnego użycia nowych środków komunikacji, takich jak telefonia internetowa (VoIP) zintegrowana z technikami P2P.

Usługi telekomunikacyjne

Inną grupą usług o potencjalnym zastosowaniu w MCPD są usługi telekomunikacyjne. Podstawą komunikacji w przedsiębiorstwie od wielu lat były: łączność telefoniczna, zapewniająca transmisję głosu, i łączność faksowa do przesyłania danych. Wraz z rozwojem infrastruktury telekomunikacyjnej i pojawianiem się nowych aplikacji niezbędnym elementem do komunikacji w przedsiębiorstwie stał się dostęp do Internetu. Sama sieć Internet również przyczyniła się do dynamicznego rozwoju usług telekomunikacyjnych. Pojawiły się nowe usługi umożliwiające komunikowanie się poprzez sieć komputerową. Początkowo była to poczta elektroniczna (e-mail). Następnie pojawiały się aplikacje będące komunikatorami tekstowymi, które w kolejnych uaktualnieniach posiadały również możliwość komunikowania się głosem. To był zaledwie mały krok od popularnej obecnie

telefonii internetowej opartej na protokole VOIP. Połączywszy wspomniane usługi z obrazem w czasie rzeczywistym z kamery otrzymamy narzędzie multimedialnej telekomunikacji. Może być ono wykorzystane również jako narzędzie e-learningu w celu interaktywnej prezentacji np., wykładów, seminariów a nawet zabiegów medycznych. Redundantna struktura centrum, zwłaszcza jeśli chodzi o przepustowość łączy, będzie doskonałym miejscem dla tego typu usługi multimedialnej. Systemy transmisyjne o wysokiej przepływności w sieciach szkieletowych (SDH, ATM) nie są wystarczającym środkiem, aby zapewnić szerokie pasmo abonentowi sieci IP. Do zapewnienia dużego ruchu w sieci, oprócz skalowanych urządzeń komutacyjnych instalowanych w węzłach sieci transportowej (przełączniki, routery i terakomutatory), są potrzebne sieci dostępowe o różnych szybkościach działania. Niezależnie od używanego medium przekazu (miedź, światłowód czy fale radiowe) najbardziej ogólny podział abonenckich sieci dostępowych obejmuje trzy grupy systemów transmisyjnych, umożliwiające usługi o zróżnicowanych przepływnościach:

Usługi telemonitoringu

Kolejnym elementem powyższego podejścia usług które mogą być wdrożone w MCPD jest telemonitoring. W ramach tej usługi może być obsługiwanych wielu pacjentów, którzy wymagają pomocy ze względu na długotrwały proces leczenia skomplikowanych schorzeń. Ich leczenie pochłania dużą ilość środków oraz czasu. Potencjalne usługi MCPD w zakresie usług telemonitoringu polegają na monitorowaniu procesu leczenia. Usługa ta może mieć zastosowanie w różnych dziedzinach medycyny takich jak kardiologia <ekg> spirometria I glukometria. Działają one według jednego schematu. Głównie elementy to centrum gromadzenia danych i diagnozowania (lub też centrum konsultacyjne) oraz rozproszona sieć placówek/odbiorców/pacjentów. Korzystają one z centrum w różnych konstelacjach a wspólnym mianownikiem dla wszystkich teleusług monitoringu może być sposób przesyłu informacji i format tej informacji (np zdjęcie, film z koronarografii czy tylko prosty zapis EKG lub wartość liczbowa poziomu cukru.

Przykładem może też być pomysł polegający na tym, że za pośrednictwem domowej telewizji zaproponowano rozwiązanie umożliwiające zdalne prowadzenie pacjentów, które zapewnia im zindywidualizowaną opiekę zdrowotną. Nie nakłada to na pacjenta obowiązku regularnego odwiedzania placówek służby zdrowia.

