Safety and security on the Internet

Challenges and advances in Member States

Based on the findings of the second global survey on eHealth

Global Observatory for eHealth series - Volume 4

World Health Organization

WHO Library Cataloguing-in-Publication Data

Safety and security on the Internet: challenges and advances in Member States: based on the findings of the second global survey on eHealth.(Global Observatory for eHealth Series, v. 4)

1.Internet - utilization. 2.Computer security. 3.Computers. 4.Access to information. 5.Medical informatics. I.WHO Global Observatory for eHealth.

ISBN 978 92 4 156439 7 (NLM classification: W 26.5)

Printed in Switzerland.

Safety and security on the Internet

Challenges and advances in Member States

Based on the findings of the second global survey on eHealth

Global Observatory for eHealth series - Volume 4

2011

World Health Organization

Acknowledgments

This report would not have been possible without the input of the Observatory's extensive network of eHealth experts and the support of numerous colleagues at the World Health Organization headquarters, regional, and country offices. Sincere thanks are due to over 800 eHealth experts in 114 countries worldwide who assisted with the design, implementation, and completion of the second global survey.

Special thanks to the authors of this work Kevin Clauson and Karen Vieira, and the international expert reviewers including: Erin Holmes, Lana Ivanitskaya, Pauline Sweetman, and Michael Veronin. The publication was internally reviewed by Najeeb Al Shorbaji and Joan Dzenowagis.

We are grateful for the financial support and collaboration of the Rockefeller Foundation.

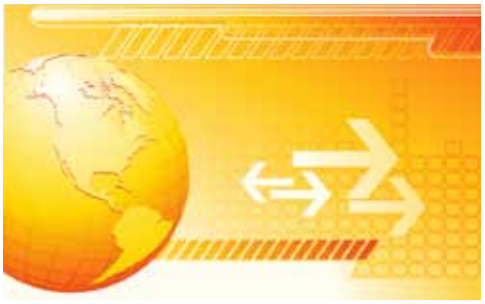
Our appreciation goes to Jillian Reichenbach Ott for the design and layout, and Kai Lashley for editing.

The global survey and this report were prepared and managed by the WHO Global Observatory for eHealth: Misha Kay, Jonathan Santos, and Marina Takane.

Photo credits: ©Thinkstock, page 55 - ©WHO

Table of contents

Executive summary


The Internet has moved beyond an educational and research tool that served as a social network for a few elite scientists and has been transformed into a commerce and health care juggernaut accessible to much of the planet. However, the accessibility of this resource has not been unencumbered by complication and challenge.

Internet pharmacies demonstrated potential early on as a hub within a wider set of eHealth services, but has since been mired in doubts regarding transparency, fraud, product quality, and even its viability as an ethical business model. Even now, over a decade after the first Internet pharmacies, questions of legality and policy plague this venture. It is telling that among the total responding countries to this survey *(114)*, most Member States (66%) remain uncommitted on this issue, unable to decide whether Internet pharmacies should be prohibited or allowed. And while those among World Bank categorized upper-middle and high-income countries are most likely to have addressed this issue, overall there is still more prohibition (19%) than permission (7%) of Internet pharmacy operations.

Internet security, in the form of spam, is another persistent challenge. Crime follows opportunity and the first spam actually appeared in 1978, shortly after the Internet itself had been opened to the public. Spam itself poses a risk for individuals and institutions, but its greater threat may be as a vehicle for fraud, viruses, malware, and spyware. Spam has also been used to target vulnerable populations suffering from poorly treated or socially stigmatized medical conditions. Overall, technology filters remain the most common tool employed to combat spam. E-mail filters are used by Member States at both the local organizational/business (75%) and Internet service provider (67%) levels. A combination of legislative (33%) and educational (30%) responses also remain staples in attempting to reduce spam by responding countries, although these are most likely to occur in high-income countries, at rates of 55% and 52% respectively.

The Internet presents a world of opportunities for children and adolescents, but it also threatens communities with inappropriate content, cyberbullying among peers, and online predators – whether that is via connection to the Internet at home, in a cybercafé, or by Smartphone. To date, of those Member States that have some type of government-sponsored initiative on Internet safety (47%), the vast majority also specifically direct efforts at protecting children (93%). However, there is much room for growth as less than a quarter (22%) of responding countries legally require the use of "safety tools" in locations children are known to frequent (e.g. libraries and schools) in more developed countries.

For one of the most daunting challenges associated with the Internet and health care, assurance of online health information quality, the most common approach (55%) was voluntary compliance by content providers and web site owners. All the other measures to assure quality information online (e.g. education programmes, government intervention, official seals of approval) were used by less than one third of Member States.

To address unresolved issues with Internet pharmacies, Member States should consider regulation to protect public health and, when feasible, create an alternative, but secure distribution channel for delivery of essential medicines. Member States with existing legislation identified in this volume can be a valuable point of contact and data for other countries wishing to move forward in this arena. Organizations and institutions including the International Pharmaceutical Federation (FIP) also merit consulting based on their work in these areas.

Distribution and receipt of spam should be targeted based on the findings in this volume including continued international support of non-profit-making efforts (e.g. Spamhaus) as well as consolidation of fragmented educational efforts. Stronger definitions, penalties, and enforcement should also be established for spam when possible. Additionally, findings suggest reallocating existing resources – currently diluted in multiple ways – to educational programmes for citizens to help avoid the more serious threats that can accompany spam (e.g. viruses).

While security issues such as spam create problems costing billions in any currency, the most polarizing public health threat presented by the Internet may be to the safety of children and adolescents. For those Member States contemplating introduction and prioritization, or strengthening legislation for online child safety, libraries, schools, and community centres granting Internet access to children and teenagers are natural foci for directing legislative and intervention efforts.

Moving into the next decade, Internet safety and literacy present enormous challenges, as basic and health literacy are still hurdles to be overcome in most Member States. Developing countries and those with low initiative rates should consider emphasizing this area; lower rates of Internet penetration have insulated youth in developing countries to date, but with the explosion of Internet accessibility via mobile devices the face of Internet access has changed. Formalizing or codifying educational practices to integrate digital literacy and awareness of online safety issues into requisite schooling and adult education would be beneficial.

