

## **Internet medyczny i telemedycyna – wpływ nowych środków komunikacji na współczesne oblicze medycyny.**

Piotr Kasztelowicz <Piotr.Kasztelowicz@am.torun.pl>  
Polskie Stowarzyszenie Internetu Medycznego  
Oddział Gruźlicy i Chorób Płuc, Wojewódzki Szpital im. Ludwika Rydygiera w Toruniu

**T**echnologia komputerowa stała się na przełomie wieku dziedziną, którą określa się jako definiującą rozwój społeczeństwa<sup>1</sup>, technologią wszechobecną we wszystkich dziedzinach ludzkiego życia. Szerokie zastosowanie komputerów nie ominęło także medycyny. Zdążyliśmy się już przyzwyczaić i w pełni zaakceptować obecność mikroprocesorów w przyrządach diagnostycznych i terapeutycznych, stosowania programowanych urządzeń wszczepianych do narządów pacjenta, wykorzystywania komputera do prowadzenia codziennej pracy lekarskiej i badań naukowych. Najnowszym zjawiskiem w dziedzinie komputeryzacji są sieci komputerowe, z których Internet po 1994 roku „wygrał walkę o prymat” z pozostałymi, rozwijającymi się do tego czasu równoległe sieciami. Dziś już tak naprawdę do końca nie da się ustalić kiedy narodził się Internet w szerokim tego słowa znaczeniu – choć datę roku 1983, w którym ostatecznie internetowy protokół wymiany danych (czyli protokół TCP/IP) został przyjęty jako ogólnie obowiązujący standard i włączony do systemu operacyjnego UNIX można byłoby określić jako narodziny Internetu znanego w dzisiejszej postaci. Medycy, co jest istotne, nie tworzyli i nie tworzą w zasadzie technologii informatycznych, ponieważ jest to domena informatyków. Ten fakt także wskazuje jaka może być rola lekarzy i innych profesji medycznych zarówno w przyczynianiu się do rozwoju informatyki jak i korzystaniu z niej. Stopień umiejętności korzystania z nowoczesnych technologii w medycynie będzie wynikał z umiejętności zaadoptowania istniejących rozwiązań do wykorzystania ich w medycynie – w szczególności we wzajemnej komunikacji pomiędzy lekarzami (a więc wykorzystaniu jej do celów edukacyjnych) lub w komunikacji lekarz pacjent – czyli telemedycynie. Nowe wyzwania tworzą także nowe problemy prawne, etyczne i praktyczne. Wraz z szerokim rozprzestrzenieniem się sieci komputerowych i komputerów w ogóle pojawiły się takie problemy jak wirusy komputerowe, włamywanie się do systemów komputerowych, nielegalne kopiowanie oprogramowania i danych, awarie systemów i ich konsekwencje, niezgodność formatów danych, błędy w oprogramowaniu. Problemem, który w bieżącym roku obiegł i złączył we wspólnej z nim walce całą kulę ziemską był problem roku 2000, czyli niezgodności formatu daty, który na szczęście wyrządził znacznie mniej strat, niż się wcześniej spodziewano. Zaistnienie takiego faktu zwraca uwagę na szereg uwarunkowań związanych z tworzeniem globalnego społeczeństwa informatycznego oraz wskazuje na skalę uzależnienia strategicznych dziedzin rozwoju świata – w tym także medycyny – od technologii cyfrowej.

### **Telemedycyna – nowe pojęcia**

Telemedycyna powstała przed erą komputerów wraz z pojawieniem się telefonu<sup>2</sup>. Już wówczas pojawiły się pierwsze dyskusje na temat, czy telefon może być i w jakim stopniu wykorzystywany do komunikacji lekarz-lekarz, lekarz-pacjent – czyli diagnozowania i leczenia na odległość. Prawdziwy jednak rozwój telemedycyny nastąpił dopiero w erze sieci komputerowych. Istotnym elementem tego rozwoju są sieci wirtualne tworzone w

środowiskach medycznych. Z tym wiążą się nowe pojęcia<sup>3</sup> takie jak „*electronic work groups*”, „*virtual teams*” czy „*network organizations*”. Terminy te określają nowe formy współpracy opierające się na tworzeniu wirtualnego społeczeństwa, przy czym pojęcie *wirtualny* określane jest jako „działający i zmieniający rzeczywistość ale nie będący fizycznie w danym miejscu, gdzie to oddziaływanie następuje, w sensie faktycznej obecności”.