Dla zwiększenia bezpieczeństwa oraz poprawienia nadzoru nad tym procesem wykorzystuje się metody telemedyczne. Podobnym przykładem jest rehabilitacja kardiologiczna (RK) prowadzona w warunkach domowych. Jest ona jedną z nowoczesnych form i alternatyw w

postępowaniu z pacjentem ze schorzeniami układu sercowo-naczyniowego. Możliwość realizacji programu RK w warunkach domowych stwarza szansę na uczestniczenie w tym procesie terapeutycznym pacjentom, którzy nie mogą skorzystać z różnych powodów z RK stacjonarnej lub też ambulatoryjnej np. z powodu zbyt dużej odległości ośrodka od miejsca zamieszkania. Podobnie i w tym przypadku w warunkach domowych wykorzystano telekardiologię jako metodę kontroli.

Doskonałym narzędziem może być tutaj struktura teleinformatyczna w postaci rozbudowanej obecnie sieci z dostępem do Internetu oraz infrastruktura MCPD. Zaprojektowane na zasadzie nadmiarowości Medyczne Centrum Przetwarzania Danych wraz z wysoko wyspecjalizowanym personelem będzie doskonałym koordynatorem takich działań.

Aplikacja ASP dla e-Zdrowia

Jednocześnie przewiduje się stopniową rezygnację z użytkowania systemów aktualnie eksploatowanych, związku z bardzo wysokimi kosztami rozszerzenia funkcjonalności tych systemów. W to miejsce proponuje się rozwiązanie podobnie technologicznie do w pełni zintegrowanego systemu „SAP for Healthcare”. Takie rozwiązanie umożliwi zmianę funkcjonowania szpitali z zapewnieniem jakości obsługi pacjentów.

System SAP dla służby zdrowia zapewnia pełną integrację części administracyjnej i szpitalnej. Firma SAP wdrożyła na całym świecie ok. 850 instalacji systemu „SAP for Healthcare”. System ten oferuje pełne i naturalne połączenie części administracyjnej (szarej) z częścią szpitalną (białą). Rozwiązanie to stosowane jest zarówno w dużych szpitalach uniwersyteckich jak i w małych szpitalach specjalistycznych. Rozwiązanie to obsługuje wszystkie procesy związane z działalnością szpitala, a jego zalety można opisać w kilku grupach. Jedną z nich jest zarządzanie i koordynacja opieki nad pacjentami od rejestracji i przypisania łóżek po informowanie pacjentów. Inną jest dostęp do funkcji internetowych służących do zarządzania danymi pacjentów, dostarczających danych do diagnozowania i leczenia. Kolejna grupa to analiza przypadków chorobowych, rozwój i wprowadzanie w życie metod leczenia oraz dokumentowanie opieki szpitalnej. Waznym elementem jest też komunikacja online z oferentami, płatnikami, pacjentami, lekarzami ogólnymi, szpitalami i dostawcami oraz wykorzystanie zalet obszernej hurtowni danych i związanych z nią funkcji do planowania docelowego, kalkulacji zasobów i przypadków oraz zarządzania wynikami.

Poza tym istotne jest skupienie działań związanych z zarządzaniem relacjami z klientami na pacjentach, lekarzach zewnętrznych, pracownikach, dawcach itp.

Należy zaprosić, na warunkach komercyjnych, do skorzystania z doświadczeń i współużytkowania systemu również szpitale spoza stowarzyszenia. Z punktu widzenia ZOZ i palnika celowe jest utworzenie Ogólnopolskiego Systemu Informatycznego dla ZOZ.

Zawarcie umowy outsourcingowej przynosi Zleceniodawcy wiele korzyści.

Umożliwia uniknięcie dużych jednorazowych wydatków inwestycyjnych mogących dramatycznie wpłynąć na wskaźniki płynności. Powoduje zmniejszenie kosztów utrzymania własnej infrastruktury informatycznej (pomieszczenia, pracownicy, oprogramowanie). Lepsza jest również ochrona przetwarzanych danych oraz istnieje możliwość przerzucenia na firmę usługową konieczności modernizowania oprogramowania. Takie rozwiązanie umożliwia skupienie się na działalności podstawowej a planowanie budżetu wydatków na informatyzację jest łatwiejsze ze względu na stałą opłatę.

Prawne uwarunkowania outsourcingu jako formy usług IT.