The capacity for digital literacy is intertwined with accessibility to and quality of online health information. It is anticipated that the importance of these issues will become even more prominent in the coming years. Solutions for managing the quality of health information proposed included use of medically focused search engines as well as official seals of approval (e.g. HONcode). While those tools have utility, stakeholders are seeking a more holistic approach being developed and implemented globally: stricter guidelines and regulations on health content, and more abiding codes of ethics and content provider accountability. One approach that is taking these factors into consideration is that of the proposed dot health top-level domain (TLD). A dot health TLD could serve as an organizational indicator for quality health information sources on the Internet; hence it could then act as a global resource to address many of the related eHealth issues raised here.

The results of this survey indicate a need for action and progress across the eHealth spectrum. However, case studies illustrating successes with Internet pharmacies along with citizen- and institution-initiated methods of addressing online health information quality are provided in the text of the report; these could be considered examples of a foundation on which to build upon. Similarly, World Health Organization (WHO) conclusions regarding approaches to navigate obstacles detailed in the report as well as measures to build on existing initiatives are included in the discussion.

1 Introduction


The Internet, which began as a government-funded initiative, has spread throughout the world at a remarkable rate during the 1990s and 2000s. This transition of the Internet from a curiosity among a few academics to permeating nearly all facets of personal and professional life has been described as revolutionary by technology experts and media alike *(1)*. While just 3 million people had access to the Internet in 1990 (73% of which lived in the United States of America and 15% in western Europe; *2*), there are now nearly 2 billion people connected to the Internet worldwide (Table 1; *3)*.

Table 1. Global Internet access

Region	Internet users (millions)	Distribution (%)
Asia	825.1	42.0
Europe	475.1	24.2
North America	266.2	13.5
Latin America / Caribbean	204.7	10.4
Africa	110.9	5.6
Middle East	63.2	3.2
Oceania / Australia	21.3	1.1

Source: *(3)*.

The scope of the Internet has changed drastically during this period as well. In its infancy, the Internet was limited to research, education and government uses; commercial use was barred until the early 1990s unless it directly served research or education goals. In its current incarnation, the Internet has developed vast commercial potential. Worldwide e-commerce sales are predicted to reach US$ 963 billion by 2013, averaging growth of 19.4% a year *(4)*.

While the evolution of the Internet away from being a tightly controlled, research-based medium has produced great potential for mass communication, commerce and information sharing, this growth comes at a price. Misinformation on the Internet is rife. Phishing[1] scams using e-mail to steal information and identities carry a tremendous cost (e.g. £1.7 billion annually in the United Kingdom of Great Britain and Northern Ireland alone) *(5)*. Some Internet pharmacies sell potentially addictive substances without a prescription, as well as dangerous counterfeit medications. Children and teenagers are groomed and lured by predators into abusive situations.

Because of the lack of systematic research into the use of information and communication technologies (ICT) for health, the World Health Organization's Global Observatory for eHealth (GOe) conducted a survey of Member State's eHealth practices in 2005. This was followed by a more detailed survey in 2009 (the methodology of which is explained in Appendix 1). This report focuses on Internet pharmacies, Internet security, online safety of children and adolescents, and digital literacy and online health information quality. It begins by providing an overview of these four topics, as well as an evaluation of the available literature. The results of the corresponding sections of the second global eHealth survey are then analysed and discussed, highlighting key findings. These results are given a deeper context through a series of case studies, before the remaining unanswered questions and future directions for Internet pharmacies, online health information, and cross-border regulation are discussed.

1.1. Internet pharmacies

Pharmacies as commercial enterprises began to appear in Europe during the Middle Ages. Pharmacy's modern era has witnessed its development largely in western European countries with the aid of strong, centralized, mandatory government controls and occurred as a discrete system separate from medical practice *(6)*. In countries such as the United Kingdom and the United States, the line between pharmacy and medical practice was much less distinct.

For centuries, the brick-and-mortar approach to selling pharmaceuticals served as the template around the world. However, in the late 1870s, pharmacies began selling prescription medications via mail order in the United States. More than 120 years later, this mail-order tradition would underpin the formation of the first Internet-based pharmacy, Soma.com, in January 1999. A few months later, the first Internet pharmacy launched in the United Kingdom *(7)*. By the end of 1999, a staggering 400 web sites were selling medications. And by early 2004, this number was estimated at more than 1000 *(8)*. Shortly following the launch of these first Internet pharmacies, the World Health Organization (WHO) highlighted the possible risks to individuals and the public health if medical products were sold via online means in a manner that

1 Phishing is the use of e-mail messages that falsely claim to be from an established, legitimate business or organization but are designed to steal your identity.

could bypass legislative measures that had been introduced to assure consumer safety *(9)*. Currently it is unknown how many pharmacies are doing business over the Internet, but estimates of the industry range from US$ 50 to 75 billion *(10; 11)*.

Globally, Member States' national pharmacy organizations are connected by the International Pharmaceutical Federation (FIP[2]) *(12)*. The FIP and its member associations have developed a dialogue with WHO, evidenced in efforts such as the WHO/FIP Joint Declaration on the Role of the Pharmacist in the Fight Against the HIV-AIDS Pandemic, Good Pharmacy Practice guidelines, and involvement in the International Medical Products Anti-Counterfeiting Taskforce (IMPACT) coalition.

In 2005, a cross-sectional study was performed that examined 275 English-language web sites located using the search engines Google and AltaVista with the keywords "prescription drugs" *(13)*. Based on their investigation, the authors grouped Internet pharmacies selling prescription medications into four distinct categories (Table 2).

Table 2. Models of Internet pharmacies

Pharmacy category	Operational approach
Legitimate	Provide medications as extension of established brick-and-mortar pharmacy, contingent upon patient possession of a valid medical prescription.
Subscription	Advertise online access to pharmacies selling prescription-only drugs without a prescription in return for a subscription fee paid online with a credit card.
Lifestyle	Supply 'lifestyle drugs' (e.g. erectile dysfunction, obesity, or male pattern baldness) directly to the patient after being issued a prescription through an 'online consultation'.
No-prescription	Offer mail-order delivery of drugs such as opioids, benzodiazepines and methylphenidate without a prescription in return for online credit card payment.

Source: *(13)*.

These categories of Internet pharmacies speak to the fact that when compared with traditional pharmacies, buying prescription medications online is truly a matter of *caveat emptor.*

2 http://www.fip.org/?page=menu_about.