### Telemedycyna w aspekcie organizacyjnym

Jeśli pojęcie wirtualny rozumieć jako „oddziaływający i zmieniający rzeczywistość choć nieobecny fizycznie” to pod pojęciem wzajemne relacje<sup>3</sup> takich oddziaływań tworzą wirtualną sieć. Nie trzeba się domyślać, że zwłaszcza w tak istotnej dziedzinie jak medycyna powstawanie takich sieci wymaga specyficznego jej zorganizowania już w momencie tworzenia takiego projektu. Zadać musimy sobie zatem pytanie

- Na kogo – konkretnie w przypadku telemedycyny – na jaką grupę pacjentów a w przypadku nauczania na odległość (*distance learning*) na jaką grupę lekarzy czy studentów chcemy oddziaływać w sposób zdalny (*remote action*)
- Kto będzie pełnił merytoryczny nadzór – dbał o jakość, zgodność z zasadami etyki i prawem a idąc dalej jakie instytucje powinny wydawać licencje na taką działalność i w oparciu o jakie reguły (*medical staff*)
- Ile ośrodków będzie brało udział i jaki będzie status poszczególnych uczestników takiego projektu i (*participation*)
- Jaka będzie używana technologia i kto będzie odpowiadał, za jej prawidłowe działanie (*technology*)
- Jaka będzie metodologia badawcza i w jaki sposób technologia komputerowa będzie wspomagała jej realizację (*research*)
- Jak będą mierzone efekty przedsięwzięcia i jak będą wpływać na dalszą realizację projektu (*feedback*)

### Przykłady projektów i badań medycznych wykorzystujących technologie sieciowe

Podając przykłady projektów telemedycznych ich autorzy starają się dokładnie ustalić wymienione cele projektu. Warto podać kilka przykładów -Projekt The Northern Manitoba (Canada) Community of Norway House<sup>4</sup> jest pilotażowym projektem, którego celem jest dostarczenie opieki medycznej i podniesienie edukacji zdrowotnej w prowincji Manitoba (Kanada) w oparciu o oddziaływanie poprzez sieć. Projekt obejmuje trzy oddalone od siebie społeczności a zakres projektu obejmuje telekonsultacje – łącznie z przesyłaniem ekspertom poprzez sieć wyników badań, edukację poprzez wideokonferencje i telekonferencje. Sieć budowana jest w technologii ATM a merytoryczny nadzór pełnią lekarze i pielęgniarki University of Manitoba Podobne cele wytyczyli sobie twórcy projektu „From Bench to Bedside and Beyond” (University of Washington Academic Medical Center)<sup>5</sup>. Projekt PCASSO<sup>6</sup> (University of California, San Diego) ogniskuje się na znalezieniu bezpiecznych – to znaczy odpornych na przechwycenie danych i włamania – a zarazem prostych w obsłudze systemów informatycznych służących do komunikacji lekarz-pacjent, a więc możliwych do

wykorzystania bezpośrednio w telemedycynie. Na tym tle ważnym przykładem jest nasza, polska praca POL-WEB-AMI<sup>7</sup> – zaplanowana i przeprowadzona staraniem Kliniki Kardiologii w Łodzi i Komisji Informatyki Polskiego Towarzystwa Kardiologicznego ogłoszona na XXII Kongresie European Society of Cardiology w Amsterdampie, która przy pomocy formularza umieszczonego na stronie WWW Polskiego Towarzystwa Kardiologicznego (<http://www.ptkardio.pl>) gromadziła dane na temat pacjentów ze świeżym zawałem mięśnia sercowego. Badania te są przykładem wykorzystania Internetu do przeprowadzenia badań naukowych i wskazują na możliwość wykorzystania Internetu do badań naukowych, co jest również częścią telemedycyny oraz mogą być wstępem do stworzenia pełnoprofilowego projektu telemedycznego w dziedzinie kardiologii wykorzystującej istniejącą infrastrukturę sieciową. Linki do stron internetowych prezentujących inne tego typu projekty i inicjatywy są przedstawione w dołączonym do referatu spisie adresów URL.

### Problemy dystansu związane z telemedycyną

Diagnozowanie i leczenie wymaga zastosowania odpowiednich technologii jak również rozpatrzenia, jakie przypadki – czyli jakie schorzenia i jakie grupy chorych nadają się do tego typu terapii. Problem wyboru odpowiedniej grupy chorób i schorzeń został przedstawiony na przykładzie problemów związanych z pulmonologią i intensywną terapią przez M.Ch. Boyars'a<sup>8</sup> z Dep. of Internal Medicine University of Texas Medical Branch at Galveston. Do schorzeń, które nadają się do telemedycyny zaliczono:

- 
- Przewlekłą obturacyjną chorobę płucną
  - Astmę oskrzelową w stadium wydolności oddechowej
  - Diagnostykę cieni w płucach i śródpiersiu
  - Choroby śródmiąższowe płuc
  - Zmiany opłucnowe
  - Obturacyjny bezdech senny