Outsourcing określa nowy sposób myślenia, który przekłada się na korzyści gospodarcze podmiotów, które umiejętnie go stosują, wykorzystując elementy specjalizacji, koncentracji i konkurencji. CMPD może w ten sposób prowadzić działalność gospodarczą umożliwiającą jego rozwój. Oczywiście, nie każdy obszar działalności w równej mierze podatny jest na zastosowanie tej formuły, tym niemniej coraz wyraźniej odchodzi w przeszłość myślenie oparte na przekonaniu, iż jednym z warunków sukcesu szpitala jest to, by we własnym gospodarstwie posiadała wszystko, co może jej być potrzebne w pracy. Tym samym rośnie rola instrumentów cywilnoprawnych, niezbędnych do zapewnienia sobie dostępu do usług świadczonych przez podmioty zewnętrzne, ich właściwej jakości i bezpieczeństwa. Począwszy od lat 80. rośnie znaczenie outsourcingu, jako swoistej manifestacji koncentracji firm na podstawowym przedmiocie działalności, w odróżnieniu od uprzednio lansowanej tendencji do dywersyfikacji działalności.

Istotą i zarazem efektem outsourcingu winno być wykonywanie pewnej usługi lub funkcji danego przedsiębiorstwa przez inne przedsiębiorstwo, które czyni to lepiej, szybciej i taniej. Czy tak ostatecznie się dzieje, w dużej mierze zależy od osoby dostawcy oraz wynegocjowanych warunków kontraktu. W miarę wzrostu popularności outsourcingu częste stało się używanie tego terminu w rozmaitych kontekstach. Outsourcing stał się jednym ze słów-wytrychów na oznaczenie różnych typów kontraktu handlowego na świadczenie usług.

Aplikacje klasy ERP i EHR dla szpitali

W Polsce Electronic Health Record tłumaczony jest bardzo różnie, np.: Medyczny zapis cyfrowy, Elektroniczna książka zdrowia. Elektroniczny Rekord Zdrowotny Elektroniczny rekord Pacjenta (ERP). Jest on ogromną 'porcją' danych dotyczących pojedynczego pacjenta, która wirtualnie wędruje za pacjentem. EHR winien zawierać wszelkie informacje dotyczące identyfikacji pacjenta, określenia etapów jego opieki zdrowotnej, w tym dane o lekarzach, instytucjach i świadczeniodawcach, z jakimi pacjent był lub jest związany.

W dzisiejszych czasach mobilność staje się czymś bardzo naturalnym, a zatem informacja potrzebna do zachowania kompletności EHR. Elektroniczny Rekord Zdrowia jest pomostem pomiędzy świadczeniodawcą usług zdrowotnych a ich odbiorcą. Umożliwi on lekarzom stały dostęp przez Internet do kartoteki chorobowej pacjenta, a tym samym pozwoli na uzyskanie wiedzy o stanie zdrowia pacjenta w przeszłości, chorobach, które przeszedł, przebiegu leczenia, zapisanych lekach, itp. Ma to szczególne znaczenie wobec mobilnego charakteru procesów biznesowych i przemieszczania się ludzi w celach turystycznych. Bez pełnego zapisu Elektronicznego Rekordu Zdrowia wiedza o pacjencie jest niepełna, a to skutkować może niedopasowaną diagnozą. Katalog informacji jaki zawarty powinien być w EHR jest tak ogromny, iż wymaga globalnego spojrzenia na opiekę zdrowotną nie tylko w mieście, z którego pacjent pochodzi, czy gdzie się leczy, ale także danego kraju, czy całego układu w rozumieniu na przykład struktur Unii Europejskiej. Możliwe jest również użycie systemu słowników dzięki którym lekarz w dowolnym miejscu w Europie będzie mógł diagnozować pacjenta we własnym języku. Dzięki temu pacjent będzie miał pewność, że leczony będzie w sposób najbardziej efektywny, uwzględniający wszelkie przeciwwskazania wynikające z wcześniej wykrytych problemów zdrowotnych.

Wdrożenie tej usługi stanowić będzie zatem przełom w funkcjonowaniu służby zdrowia na terenie Polski. Dostosuje ją do standardów europejskich a także tych dotyczących rozwoju społeczeństwa informacyjnego. Realizacja przedmiotowej usługi stanowić będzie wersję pilotażową, która obejmie przede wszystkim województwo dolnośląskie, ale w następnych etapach może objąć pozostałe województwa w kraju.