1.2 Internet security

With the growth of global e-commerce, an ever-increasing number of people are becoming more comfortable with making monetary transactions online. This has naturally led to the expansion of online criminal activity, or cybercrime. Cybercrime began as a job perpetrated by those with functional inside knowledge of businesses but has transformed into an anonymous attack often backed by organized crime. There are a number of different means for cybercriminals to perpetuate their agendas, including spam, malware and phishing scams. Selected examples are described hereafter.

Spam

The term 'spam' describes unsolicited electronic messages sent in bulk *(14)*. Spam is most frequently seen as e-mail but is increasingly being employed via short message service (SMS) or text message, computer instant message (IM), and by telephone. Spam e-mails often direct the recipient to an external web site, but it can as serve as a vehicle for malware dissemination or phishing scams (see following sections). In this manner, spam is also increasingly used as a tool of the aforementioned no-prescription or 'rogue' pharmacies.

Spam is very common. MessageLabs Intelligence recently reported a global ratio of spam in e-mail traffic of 75.8%, which corresponds to one in every 1.32 e-mails received *(15)*. As spam levels increased by 2.9 percentage points over the previous month, the Russian Federation became the most spammed country in the world, with a spam rate of 82% (Table 3).

Table 3. Spam rates by country

Country	Spam rate (%)
Russian Federation	82.2
Hungary	81.6
Saudi Arabia	81.0
Luxembourg	80.1
China	79.8
The Netherlands	77.5
United States	76.4
South Africa	75.9
Germany	75.5
United Kingdom	75.4
China, Hong Kong SAR	75.2
Denmark	75.1
Brazil	74.8
Singapore	74.0
Australia	73.9
Japan	72.3

Source: *(15)*.

Spam messages are an inefficient, but low-risk means for perpetuating cybercrime. A study of spamming conducted in 2008 calculated that spammers only receive one response for every 12.5 million e-mails they send *(16)*. Despite this low response rate, spammers are still able to generate a profit, albeit not the millions of US dollars assumed in some circles. This profit may be due, in part, to identity theft and a more targeted use of spam in which certain consumer groups (e.g. those suffering from poorly managed medical diseases or conditions with a social element like obesity) are more likely to receive, open, and purchase items from spam e-mails *(17)*.

Pharmaceutical spam, as a subset of spam, is very common. In fact, Internet security experts estimate that over 65% of all spam is "Pharmaceutical spam" *(18)*. The most common brands featured in pharmaceutical spam is the "Canadian Pharmacy"; however, other similar web sites such as the "United Pharmacy," or the "Indian Pharmacy" are appearing more frequently *(18)*.

One of the most coordinated attempts to combat spam to date is the Spamhaus Project. Spamhaus is an international non-profit-making organization based in Geneva, Switzerland and London, United Kingdom and maintains numerous spam blocking databases as well as publishing the Register of Known Spam Operations (ROKSO).[3] Spamhaus also works with various cybercrimes units and law enforcement including Scotland Yard Computer Crime Unit (United Kingdom), Independent Authority of Posts and Telecommunications (Netherlands), Australia Communication and Media Authority, and the National Cyber-Forensics & Training Alliance (United States). Notably, Spamhaus has received a number of accolades in support of their efforts by both governmental agencies (e.g. Federal Bureau of Investigation, FBI, in the United States), and media (e.g. Virus Bulletin Award for the greatest contribution to combating spam in the past 10 years).

3 www.spamhaus.org/.

Viruses and malware

Malware is the term for the "broad range of software" with "malicious or fraudulent intent" *(19)*. Examples of malware include computer viruses, dishonest adware, spyware, scareware,[4] Trojan horses, and worms. In a recent report, MessageLabs Intelligence calculated that one in every 290.1 e-mails worldwide contained some form of malware *(20)*. The highest levels of malware were detected in South Africa, with one in every 81.8 e-mails containing malware; additional country information can be found in Table 4.

Table 4. Malware rates by country

Country	Malware ratio (per e-mail)
South Africa	1 in 81.8
United Kingdom	1 in 139.0
Canada	1 in 328.8
Australia	1 in 365.8
Germany	1 in 393.1
Denmark	1 in 451.1
China, Hong Kong SAR	1 in 455.3
China	1 in 457.0
United States	1 in 713.6
Singapore	1 in 828.9
The Netherlands	1 in 910.4
Japan	1 in 1331

Source: *(20)*.

Perhaps most notably, portable document format (PDF) file attachments are now the attack vector of choice for targeted attacks, with their usage increasing 12.4% between 2009 and 2010 *(20)*. Cybercriminals are taking advantage of the fact that PDFs are one of the most common ways to share electronic documents and the majority of people consider PDFs to be a trusted file type. However, it is exceptionally easy to conceal malicious programs in PDF files.

These malicious programs could be spyware, which monitors the user while he/she is browsing the Internet in order to display advertisements or redirect marketing revenues to the spyware's creator. Spyware can also be used to steal private data like passwords, medical insurance information, or credit card and bank account numbers, resulting in theft and fraud. In 2010 more than 100 cybercriminals and money mules were arrested for stealing US$ 70 million from bank accounts using the crimeware toolkit named 'Zeus' *(21)*. Similarly, complete medical identity theft is increasing at alarming rates *(22)* and spyware and phishing can accelerate that process, especially as more patient data is digitally housed in open-system electronic health records and personal health records. This development prompted the Office of the National Coordinator (ONC) for Health Information Technology in the United States to release a report in 2009 that included a provision for the role of health information technology in helping combat medical identity theft *(23)*.

4 Scareware is deception software that is used to frighten people into purchasing and installing it.

Internet users in developing countries are particularly susceptible to viruses and other malware because licences for operating systems (OS) and antivirus software are simply unaffordable. Vulnerability may be further exacerbated due to a culture of piracy and a general lack of network security. Based on the Organisation for Economic Co-Operation and Development (OECD) Task Force on Spam findings, the combination of a basic Windows OS and antivirus program can cost the equivalent of a month's salary in developing economies *(24)*. Consequently, a high percentage of computer owners purchase cheaper (and more often than not, pirated) versions of software and operating systems that not only leaves their machines vulnerable because they are nearly impossible to update, but also because they are, themselves, another likely source of viruses.