---

Do schorzeń natomiast, które nie nadają się do diagnozowania i leczenia metodą na odległość zaliczono:

- 
- Stan astmatyczny
  - Krwioplucie
  - Ostrą kwasicę oddechową
  - Ostrą odmę opłucnową

- Ostrą zatorowość płucną
- Niewydolność serca o niestabilnym przebiegu
- Pacjenta z towarzyszącymi zaburzeniami psychicznymi i znaczną dusznością

---

Autorzy tej jednej z najbardziej znanej książkowej publikacji<sup>9</sup> poświęconej telemedycynie nie przedstawili podobnego podziału w dziedzinie innych chorób, niemniej patrząc na ten podział widać intencje autorów, którzy takiego podziału dokonali. Do chorób nadających się do diagnozowania i leczenia na odległość zaliczono bowiem wszelkie choroby przebiegające stabilnie lub w stabilnym stadium, gdzie raczej nie przewiduje się szybkiego pogorszenia stanu czy nieoczekiwanych powikłań. Również warunkiem zaliczenia tych chorób do podobnego stadium jest możliwość dobrego i pełnego kontaktu z chorym. Ciężkie i zaawansowane stany kliniczne oraz te, które stanowią bezpośrednie zagrożenie życia nie nadają się *ex definitione* do diagnozowania i leczenia na odległość. Wydaje się, że przed podjęciem działań telemedycznych w kardiologii byłoby cenne stworzenie takiego podziału odnośnie chorób serca – po to aby projekt telemedyczny był spójny – warunek taki podał także cytowany przeze mnie F. Lau<sup>3</sup> (warunek odpowiedzi na pytanie na kogo – konkretnie w przypadku telemedycyny – na jaką grupę pacjentów a w przypadku nauczania na odległość - *distance learning* na jaką grupę lekarzy czy studentów chcemy oddziaływać w sposób zdalny - *remote action* )

### Internet w edukacji – jedna z alternatyw czy „złoty standard”

O ile szerokie zastosowanie Internetu w diagnozowaniu i leczeniu na odległość budzi liczne wątpliwości, to w przypadku edukacji – takich wątpliwości nie ma. Patrząc na przyszłość edukacji na odległość zastanawiające jest, czy i w jakim zakresie nauczanie na odległość będzie zastępować klasyczne metody edukacji<sup>10</sup>. Aktualnie na świecie zorganizowane (a więc takie, które uwzględnia nadawanie certyfikatów zawodowych lekarzom) metody nauczania przez Internet są już dość znacznie zaawansowane. Zorganizowany przez Royal College of Physicians and Surgeons of Canada<sup>11</sup> system szkolenia ciągłego (Continous Medical Education) i certyfikacji z tym związany pozwala na komunikowanie się z uczestników programu z centralą w Ottawie wyłącznie za pomocą Internetu. Każdy uczestnik może otrzymać specjalne oprogramowanie dla komputerów PC lub MAC i poprzez nie odnotowywać ilość godzin przeznaczonych na różne formy szkolenia. Oprogramowanie to również zestawia cząstkowe i finalne raporty wyników nauki i przesyła je do centrum w Ottawie. Przykład ten pokazuje, że jakkolwiek w przypadku kształceniu studentów – jednak należy się spodziewać konieczności przeprowadzania nauczania klasycznymi metodami – z żywym kontaktem z wykładowcą i pacjentem podczas ćwiczeń, tak w przypadku szkolenia podyplomowego lekarzy – nauczanie na odległość ma szansę stać się w niedalekiej przyszłości „złotym standardem”. Daje to bardzo dużą wygodę i szkolącym się lekarzom, którzy mogą to robić na miejscu – co jest ważne w przypadku lekarzy czynnie pracujących a także wykładowców nadzorujących proces szkolenia podyplomowego i ciągłego, ponieważ mogą oni wygodnie nadzorować proces kształcenia bez potrzeby „ruszania się z miejsca”, co daje możliwość edukacji typu „tutor”. Kontakt pomiędzy wykładowcą i kształcącym się lekarzem może być nawiązany o każdej porze a nie tylko w okresie stażu. Oczywiście ten typ kształcenia nie zastąpi staży specjalizacyjnych – ale w wybranych przypadkach może je skrócić. Moje roczne doświadczenia w uczestniczeniu (dzięki pomocy dr Adama Poradziśa z Edmonton w Kanadzie) we wspomnianym