Aplikacja dla administracji, statystyki publicznej i ewidencji zasobów zdrowotnych e- Zdrowie

Implementacja EHR na poziomie kraju jest zadaniem wyjątkowym. Służyć temu musi polityka rządu i odpowiednich jednostek odpowiedzialnych za politykę zdrowotną w danym kraju. W Polsce są to głównie Ministerstwo Zdrowia oraz Centrum Systemów Informacyjnych Ochrony Zdrowia. Sporządzenie i podpisanie dokumentacji prowadzonej w postaci elektronicznej polega na zapisaniu sekwencji danych na elektronicznym nośniku informacji i podpisaniu tych danych, zgodnie z ustawą z dnia 18 września 2001 r. o podpisie elektronicznym. W celu zachowania czytelności i standaryzacji zapisu danych dokumentacja powinna być sporządzona w formacie XML. Dla oznaczenia daty sporządzenia dokumentu, złożenia podpisu na dokumencie oraz w celu zachowania chronologii wpisów w dokumentacji zbiorczej wewnętrznej stosuje się znacznik czasu, zgodnie z ustawą z dnia 18 września 2001 r. o podpisie elektronicznym. Jeśli do dokumentacji konieczne jest załączenie innych dokumentów medycznych, dokumenty te przenosi się na elektroniczny nośnik informacji, opatruje podpisem elektronicznym i umieszcza się w elektronicznych zbiorach danych w sposób zapewniający dostęp i powiązanie pomiędzy dokumentami. Utrwalenie dokumentacji prowadzonej w postaci elektronicznej polega na jej zapisaniu na elektronicznym nośniku informacji w sposób zapewniający sprawdzenie jej integralności, możliwości weryfikacji podpisu elektronicznego lub danych identyfikujących oraz możliwość odczytania wszystkich informacji zawartych w tej dokumentacji, aż do zakończenia okresu przechowywania dokumentacji. Udostępnianie dokumentacji prowadzonej w formie elektronicznej może nastąpić przez przekazanie elektronicznego nośnika informacji, na którym została utrwalona dokumentacja, lub dokonanie elektronicznej transmisji dokumentacji. Dokumentację prowadzoną w formie elektronicznej udostępnia się z zachowaniem jej integralności oraz ochrony danych osobowych. Dokumentacja udostępniania pacjentom oraz organom i podmiotom uprawnionym na podstawie odrębnych przepisów powinna być opatrzona bezpiecznym podpisem elektronicznym weryfikowanym za pomocą kwalifikowanego certyfikatu, zgodnie z ustawą z dnia 18 września 2001 r. o podpisie. Strona przyjmująca potwierdza otrzymanie udostępnionej dokumentacji elektronicznej podpisem odręcznym lub podpisem elektronicznym zgodnie z ustawą z dnia 18 września 2001 r. o podpisie elektronicznym.

Administracja Centrum Medycznego powinna podjąć działania monitorowania i przeglądu ISMS. Procedury z tym związane i inne zabezpieczenia mają na celu natychmiastowe

wykrywania błędów w wynikach przetwarzania oraz identyfikowanie naruszeń bezpieczeństwa i incydentów, zakończonych niepowodzeniem lub sukcesem. Kierownictwu powinno mieć możliwość stwierdzenia, czy działania związane z bezpieczeństwem delegowane są na poszczególne osoby lub wdrożone za pomocą środków informatycznych są wykonywane zgodnie z oczekiwaniami. Użycie wskaźników pomocy w wykrywaniu naruszeń bezpieczeństwa ma na celu niedopuszczenie do incydentów bezpieczeństwa.