Phishing scams

Phishing scams involve e-mail messages that falsely claim to be from an established, legitimate business or organization but are designed to steal your identity. These e-mails either ask the recipient to send their private information, such as passwords, bank account numbers, medical insurance registry numbers, and credit card details, via e-mail or direct the recipient to a web site where they are duped into providing these data. Just like a fisherman, the cybercriminals throw out their e-mails like bait, knowing that while most will ignore their message, some will be tricked into biting.

Rogue Internet pharmacies are often used as an online front for phishing scams. The web site provides a convincing 'storefront' that purports to sell a range of lifestyle drugs; however, after placing an order the cybercriminals take the buyer's money and credit card details without ever intending to fill the order.

Phishing has progressed to the point that 1 in every 216.7 e-mails could be linked to a phishing scam *(20)*. South Africa was the most targeted country with phishing levels calculated at one in 32.5 e-mails (Table 5).

Table 5. Phishing rates by country

Country	Phishing ratio (per e-mail)
South Africa	1 in 32.5
United Kingdom	1 in 96.3
Canada	1 in 167.9
China, Hong Kong SAR	1 in 477.1
United States	1 in 536.9
Australia	1 in 545.2
China	1 in 780.5
The Netherlands	1 in 817.4
Germany	1 in 853.4
Singapore	1 in 1117
Denmark	1 in 1288
Japan	1 in 4466

Source: *(20)*.

As with all e-mail-mediated cybercrime, the most effective means of protection is awareness and caution, as the recipient is the last line of defence.

1.3 Online safety of children and adolescents

Adults are increasingly spending their discretionary time on the Internet, and children and adolescents "spend more time with media than they do in any other activity except for sleeping" *(25)*. However, because of the easy and often private access to children that the Internet offers, it has provided a new medium through which child exploitation, child maltreatment, and sexual and emotional abuse can propagate *(26)*. Broadly speaking, the Internet gives child predators instant access to a large group of potential victims, as well as the opportunity to create their own 'communities' to exchange ideas and reinforce their prurient desires.

Unsupervised access to children and teens

When it comes to finding and luring potential victims, the Internet provides numerous opportunities and advantages for predators. Chat rooms, role playing games (e.g. World of Warcraft), virtual worlds (e.g. Second Life), and social networking sites (e.g. Facebook), facilitate predators' agendas by allowing participants to remain anonymous or create false identities. By disguising their true identity and motives, predators are able to build long-term online relationships with their targeted victims prior to any attempt to promote physical contact.

More recently, varying forms of harassment have become a more prominent issue for children and teens. Examples include students in New Zealand who were recipients of bullying by text and were significantly more likely to feel unsafe at school *(27)*, the link between online and offline stalking of teens in Canada *(28)*, and cyberbullying[5] beginning in middle school *(30)*.

1.4 Digital literacy and online health information quality

Prior to the 21st century, literacy was simply defined as a person's ability to read and write; today, with the advance of modern technology and the advent of the Internet, the concept of literacy has taken on a broader meaning *(31)*. In this new era, literacy encompasses a person's ability to effectively perform tasks in a digital medium, understand and use information gathered from a variety of digital sources, and evaluate the new knowledge gleaned from digital environments *(32)*. The ability to critically evaluate information retrieved online is an integral part of the concept of digital literacy. Going forward, the related concept of eHealth literacy will also be of growing importance as individuals work to achieve competency in and reconcile computer literacy, health information literacy *(33)*, and media literacy *(34)*.

5 "The harassment of one party by another, by means of the Internet or any electronic device" *(29)*.

While the Internet provides practically unlimited potential for acquiring new knowledge, rash, unconsidered acceptance of its content can mislead. Therefore, one cannot be considered digitally literate until he/she has the ability to judge the reliability of online information (32; 34). Unfortunately, critical evaluation of online information is generally lacking in society. A pair of studies conducted five years apart by the Open University in Israel detected that the "information and literature reproduction" subset of digital literacy skills actually suffered decline over time demonstrating potentially flawed assumptions about increasing abilities of digital natives and others *(35)*. Similarly, a study of university students (n=1914) in the United States found that a quarter of all students were unable to use similar cues to detect multiple signs of danger associated with rogue Internet pharmacies *(36)*. This lack of critical thinking and analysis is particularly worrying in the context of health information found on the Internet.

Accuracy and reliability of online health information

Searching for health information online is among the most commonly performed Internet activities; recent estimates suggest approximately 8 out of every 10 adults who have online access do so in the United States *(37, 38)*, European countries *(39)*, as well as India, China, Russia, Brazil, and Mexico *(40)*. However, according to a survey conducted by the Pew Research Center, only 15% of online health information seekers said they "always" checked the source and the publication date of the information they found online *(41)*. This means that nearly 115 million Americans are gathering health information online without evaluating its quality. Not all of the blame for diminished quality control mechanisms can be put on patients, however. A study conducted under the direction of the U.S. Department of Health and Human Services calculated that only 4% of the most frequently visited health web sites published the source of their content and just 2% revealed how the content was updated *(42)*.

These practices are worrying because patients use the information they find online to make health-related decisions. In a 2010 survey by Fox and Purcell *(43)*, 53% of American respondents stated that their last Internet search impacted their personal health care in some way or the way they cared for someone else. Further, one third of e-Patients reported that what they found online specifically affected their decision whether or not to see a doctor. A study conducted at an outpatient clinic in India similarly found that respondents reported that information found on the Internet prompted them to ask their physicians questions (62%) and some to even seek a second opinion (28%) *(44)*.

Separately, it has been reported that one in every two people searching for health information online do so to self-diagnose, with the highest rates of this practice occurring in Russia, the United States, the United Kingdom, and Australia *(40, 45)*. However, many other patients use online health information to determine treatment options.

Case study 1. Foundation in Switzerland helps citizens determine trustworthiness of online health information

As members of the public increasingly gravitate to the Internet to seek guidance or find answers to their questions about health, disease, and treatment options, the quality of the information they locate online becomes paramount. To this end, the Health On the Net Foundation (HON) aims to "help unify and standardize the quality of medical and health information" that can be found online *(46)*. In 1995, HON was born out of a meeting of experts at a conference in Geneva, Switzerland and is a nongovernmental organization (NGO). The following year, HON launched operations to implement its Code of Conduct (HONcode).