kanadyjskim programie Continuous Medical Education oraz kontynuacja uczestnictwa w tym roku pokazują, że można poddać się przynajmniej części procesowi edukacji „nie ruszając się z miejsca” nadzorowanemu przez oddalony ośrodek zagraniczny. Wirtualne kongresy medyczne na świecie stały się już praktyką. Przykładem jest zorganizowany w Argentynie przez Federación Argentina de Cardiología Pierwszy Wirtualny Kongres Kardiologiczny<sup>12</sup>. Podobne konferencje i kongresy odbywają się także w innych specjalnościach medycznych. W obu Amerykach Internet staje się spoiwem dla wymiany doświadczeń w zakresie medycyny pomiędzy krajami języka angielskiego i hiszpańskiego co prawdopodobnie korzystnie wpłynie na niwelację różnic oraz barier – także w medycynie – jaką dotąd stanowiła rzeka Rio Grande zaś w Europie, w dziedzinie kardiologii jest ważnym medium łączącym należące do European Society of Cardiology<sup>13</sup> towarzystwa krajów członkowskich – w tym także Polskie Towarzystwo Kardiologiczne i likwiduje podobne bariery pomiędzy Europą Zachodnią i Środkową.

## Technologia

Na pierwszy rzut oka technologia komputerowa adaptowana na potrzeby komputerów nie różni się od technologii komputerowej używanej w innych dziedzinach medycyny. Specjalnym jednak warunkiem dla możliwości zaadaptowania Internetu – czyli sieci publicznej – dla wymiany informacji medycznej, w szczególności telemedycyny jest konieczność zapewnienia odpowiednich warunków bezpieczeństwa. Przez pierwsze lata rozwoju Internetu – w zasadzie aż do 1999 roku – uważano, że używania Internetu dla przesyłania informacji poufnych, dotyczących konkretnego pacjenta z uwagi na brak zapewnienia odpowiedniego bezpieczeństwa sieci jest niemożliwe. W ostatnim czasie jednak zaakceptowanie Internetu dla przesyłania poufnych danych bankowych<sup>14</sup> i finansowych, w szczególności udostępnienie przez banki możliwości zdalnego wydawania dyspozycji swoim klientom zmieniła także pogląd na możliwość stosowania Internetu w medycynie, ponieważ poziom wymaganych zabezpieczeń niezbędnych dla bezpieczeństwa transakcji bankowych jest zbliżony do wymaganego poziomu bezpieczeństwa niezbędnego dla przekazywania medycznych danych poufnych. Warto zwrócić jednak uwagę na dwa przeciwstawne problemy. Z jednej z uwagi na pojawienie się od roku 1996 plagi włamań sieciowych generalnie zwiększono i wyposażono w aplikacje zabezpieczające systemy operacyjne serwerów sieciowych<sup>15</sup>, to z drugiej strony sieciowi włamywacze próbują stosować coraz bardziej wyszukane i nieoczekiwane metody włamań wykorzystując różne błędy (*bugs*) systemów i oprogramowania. Ostatnim przykładem może być wykorzystanie błędu w jądrze (*kernel*) systemu Linux w wersji 2.2.x który pozwalał na włamanie<sup>16</sup> poprzez oprogramowanie serwera pocztowego *sendmail 8.9.x* wykorzystując prawa rozszerzone użytkowników (*setuid*).

Systemy zabezpieczeń generalnie składają się z czterech elementów

- Systemów oddzielania sieci – „ścian ogniowych” – *firewalls*<sup>17</sup>
- Systemów kontroli dostępu do serwerów – *tcpwrapper*<sup>18</sup>, *tcpserver*<sup>19</sup>
- Systemów szyfrowania przesyłanych danych na poziomie systemu (*ssh*<sup>20</sup>, *SSL*<sup>21</sup>) i użytkownika (*PGP*<sup>22</sup>, *SSL*)
- Systemów identyfikacji i uwierzytelniania użytkownika wykorzystującego aplikacje kontrolujące dostęp do serwerów i szyfrowanie (*identd-rfc931*<sup>23</sup>, *PGP*, *S/Key*<sup>25</sup>)

Zabezpieczenia systemów serwera UNIX mogą być wzbogacone o zabezpieczenia stacji roboczych końcowych opartych o system Windows95/98/2000/NT – przykładem takiego oprogramowania może być *IdeNT*<sup>24</sup>. W zakresie bezpiecznej komunikacji stacja robocza – serwer możliwe jest wykorzystani także generatora haseł jednokrotnych *s/key*<sup>25</sup>, który eliminuje niebezpieczeństwo przechwycenia hasła.