Może to polegać na określeniu czy działania podjęte w celu stwierdzenia naruszeń bezpieczeństwa były efektywne. Regularne przeglądy efektywności ISMS, w tym zgodności z polityką i celami ISMS oraz przegląd zabezpieczeń, powinny brać pod uwagę wyniki audytów bezpieczeństwa, rezultatów incydentów, pomiarów efektywności, sugestii oraz informacji zwrotnych od wszystkich zainteresowanych stron. Dokonywanie pomiarów efektywności zabezpieczeń w celu ich weryfikacji zgodności z wymaganiami bezpieczeństwa oraz przegląd szacowania ryzyka w zaplanowanych odstępach czasu, przeglądy ryzyka szacunkowego oraz przeglądu poziomów ryzyka akceptowalnego, powinny brać pod uwagę zmiany w organizacji, technologii, celów biznesowych i procesów, zidentyfikowanych zagrożeń, efektywności wdrożonych zabezpieczeń, zewnętrznych zdarzeń, takich jak zmiany prawa lub stosownych regulacji, zmian wynikających z umów oraz zmiany o charakterze społecznym.

Wewnętrzne audyty ISMS powinny być przeprowadzane w zaplanowanych odstępach czasu, przez lub w imieniu Centrum na potrzeby wewnętrzne. Przeglądy ISMS realizowane przez kierownictwo należy podejmować w regularnych odstępach czasu tak aby ich zakres był odpowiedni do potrzeb.

Analiza konkurencji

W Polsce w zasadzie nie istnieje zdecydowana konkurencja dla CMPD i to z dwóch powodów. Przede wszystkim, z powodu braku konkurencji, nie istnieje jeszcze rynek Centrów Medycznych Przetwarzania Danych. Szereg dostawców oprogramowania dla szpitali wprowadza już pewne elementy jednak nie jest to jeszcze gotowy integrowany system EHR. Po połączeniu szpitali do CMPD powstanie jednorodna struktura logiczna. Na początku może być z różnymi systemami informatycznymi. Jednak dla poprawy konkurencyjności oraz w celu zapewnienia płynnej pracy szpitala systemy te należy połączyć. Procesy integracyjne i administracyjne a głównie ich obsługa poprzez typowe systemy tzw. szare będzie

przebiegała w etapach. Proponowany harmonogram wdrożenia systemu informatycznego dla połączonych szpitali podzielono na etapy. Obejmują one modernizację istniejącego systemu informatycznego, kolokację serwerów z oprogramowaniem w Data Center z wykorzystaniem SAP oraz wykorzystanie regionalnego systemu informatycznego dla ZOZ na zasadach ASP. Celem realizacji MCPD jest utworzenie/przystosowanie systemu informatycznego obsługującego w jednolity sposób grupę szpitali. Musi nastąpić wybór i wyskalowanie architektury systemu oraz aplikacji dla połączonych szpitali. Ważnym zadaniem jest połączenie lokalnych sieci (LAN) Szpitali w jedną rozległą sieć WAN. Z zadaniem tym związany jest zakup urządzeń aktywnych oraz organizacja zestawienia łączy teleinformatycznych (łącza sztywne, dzierżawione, szerokopasmowy Internet). Użytkownikowi pozostaje tylko okresowa wymiana danych między dwoma systemami poprzez pliki tekstowe i odpowiednie wczytywanie ich przez interfejsy wewnętrzne systemów. W kolejnym etapie nastąpi przeniesienie niektórych serwerów użytkowanych w szpitalach do MCPD. Rozwiązanie to ma szereg zalet. Szpital nie ponosi wówczas kosztów utrzymania własnej infrastruktury technicznej. Serwery pracują w optymalnych warunkach (temperatura, wilgotność) i podlegają całodobowej ochronie przed atakami hakerów. Szpital ma zapewniony ciągły serwis techniczny i zapewnione jest bezpieczeństwo zasilania. Poza tym zapewniona jest szybka i bezpieczna łączność z Internetem. Przy budowie łączności z MCPD wykorzystane byłyby elementy zbudowane w trakcie łączenia szpitali w etapie I. Rozwiązanie takie pozwala uniknąć olbrzymich kosztów związanych z budową i utrzymaniem własnych, nowoczesnych pomieszczeń DATA CENTER. Usługę kolokacji można połączyć z założeniem skrzynek pocztowych dla pracowników szpitala oraz z utrzymaniem strony WWW.