The HONcode was created to benefit the public, health-care professionals, and web publishers. The presence of the HONcode logo signifies to patients and providers that the site adheres to certain principles and has undergone HON's certification process. The eight principles governing the HONcode are: authority; complementarity; confidentiality; attribution; justifiability; transparency; financial disclosure; and advertising.

The actual certification process is voluntary and conducted by a HON review committee. Those sites satisfying the eight principles are given the HONcode seal, which links back to a certificate on HON's web site detailing the performance. From that point on, monitoring of the site is periodic and begins one year after initial certification.

Courtesy of the Health On the Net Foundation

Since its initial formation, HONcode has been used by over 100 countries and covers 10 million web pages *(47)*. HON has also entered into partnerships with government agencies such as the French National Authority for Health (Haute Autorité de Santé, HAS), which resulted in improvements in web sites in France *(48)*.

> *In the beginning, HON's strategy and vision in improving the quality of medical and health information on the web was not well-known. In 2004, the European Commission and the European Union recognized Health On the Net Foundation's activities and services supporting the quality of health information at a multilingual level with an award, the Europe Award for eHealth. This distinguished award has given legitimacy to HON and visibility to its actions …*
>
> *Thanks to the introduction of the EU quality criteria developed in 2002, to which HON contributed, the HONcode has been recognised and become the first organization implementing the quality standards set by the EU (49).*
>
> **—Celia Boyer, Executive Director, Health On the Net Foundation**

New resources have been formulated by the Foundation such as the HONcode Toolbar, which acts as a plug-in for Internet browsers to check the web site that is being visited. If the site status is compliant with the HONcode, the Toolbar displays the seal in colour. Looking ahead, the Foundation also developed eight principles for their nascent 'HONcode Web 2.0'. Web 2.0 or social media are descriptors of the second iteration of the web and are characterized by a bidirectional, dynamic web featuring user-generated content. Web 2.0 principles include information on sites regarding moderator status, privacy policy, documentation of health claims, and advertising policies.

6 http://www.hon.ch/HONcode/Pro/Visitor/visitor.html.

Online Health Information in developing countries

It has been suggested that citizens in emerging economies like Brazil, China, India, Mexico, and Russia may have a greater reliance on health information they find online than people in developed nations because of the higher costs associated with seeing a medical professional face to face *(40, 45)*. Despite this possible demand, people in developing countries face two important disadvantages to accessing health information: much of the health content online is based in the United States and written in English; and health information in developing nations is often inadequate and unreliable.

With the exception of www.who.int, the remaining 20 most popular global health sites are based in the United States – including the U.S. National Institutes of Health, WebMD, PubMed, Medicinenet.com, Natural Health Information Articles and Health Newsletter (mercola.com), Medline Plus, Drugs.com, Medscape, and the United States Patent and Trademark Office's AIDS Patents Database *(40, 45)* – the highest utilizers of these health portals, after Americans, come from India, the United Kingdom, Australia, and China respectively. According to a study published in the Journal of the American Medical Association, all English-language health web sites required a reading ability at high school level or better *(50)*. This indicates that these sites are only useful resources for people with a relatively strong grasp of the English language.

Further, an investigation of health-related web sites in Sri Lanka found that only 64% were controlled by a Sri Lankan or a Sri Lankan organization *(51)*. Overall, 87% of the health-related web sites comprised fewer than 100 pages and only 8% contained health education for the general public as their main content. The authors concluded that the number of web sites available to Sri Lankans had not increased despite significant increases in Internet usage over the previous few years.

Another example comes from Thailand, where the reliability of available online health information has been called into question: a study investigating the credibility of 255 health-related web sites found that 99% of these sites have legal and/or ethical issues, while only 9% provide a disclaimer *(52)*.


http://www.

2 Review of the literature



A comprehensive review of the literature was conducted for each of the four main areas covered in this report in order to gain a better understanding of both the risks and benefits found online in the eHealth arena.

2.1 Internet pharmacies

For consumers, there are many perceived benefits of purchasing prescription pharmaceuticals online, including lower prices, greater convenience, and avoidance of embarrassment *(8)*. However, there are also real health risks associated with Internet pharmacies, especially when purchasing from sites that do not require a valid prescription for prescription-only medications *(53)*. Because of these potential threats to safety, researchers have started to forecast and evaluate the safety, reliability, and accessibility of Internet pharmacies, as well as the impact on consumers and the industry of the prescription medications sold via these portals *(54)*.

Methodology

Medline, EMBASE, Cochrane Database of Systematic Reviews, and EBSCO databases, as well as Google Scholar, were searched for the periods January 1999 to March 2011 using search terms including 'Internet pharmacy', 'online pharmacy', 'Internet pharmacy safety', 'safety online medic*',[7] 'safety Internet medic*', 'online pharmacy safety', 'online counterfeit medic*', 'Internet counterfeit medic*', and 'online medic* access'.

7 Asterisk is a character used in wildcard searching.

The literature search also included a limited search of references retrieved from included articles but did not extend to searching Internet web sites, grey literature, conference abstracts, or contacting authors for unpublished data. Clinical studies, feasibility studies, survey studies, meta-analyses, and review articles published in English and those obtainable in English translation were considered for inclusion in this review. Studies discussing policy and/or legal implications for herbal supplements, natural health products or 'legal highs' were not included for review. Lists of articles were deduplicated.

Safety of medications purchased online: is there cause for concern?

Incidents highlighting the dangers of purchasing prescription medications online are widely reported in the media of developed countries. Despite concerns about those dangers, consumers are still purchasing them in countries such as Hungary *(55)*, Italy *(56)*, Germany *(57)*, and the United States *(36)*.

However, do data exist to show there are significant risks posed to consumers by Internet pharmacy sites? And if so, is this evidence sufficient and compelling enough to warrant the development of a more stringent legal framework for Internet pharmacies worldwide? The discussion that follows seeks to answer these questions.

Availability of prescription-only drugs and lack of clinical oversight

A number of studies have shown that nearly every major category of prescription drug is available online without a prescription *(58–65)*. In 2009, French researchers investigated the online availability of treatments for psoriasis *(62)*. They discovered that it was a facile process for consumers without significant Internet expertise to find Internet pharmacies selling the majority of available treatments without requiring a prescription; even the newest and most expensive products (e.g. biological agents) were readily available.