## Zasada działania systemów zabezpieczających

Poszczególne sposoby ataku jakie mogą zostać dokonane na serwer są skrupulatnie dokumentowane i opisywane<sup>15</sup>. Pozwala to na tworzenie oprogramowania. Oprócz czterech – wspomnianych wyżej – istotną rolę pełnią łatki systemowe (*patche*) tworzone celem przeciwdziałania błędom wykorzystywanym przez sieciowym włamywaczy. Dla systemu Solaris informacje na temat łatek dla tego systemu podane są między innymi na stronach Sunworld<sup>26</sup>. (admistrowany we współpracy z Uniwersyteckim Centrum Komputeryzacji główny serwer Polskiego Towarzystwa Kardiologicznego, którym jest komputer Sun'a posiada zainstalowane w systemie ponad 30 łatek mających na celu poprawiać wykryte błędy systemu). Drugim z omawianych systemów jest ściana ogniowa (*firewall*). Rozwiązanie to jest wykorzystywane wówczas, kiedy istnieje potrzeba ścisłego rozdzielania sieci lokalnej od sieci rozległej – czyli Internetu. Wykorzystać tu można zarówno oferowane przez wiele firm oprogramowanie komercyjne jak również rozwiązanie oparte o komputer Linuxowy ze specjalnie w tym celu kompilowanym jądrem Linuxa. Szczegóły tego rozwiązania omówione zostały wyczerpująco w podanym uprzednio źródle<sup>17</sup>. Najpowszechniej stosowanym zabezpieczeniem jest jednak kontrola dostępu do serwera. Przyjęło się, że instalacja oprogramowania pozwalająca na ograniczaniu dostępu do określonych usług internetowych dla wybranych tylko użytkowników stała się nieomal standardem. Nowoczesne systemy UNIXowe posiadają już na ogół zaimplementowane wspomniane oprogramowanie *tcpwrapper* autorstwa Wietse Venema. Na administratora z reguły więc spada przydzielanie dostępu dla określonych usług z zewnątrz dla konkretnych użytkowników. Innym, konkurencyjnym oprogramowaniem służącym do kontroli dostępu jest *tcpserver* autorstwa Dan'a Bersnstein'a. Aplikacja ta posiada ponadto cechy pozwalające – w ograniczonym co prawda zakresie – na wykorzystywaniu tego programu w funkcji „ściany ogniowej” – czyli *firewall'a*, ponieważ pozwala na blokowanie usług i portów. Wreszcie warto dodać, że część aplikacji serwera posiada własne mechanizmy kontroli dostępu – dla przykładu serwer WWW *Apache*<sup>27</sup> posiada własne mechanizmy pozwalające na ograniczanie dostępu dla użytkowników i określonych usług świadczonych za jego pośrednictwem. Kolejnym ważnym elementem jest korzystanie z połączeń szyfrowanych. Aczkolwiek oprogramowanie pozwalające na bezpieczne – w odróżnieniu od „niebezpiecznego” telnetu – łączenie się z Internetem (*SSH*<sup>28</sup>) stosowane jest od dawna, prawdziwym przełomem stało się *SSL*<sup>29</sup> używane, które pozwala na tworzenie bezpiecznych, szyfrowanych połączeń z serwerem WWW. Właśnie ta technika używana jest w tworzeniu bezpiecznych internetowych transakcji bankowych. Równoległe z systemami zabezpieczeń niezbędne jest stworzenie systemów uwierzytelniania. Zdalny system „musi wiedzieć” czy użytkownik przedstawiający się konkretnym identyfikatorem sieciowym jest na pewno tą osobą – czy ktoś inny nie próbuje się podszyć. W proces uwierzytelniania zaangażowane są wszystkie systemy zabezpieczające<sup>15</sup>, niemniej systemem, który jako pierwszy pozwolił na stworzenie elektronicznej sygnatury – „wirtualnego podpisu” jest *Pretty Good Privacy (PGP)*<sup>30</sup>. Mechanizm działania tego programu polega na tworzeniu przez każdego użytkownika dwóch kluczy. Jednego publicznego (*public key*), który jest znany publicznie oraz sekretnego (*secret key*) znanego tylko właścicielowi. Tekst sygnowany jest przez nadawcę własnym (nadawcy) kluczem sekretnym i publicznym kluczem adresata, który nadawca musi oczywiście otrzymać z wiarygodnego źródła. Odbiorca weryfikuje

elektroniczny podpis za pomocą klucza publicznego nadawcy, który musi od niego uzyskać i własnego klucza sekretne. Warto więc zauważyć, że w systemie tym używa się zawsze pary kluczy (nadawcy i adresata) i że klucze sekretne nigdy nie muszą ulegać wymianie – czyli przesyłaniu. System zabezpieczania stacji roboczych Windows95/98/2000/NT – *IdeNT* niweluje „dziurę” i niedogodność tego systemu, która pozwala na pełny dostęp każdemu użytkownikowi tego komputera i do wszystkich jego zasobów. Wykorzystanie tego systemu zabezpiecza więc w taki sposób, że końcowi, różni użytkownicy jednego komputera mają dostęp tylko do przydzielonego przez administratora zasobów. Na kontrolę dostępu do zasobów plików serwera w układzie lokalnym pozwala również oprogramowanie serwera plików *Samba*<sup>31</sup>.