Cennik usług

Opierając się na japońskim medycznym centrum przetwarzania danych, którego roczny budżet wynosi 400 milionów jenów (ok. 9 milionów PLN). Całkowite zatrudnienie w Centrum wynosi 68 osób personelu (w tym 49 osób zatrudnionych na stałe) oraz pięcioosobowe kierownictwo. Przy czym główne zadanie polega na serwisowaniu danych w zakresie statystyki medycznej. Działalność Centrum jest wspierana przez 5 banków oraz około 12 głównych udziałowców włączając kierownictwo.

DATA CENTER BELLATRIX oferuje usługi profesjonalnej kolokacji serwerów każdego rodzaju, od wolnostojących po 7U. Zabezpieczenia i infrastruktura zapewnia maksymalne bezpieczeństwo, bezawaryjność i praktycznie nieograniczony transfer danych.

DATA CENTER BELLATRIX zapewnia szereg usług w ramach kolokacji. Dobowy backup danych, dedykowany firewalling, dowolna ilość adresów IP a także na życzenie Klienta system VirtualAdmin do pełnej administracji serwerem przez www.

DATA CENTER BELLATRIX świadczy pełne usługi outsourcingu, gwarantując kompleksową i stojącą na najwyższym poziomie obsługę Klientów.

1. KOŁOKACJA

- opłata instalacyjna za podłączenie serwera: 500 zł
- opłata miesięczna za serwer wolnostojący: 150 zł*
- opłata miesięczna za serwer RACK 2U: 200 zł**

2. SERWERY FIZYCZNE

- jednorazowa opłata za udostępnienie serwera: 1.490 zł***
- opłata miesięczna za serwer wolnostojący: 150 zł*
- opłata miesięczna za serwer RACK 2U: 200 zł**

3. SZAFY RACK

- jednorazowa opłata za udostępnienie szafy RACK 42U: 2.000 zł
- opłata miesięczna: 2.000 zł****

4. POZOSTAŁE OPŁATY

ROZLICZENIA ZA ZUŻYTY TRANSFER DANYCH

- za każdy rozpoczęty 1 GB transferu powyżej 5 GB: 9 zł
- j/w za każdy 1 GB powyżej 50 GB: 8 zł
- j/w za każdy 1 GB powyżej 90 GB: 7 zł
- powyżej 120 GB ceny negocjowane indywidualnie

ROZLICZENIA ZA PRZYDZIELONE PASMO (EIR=CIR)

- opłata miesięczna za 256 kbps: 390 zł
- opłata miesięczna za 512 kbps: 740 zł
- opłata miesięczna za 1 mbps (i każdy następny): 990 zł

- 10 dodatkowych adresów IP: 250 zł/rocznie
- powyżej 10 adresów ceny negocjowane indywidualnie

- VirtualAdmin (zamiast root): 50 zł/miesięcznie
- backup dobowy: 90 zł/miesięcznie

serwis

- reset "twardy": 25 zł
- wymiana, instalacja dysku, pamięci itp.: 50 zł
- pozostałe zlecenia: 100 zł/godzina pracy

Koszt serwisu w godz. 17:00-8:00 oraz w soboty i dni wolne jest wyższy o 200%.

*W cenie 5 GB transferu miesięcznego, jeden adres IP

**W cenie 5 GB transferu miesięcznego, jeden adres IP, za serwer 4U opłata razy 2 itd...

***W ramach podstawowego pakietu serwer fizyczny zawiera procesor Intel Celeron D 2.267 GHz, Dysk WD Caviar 80GB 7200 8MB SATA, Pamięć DDR 512MB PC2700

****Cena nie obejmuje pasma

Wszystkie ceny netto!

Inne specyficzne usługi lub takie, które organizowane są dla grupy użytkowników, powinny być kalkulowane indywidualnie.

Podsumowanie

Według przedstawionego stanu zastosowań i rynku usług jaki przedstawiają Cetra danych należy z pełną odpowiedzialnością stwierdzić, że projekt CMPD to inwestycja w przyszłość i

oferta dla szerokiego spektrum usług medycznych, szczególnie nowych usług, których uruchomienie jest warunkowane sprawnym działaniem CMPD.