Even more worrisome, other groups of researchers have found it surprisingly easy to purchase the class of medications called opioids over the Internet without a prescription *(65)*. Opioids are used medically as painkillers, but their use can also lead to dependence and serious side-effects such as respiratory depression. In 2006, Forman and colleagues *(60)* conducted 47 Internet searches for a range of opioids. Searches using terms such as "no prescription codeine" and "Vicodin" yielded more than 300 web sites offering to sell opioids without a prescription.

Perhaps one of the easiest drugs to find online without a prescription is the drug sildenafil. While sildenafil is used for treating pulmonary arterial hypertension (WHO Group I) (Revatio®), it is much better known for its use to treat erectile dysfunction (Viagra®). In one of the earliest studies looking into the sale of Viagra® online, researchers conducted a systematic search of the Internet to identify all sites selling Viagra® directly to consumers between 14 April and 28 April 1999. Of 4400 potentially eligible sites returned by the search engines, 86 offered to send Viagra directly to the buyer without needing to see a doctor. Of these 86 sites, 55% required the customer to complete an online medical questionnaire, 5% offered but did not require a questionnaire, and 40% did not offer any type of evaluation *(58)*.

The online sale of sildenafil has not changed much in a decade. A more recent study conducted in 2010 found that 34% of Internet pharmacy sites offered to sell Viagra® to consumers in the United Kingdom without any form of medical consultation *(61)*. The researchers were unable to determine whether the medical questionnaires offered by 59% of sites were required to be completed prior to purchase.

Medical questionnaires

The validity and reliability of medical questionnaires hosted on Internet pharmacies sites has been called into question. Orizio and colleagues *(66)* conducted a content analysis of online pharmacy medical questionnaires to examine their completeness. While nearly all questionnaires (97%) asked if the customer had any drug allergies, other types of allergies were only queried by 70%, which was the same percentage that asked women if they were pregnant or breastfeeding. Even more telling was the fact that only 19% asked the customer if the purchase was based on a medical diagnosis provided by a health-care professional. According to the authors, these results suggest that medical questionnaires provided by online pharmacies exist more as a marketing ploy to convey a sense of security and assurance than to accurately assess health status and actual need for the medication *(66)*.

To test whether Internet pharmacies actually use the information provided on health questionnaires to control the sale of potentially dangerous medications, Memmel and colleagues *(63)* posed alternately as a "healthy 25-year-old woman", a "35-year-old woman who was obese and a heavy tobacco user" and a "35-year-old smoker on an antihypertensive medication", and attempted to purchase combination oral contraceptives or contraceptive patches without a prescription. Despite entering known risk factors for estrogen use on the questionnaires provided by two of the three targeted sites, the researchers were able to purchase, and later receive, the desired contraceptives. The investigators also noted that there was no medical follow-up to these sales except for offers of additional products *(63)*.

The unfettered availability of prescription medications online poses a significant danger to patients as it may increase the risk of side-effects and adverse reactions by not accounting for potential contraindications or drug-drug interactions or by delaying treatment *(8, 58, 67)*. The ease with which individuals are able to purchase controlled substances without a valid prescription also suggests there is ample opportunity for prescription drug abuse *(59)*.

Bate and Hess *(59)* reported that even when ordering from Internet pharmacies requiring prescriptions, the process was still under-scrutinized. The study's lead author was able to use the same prescriptions more than five times because many Internet pharmacies allow customers to fax their prescriptions and do not contact the doctor who wrote the prescription. None of the Internet pharmacies (n=55) included in this study queried why the lead author had a prescription from a doctor in Indiana when he lived in Washington, DC.

Despite the relative ease of acquiring medications like opioids, Inciardi and colleagues *(68)* used five national data sets from the United States (three of which related to the abuse of prescription stimulants and opioid analgesics) to estimate who is using non-prescribed medications purchased online. According to the authors, the results suggest that the Internet is "a relatively minor source for illicit purchases of prescription medications by the end-users of these drugs" *(68)*.

Internet pharmacy locations

Internet pharmacies have not always been straightforward about revealing where they are located. In 1999, Bloom and Iannacone *(69)* found that only five Internet pharmacies in a sample of 46 (11%) provided information concerning their geographic location beyond what information was offered online. This situation has improved but remains unresolved. Recent studies in 2009 and 2010 found that less than half of Internet pharmacy web sites disclose their location, 43% and 48% respectively *(70, 61)*.

In 2010, researchers purchased five popular drugs from various Internet pharmacies *(59)*. Three of these online pharmacies claimed to be based in Canada or the United States and posted prices on their sites in dollars; however for any purchase made, they charged in Chinese or Indian currency. Even more convoluted was the online pharmacy that described itself as an "off-shore company based in Cyprus," listed a contact address in British Columbia, received the initial money transfer for the medication purchased in Panama, shipped the order from Shanghai (according to the postmark), and labelled their tablets with the name of the brand name pharmaceutical company that sells it and "USA" *(59)*.

Deceit about location raises concerns about an Internet pharmacy's validity, its source of medications and their quality. Similarly, WHO has found that that medicines obtained from illegal Internet sites that obscure their physical address are counterfeit in more than 50% of cases *(71)*.

Counterfeit and substandard medications

Counterfeit drugs may be contaminated, contain improper ingredients, incorrect ratios of the proper ingredients, contain no active ingredients, all of which can be very dangerous for people trying to manage or treat serious health conditions such as heart disease or diabetes. The European Alliance for Access to Safe Medicines (EAASM) stated in their report, The counterfeiting superhighway, that 62% of medications purchased online are fake or substandard (e.g. expired or improperly stored during delivery) *(72)*.

Three years earlier the Office of Compliance in the U.S. Food and Drug Administration's Center for Drug Evaluation and Research commissioned a study to evaluate the quality of five drug products purchased online from foreign sources compared to products purchased from a local supplier *(73)*. Of the 20 samples received and tested, two failed United States Pharmacopeia (USP) monographs for quality attributes (dissolution and purity), which calls into question the bioavailability and safety of these products. Additional tests discovered that more than half of the samples (55%) had different formulations compared to the United States product, which is a serious quality issue.