Zabezpieczenia współczesnych systemów sieciowych pozwalają na bezpieczne – w określonym zakresie – przenoszenie danych medycznych za pośrednictwem Internetu. Skuteczność wykorzystania licznych, wymienionych aplikacji zależy od umiejętności i czujności administratora systemu i poziomu edukacji każdego z użytkowników. Żadne zabezpieczenie nie będzie skuteczne, jeśli końcowy użytkownik nie będzie stosował podstawowych reguł bezpieczeństwa. Reguły, jakie powinien stosować użytkownik zawarłem w 1998 roku w czterech zasadach<sup>32</sup>, które być może powinny już nawet ulec uzupełnieniu. Każdego nowego użytkownika sieci zachęcam do zapoznania się z tymi regułami. Dzięki nim ustrzec może się problemów, jakie mogą być spowodowane włamaniem się na jego konto sieciowe.

### Aspekty prawne

Problemy aspektów prawnych wykorzystania Internetu w medycynie są bardzo szerokie i nie do końca dają się całkowicie przewidzieć skutki prawne użycia tej nowej technologii – dotyczy to zarówno Internetu medycznego w Polsce jak i na świecie. W referacie chciałbym się skupić na aspektach prawnych dotyczących telemedycyny. Dla zaakceptowania telemedycyny jako pełnoprawnego sposobu praktykowania ważną rzeczą jest stworzenie jednolitych standardów. Przykładem takich prac jest aktywność grupy IMIA 16<sup>33</sup>, która od grudnia 1999 roku podjęła takie działania. Standardy urządzeń i aparatury w USA są objęte nadzorem FDA i urządzenia takie muszą posiadać certyfikaty<sup>34</sup>. Zasady etyczne są również przedmiotem wielu sporów, niemniej istnieje przewaga poglądów, że właściwe wykorzystanie Internetu w diagnozowaniu na odległość, leczeniu i promocji zdrowia może korzystnie podnieść zdrowotność społeczeństw<sup>35</sup>.

W zakresie szczegółowych uwarunkowań prawnych – w różnych krajach przyjmowane są odmienne zasady. W Stanach Zjednoczonych stosowanie telemedycyny w szerokim zakresie jest dozwolone w 16 stanach (dane z 1999 roku)<sup>36</sup> – w USA zależne jest to od prawa stanowego, niemniej w większości stanów amerykańskich telemedycyna jest dozwolona także w formie odrębnych projektów nadzorowanych przez placówki akademickie. Kongres Stanów Zjednoczonych zatwierdził także w 1997 roku<sup>37</sup> możliwość uzyskiwanie refundacji świadczeń telemedycznych (*reimbursement*) prawem federalnym, co pozwala na uzyskiwaniu zwrotu opłaty za świadczenie wykonane w innym stanie. Entuzjaści telemedycyny twierdzą, że ten przepis jest w praktyce działaniem na rzecz propagowania telemedycyny przez instytucje rządowe. Jeszcze wcześniej w 1996 roku telemedycynę zaakceptowały amerykańskie instytucje *managed care* - między innymi Medicare i Medicaid<sup>38</sup>. 4 maja 2000 roku senator Jeffords przedstawił w prowizorium budżetowym propozycję zwiększenia nakładów na „Telehealth Improvement and Modernization Act of

2000”. Podobne zasady prawne stosowane są także w Kanadzie, w której programy telemedyczne są intensywnie rozwijane w wielu prowincjach.

W Europie nastawienie do telemedycyny jest konserwatywne. W większości krajów europejskich nie ma żadnych uregulowań prawnych dotyczących telemedycyny. Wówczas najczęściej stosowane są przepisy wykluczające możliwość leczenia i diagnozowania na odległość bez „fizycznego” kontaktu z pacjentem. Takie zasady obowiązują we Francji jak również w Polsce. Aktualnie obowiązujący w Polsce artykuł 9 Kodeksu Etyki Lekarskiej<sup>39</sup> stanowi, że „Lekarz może podejmować leczenie jedynie po uprzednim zbadaniu pacjenta. Wyjątki stanowią nagłe sytuacje, gdy doraźna pomoc lekarska w formie porad może być udzielona wyłącznie na odległość”. Istnieje jednakże możliwość konsultacji przypadków między lekarzami – i taka forma uprawiania medycyny – jako sieciowe konsylium, w którym ostateczną odpowiedzialność przyjmuje na siebie lekarz bezpośrednio opiekujący się pacjentem jest możliwe. Standardy tego typu działań próbują ustalić poprzez przedstawiiony w 1997 roku na II Konferencji Internetu Medycznego w Krakowie projekt o nazwie „Inicjatywa Dorota”<sup>40</sup>. Prawne następstwa jakie mogą powstawać w przypadku odpowiedzialności lekarza za błędny wynik konsultacji będą w przyszłości największym problemem prawnym telemedycyny.

Reasumując – w Stanach Zjednoczonych i Kanadzie zarysowuje się tendencja dla nie tylko uznania telemedycyny jako pełnoprawnego sposobu praktykowania ale wręcz dla działań zmierzających do jej rozwoju. W większości europejskich krajów prawo albo nie reguluje albo nie zezwala na uprawianie takiej formy lekarskiej praktyki.

## Zakończenie

Ramy artykułu nie pozwoliły na dokładne omówienie wszelkich problemów. W końcu 2000 roku telemedycyna i Internet medyczny staje się poważnym wyzwaniem dla lekarzy i innych zawodów medycznych. Warto jednak także podkreślić, że o rozwoju telemedycyny i Internetu medycznego w ogóle będzie decydować zainteresowanie chorych tą formą kontaktu z lekarzem jak możliwości zdalnej edukacji, które już dzisiaj są ogromne. Patrząc na ilość pytań, jakie stawiają pacjenci lub rodziny pacjentów na wielu medycznych listach dyskusyjnych i grupach newsowych nietrudno dojść do wniosku, że popyt na tego typu „świadczenia” jest bardzo duży. To może także wypłynąć na zmianę statusu Internetu medycznego – w szczególności telemedycyny w Polsce.

Spis zasobów WWW dotyczących tematu znajduje się na stronie <http://www.am.torun.pl/telemedycyna.html>

---

<sup>1</sup> D. Bolter „Człowiek Turinga” – PIW Warszawa 1990

---

<sup>2</sup> S. Viegas – „Past as Prolog” in [ed.] S.F. Viegas , K. Dunn – „Telemedicine, practicing in information age” Lippincot-Raven, Philadelphia-New York 1996

<sup>3</sup> F. Lau, R.Hauward – „Building a Virtual Network in a Community Health Reaserch Training Program” J Am Med. Inform Assoc. 2000;7:361-377

<sup>4</sup> Telemedicine – The Research and Development Pilot Project Joining communities for health care and health education - The Northern Manitoba (Canada) Community of Norway House - on line [cited 03.09.2000] - <http://www.umanitoba.ca/CommSys/specpro/tmindex.html>

<sup>5</sup> „From Bench to Bedside and Beyond” - Building and Testing an Integrated Regional Medical Information Network for the Pacific Northwest - University of Washington Academic Medical Center –on line [cited 03.09.2000] - <http://www.hslib.washington.edu/b3/>

<sup>6</sup> PCASSO – „Patient Centered Acees to Secure Systems on Line” - University of University of California, San Diego – on line [cited 03.09.2000] - <http://medicine.ucsd.edu/pcasso/index.html>

<sup>7</sup> J. Drozd et al. – „A recent update on risk factors, treatment and complications od acute myocardial infarction in Poland: Polish multicentre WEB-based registry on Acute Myocardial Infarction (POL-WEB-AMI)” - Europ. Heart J ; 21-Suppl; Aug/Sept 2000: 12

<sup>8</sup> M Ch. Boyars „Pulmonology and Critical Care Medicine” – in [ed.] S.F. Viegas , K. Dunn – „Telemedicine, practicing in information age” Lippincot-Raven, Philadelphia-New York 1996

<sup>9</sup> S.F. Viegas , K. Dunn [ed.] – „Telemedicine, practicing in information age” Lippincot-Raven, Philadelphia-New York 1996

<sup>10</sup> R.Neame, B. Murphy, F. Stitt, M Rake – „Universities without walls: evolving paradigms in medical education” – BMJ 13.Nov.1999, 319: 1-4

<sup>11</sup> Royal College of Physycians and Surgeons Of Canada – „Maintance of Certification” Information Guide fot Fellows – on line [cited 17.09.2000] - [http://rcpsc.medical.org/english/public/maintofcert/mocomp\\_e.html](http://rcpsc.medical.org/english/public/maintofcert/mocomp_e.html)