Veronin and Nguyen *(67)* investigated 19 generic medication tablets and capsules they purchased from international Internet pharmacies and compared them to the United States innovator product. Five samples failed to meet USP standards for dissolution, and two failed for content uniformity. All 19 samples had issues with hardness, weight, and other physical characteristics. According to the investigators, this variability has implications for the safety and effectiveness of the online products.

While developing countries are obvious targets for counterfeit medications, due to both the high cost of legitimate drugs as well as the lack of regulatory controls and enforcement *(74)*, quality control studies have been conducted predominantly in North America and Europe. A notable exception is a report by WHO stating counterfeit medications found in developed countries are generally expensive hormones, anti-cancer medications, or "lifestyle drugs" while those in developing countries are commonly used to treat conditions like malaria, tuberculosis, and HIV/AIDS *(71)*.

Packaging and labelling

A drug's packaging and labelling is an important safety feature. After purchasing a drug, the label affixed to the prescription container may be the only source of instructions a patient has on how it should be taken. The container is also the only mechanism used to maintain a product's identity, strength, quality and purity. Child-resistant packaging also protects young children from accidental overdose or poisoning.

Despite its importance to consumers, packaging and labelling is often absent or deficient when pharmaceuticals are purchased over the Internet. Westenberger and colleagues *(73)* found that packaging was a significant problem for practically all of the samples they purchased online during their study. Many of the drugs had no or minimal information on their labels regarding the proper usage of the product, and some were written in foreign languages.

More recently, Veronin *(75)* investigated the packaging of 41 drug products obtained from online pharmacies from 12 different countries. Of these samples, seven were dispensed in paper envelopes with an affixed label that was missing important information, such as directions for use, while 28 products did not have labels at all. According to the authors, these substandard distribution processes present a challenge to patient comprehension and health literacy and may affect the patient's adherence to their drug treatment regimen.

Summary

Based on this literature review, the risks of purchasing prescription pharmaceuticals from Internet pharmacies generally outweigh the potential benefits for consumers. It must be noted the research contained in this review primarily focuses on North America and Europe; conclusions drawn from these data, therefore, must be limited to describing the situation in these areas. No research on this topic was identified from developed or developing countries elsewhere in the world. A possible reason for this, however, may only reflect a time-lag of the medium: as some medications targeted by Internet pharmacies (e.g. sildenafil) are being increasingly used in parts of Latin America (e.g. Brazil, Colombia, Ecuador, Venezuela) as well as Africa and the Middle East (e.g. Egypt, Morocco, Nigeria, Pakistan) making them susceptible to the same model *(76, 77)*. In these areas, where the social stigma for a condition like erectile dysfunction is even more pronounced, Internet availability of drugs like sildenafil without involving a prescriber may further exacerbate public health concerns (i.e. erectile dysfunction has a strong association with coronary heart disease, which may go untreated if patient is self-medicating) *(78)*.

While data are not globally representative, there is sufficient evidence to back calls for stricter regulation of Internet pharmacies. As Mahe and colleagues *(62)* have delineated, multiple initiatives have been undertaken by international bodies: guidance by the World Health Organization, the U.S. FDA, and its European counterparts; creation of anti-counterfeit laboratories (i.e. 2008 inauguration of the Sanofi-Aventis Central Anti-Counterfeit Laboratory in France); creation of organizations to fight counterfeit medicines, notably those purchased on the Internet, such as EAASM, founded in 2007, and the International Medical Products Anti-Counterfeiting Taskforce (IMPACT); and the intensification of international police enquiries.

While scientific research into the effectiveness of these types of regulatory initiatives is scarce, Boyer and Wines *(79)* found that increased regulation of, and law enforcement operations directed at, Internet pharmacies may lead to significant decreases in the availability of prescription medications like opioid analgesics offered for sale.

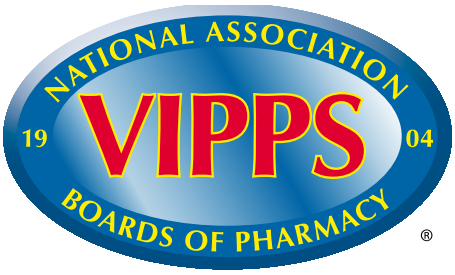
At least one study has shown that consumers can reduce the risks associated with buying prescription medications online by relying on the lists of recommended sites compiled by credentialing agencies like the National Association of Boards of Pharmacy (NABP) *(59)*. The NABP, with the support of the FDA, maintains a list of web sites likely to sell potentially harmful or illegal drugs. A programme with similar aims was launched by the Royal Pharmaceutical Society of Great Britain (RPSGP) with its green cross logo. In 2010, Bate and Hess *(59)* tested the quality of five popular drugs purchased from web sites listed in the various categories provided by the NABP. Of the drugs analysed, none from the "approved", "legally compliant", or "not recommended" web sites (O out of 86) failed, whereas 8.6% (3 out of 35) failed from "highly not recommended" and unidentifiable web sites. Nonetheless, just creating awareness of these tools remains a challenge as consumers still predominantly use search engines to find Internet pharmacies; and even those search engines that purportedly integrate quality requirements (such as those by PharmacyChecker.com) into their processes have been found to deliver unverified pharmacy web sites *(80)*.

It can be concluded from this literature review that consumers need protection from the dangers posed by Internet pharmacies. The results from the 2009 eHealth survey presented later in this report will help determine the limits of current legislation in this area and provide a more in-depth picture of what needs to be done. Box 2 shows a model to verify the veracity of Internet pharmacies being used in Canada and the United States.

Box 2. One model of verifying Internet pharmacies: case study from North America

The NABP comprises member boards from all 50 United States and eight Canadian provinces along with New Zealand, Puerto Rico, Guam, and the Virgin Islands. Its mission is to assist its members in "developing, implementing, and enforcing uniform standards for the purpose of protecting the public health". In response to mounting public health concerns about the safety of pharmacies operating online, NABP created the Verified Internet Pharmacy Practice Sites (VIPPS) programme in 1999 *(81)*. VIPPS Canada followed thereafter as a partnership between NABP and Canada's National Association of Pharmacy Regulatory Authorities (NAPRA) *(82)*. VIPPS is also the lone consumer safety programme supported by the FDA and the Drug Enforcement Administration in the United States.