<sup>12</sup> 1st Virtual Congress of Cardiology - Federación Argentina de Cardiología –on line [cited 17.09.2000] - <http://www.fac.org.ar/cvirtual/>

<sup>13</sup> European Society of Cardiology – <http://www.escario.org>

<sup>14</sup> Bezpieczeństwo systemu bankowości internetowej – Pl@net – on line [cited 17.09.2000] - <http://www.fortisbank.com.pl/services/planet/SSLPL.html>

<sup>15</sup> J. Bugajski – „Bezpieczeństwo systemu UNIX” – Magazyn „Linux & UNIX” 5(9): 15-21

---

<sup>16</sup> SENDMAIL SECURITY TEAM ADVISORY - Sendmail Workaround for Linux Capabilities Bug – on line [cited 17.09.2000] - <http://www.sendmail.org/sendmail.8.10.1.LINUX-SECURITY.txt>

<sup>17</sup> Linux Firewall and Security Site – on line [cited 17.09.2000] - <http://www.linux-firewall-tools.com/linux/>

<sup>18</sup> TCPwrapper Excerpts – on line [cited 17.09.2000] - <http://www.inx.net/~jshim/tcpwrapper.html>

<sup>19</sup> UCSPI-TCP (TCP-server) – on line [cited 17.09.2000] - <http://cr.yip.to/ucspi-tcp.html>

<sup>20</sup> SSH-Secure Shell – on line [cited 17.09.2000] - <http://www.ssh.com/about/company/index.html>

<sup>21</sup> Protokół SSL – on line [cited 17.09.2000] - <http://www.wsi.edu.pl/~galas/ssl.htm>

<sup>22</sup> PGP Security – on line [cited 17.09.2000] - <http://www.pgp.com/>

<sup>23</sup> Welcome to Identd – on line [cited 17.09.2000] - <http://info.ost.eltele.no/freeware/identd/>

<sup>24</sup> IdeNT (Optimus ATS) – on line [cited 17.09.2000] - <http://www.ident.pl/>

<sup>25</sup> S/Key – on line [cited 17.09.2000] <http://www.ece.nwu.edu/CSEL/skey/skey-brown.html>

<sup>26</sup> The Solaris Security FAQ – on line [cited 17.09.2000] - <http://www.sunworld.com/common/security-faq.html>

<sup>27</sup> Apache – on line [cited 17.09.2000] – <http://www.apache.org>

<sup>28</sup> Ssh FAQ – on line [cited 17.09.2000] - <http://www.uni-karlsruhe.de/~ig25/ssh-faq/>

<sup>29</sup> Apache-SSL – on line [cited 17.09.2000] - <http://www.apache-ssl.org/>

<sup>30</sup> Informacje o PGP – on line [cited 17.09.2000] - <http://pgp.icm.edu.pl/>

<sup>31</sup> Samba – opening window to wide world – on line [cited 17.09.2000] - <http://us1.samba.org/samba/download.html>

<sup>32</sup> Włamania do sieci – zbiór prostych reguł – on line [cited 18.09.2000] - <http://www.uni.torun.pl/~pekasz/secur.html>

<sup>33</sup> IMIA 16 – on line [cited 22.09.2000] - <http://www.ramit.be/imiawg16/>

<sup>34</sup> Telemedicine Related Activities – on line [cited 22.09.2000] - <http://www.fda.gov/cdrh/telemed.html>

---

<sup>35</sup> Health Internet Ethics – on line [cited 22.09.2000] -  
<http://www.hiethics.org/Principles/index.asp>

<sup>36</sup>State Telemedicine Legislation – on line [cited 22.09.200] -  
[http://www.arentfox.com/quickGuide/businessLines/e-health/e-health\\_telemed/e-health\\_lawsRegs/tmstateleg/state1999.html](http://www.arentfox.com/quickGuide/businessLines/e-health/e-health_telemed/e-health_lawsRegs/tmstateleg/state1999.html)

<sup>37</sup>Telemedicine & Health Care Informatics Legal Issues – on line [cited 22.09.2000] -  
<http://www.netreach.net/~wmanning/telmedov.htm>

<sup>38</sup>S R Klein, W L Manning – „Telemedicine and Law” on line [cited 22.09.2000] -  
<http://www.netreach.net/~wmanning/telmedar.htm>

<sup>39</sup> Kodeks Etyki Lekarskiej –on line [cited 22.09.2000] -  
<http://www.nil.org.pl/prawo/bbaa.htm>

<sup>40</sup> Inicjatywa „Dorota” – on line [cited 22.09.2000] –  
<http://www.uni.torun.pl/~pekasz/dorota.html>