In order to obtain certification and display the VIPPS seal, Internet pharmacies must satisfy 19 criteria including assurance of patient safety, authentication of prescription orders, and demonstration of a meaningful offer to establish a pharmacist-patient consult. For legitimacy, the logo is hyperlinked on sites that display it to the programme home page. The hyperlink will not work on sites fraudulently using the logo. Of the 8034 Internet pharmacy sites NABP has reviewed, less than 4% comply with good standards of practice; 8034 were categorized as "not recommended" *(83)*. Notable among criteria unsatisfied for those "not recommended" were 6812 sites that did not require a prescription and 5089 which did not require a pre-existing relationship. While only 260 Internet pharmacy sites appeared to be potentially legitimate, this does represent a 15% increase from the previous year.



Courtesy of the National Association of Boards of Pharmacy

Maintenance of this accreditation mandates reviews every three years following the initial application. So far almost 30 pharmacy companies representing over 12 000 brick-and-mortar pharmacies have completed the verification process.

> *VIPPS empowers the public to make informed decisions about Internet pharmacy practice. It also serves as a valuable tool to help distinguish safe Internet pharmacies from Internet sites and drug outlets that are dangerous and a threat to public health (84).*
>
> —Dr Carmen Catizone, Executive Director of the National Association of Boards of Pharmacy

At least one study has indicated that consumers can reduce the risks associated with buying prescription medications online by relying on the lists of recommended sites compiled by credentialing agencies like the NABP *(59)*. In 2010, Bate and Hess *(59)* tested the quality of five popular drugs purchased from web sites listed in the various categories provided by the NABP. Of the drugs analysed, none from the "approved", "legally compliant" or "not recommended" web sites (0 out of 86) failed, whereas 8.6% (3 out of 35) failed from "highly not recommended" and unidentifiable web sites.

It is recommended that those seeking Internet pharmacy services should consider beginning with a search for a VIPPS approved site (85). NABP has created a resource to allow anyone to verify the status of an Internet pharmacy by its uniform resource locator (URL) (http://vipps.nabp.net/). Potential users of these types of sites may also reduce the chance of receiving counterfeit medications by availing themselves of Internet pharmacies that have undergone the VIPPS process *(86)*.

A programme modelled after VIPPS may represent a scalable solution to address some of the global issues facing Internet pharmacies.

8 http://www.nabp.net/about/.

2.2 Internet security

Receiving unsolicited e-mail messages that are sent in bulk without the permission of the recipient, also known as spam *(14)*, is a major problem for people using Internet communications. One case study examining the composition of e-mail found that of the subset of spam (n=1390), 39% was generated exclusively from medication and sexually targeted advertisements *(87)*.

Methodology

Medline, EMBASE, Cochrane Database of Systematic Reviews, and EBSCO databases, as well as Google Scholar, were searched for the periods January 1999 to March 2011 using search terms including 'spam health, 'spam medic*', 'spam e-mail', 'spam drug*', 'pharma* spam', 'pharma* e-mail', 'junk e-mail', and 'pharma* phishing'.

The literature search also included a limited search of references retrieved from included articles but did not extend to searching Internet web sites, grey literature, conference abstracts, or contacting authors for unpublished data. Clinical studies, feasibility studies, survey studies, meta-analyses and review articles published in English and those obtainable in English translation, were considered for inclusion in this review. Lists of articles were deduplicated.

Pharmaceutical and health-related spam, spim, and spit

Unwanted, usually commercial, messages can come in a number of forms. Internet users are probably most familiar with spam e-mails; however, with the growth of online technology, spammers have begun to enter other communications arenas. With the increased use of instant messaging (IM) and text messaging or short message service (SMS), unwanted IM or SMS sessions containing commercial information are now appearing. This is sometimes known as "spim" or "spit" (spam over Internet telephony) *(88)*, and spamming through social networking sites (e.g. Twitter) are also on the rise *(88, 89)*.

While many people find these messages annoying and intrusive, they also pose a potential threat to those who engage with them. According to the U.S. Federal Trade Commission's Division of Marketing Practices' False claims in spam report *(90)*, 66% of all e-mail spam contained false information, whether it was the sender's name, the recipient's name or information within the body of the message. This deceptiveness increased to 69% in health-related spam.

Despite its prevalence and potential risks, few original systematic studies on health-related spam have been conducted. Researchers have only just begun to investigate the effects spam and other unsolicited commercial messages have on their recipients.

Does spam affect consumer behaviour?

There are a handful of scientific studies investigating the relationship between consumer behaviour and spam e-mail. Morimoto and Chang *(91)* found that the favourability of a recipient's attitude toward spam was inversely correlated to their perception of the advertisement's intrusiveness and the amount of irritation caused. Women generally seem to dislike spam more than men due to the sexual nature of

much of its content *(92)*. Despite the negative feelings people have about spam, they do not appear to be sufficiently motivated to take much personal action against it. According to a study conducted by Grimes *(93)*, most e-mail users have not installed anti-spam filters despite the numerous filtering programs available for free or at very low cost.

While the majority of people take no action to filter spam, anywhere between 4% and 66% of people have purchased products advertised through spam e-mails *(92, 94–97)*. Age may be a factor in the widely varying range of purchases. Grimes and colleagues *(92)* found that older adults are more likely to report purchasing a product from a spam e-mail than younger ones, although being affected by a socially stigmatized condition may be a contributing factor as well.

Fogel and Shlivko *(98)* investigated 200 recipients' responses to spam e-mails advertising sexual performance products. Some of these participants had sexual performance problems while others did not. The results of the study showed that participants with sexual performance problems received (100% versus 73.5%, p=0.024), opened (66.7% versus 11.4%, p<0.001), and purchased more products (46.7% versus 5.4%, p<0.001) from spam e-mails than participants without sexual performance problems.

The authors speculated that the increased interest in spam e-mails was three-fold: 1) those affected by sexual performance problems may be so driven to enhance their sexual performance that they will consider any product or potential solution, even if it comes from a less-than-reputable source; 2) e-mail is a very private media and may be preferred to purchasing the same products from a pharmacy due to the embarrassment that often surrounds sensitive health issues like sexual performance; 3) those with sexual performance problems may not perceive spam advertisements as negative and intrusive since they are offering a product of interest *(98)*.

A similar study conducted in 2010 by those researchers focused on the behaviour of 200 young adults who received spam e-mails advertising weight-loss products *(17)*. As in their previous study, some of the participants had weight issues while some did not. Similarly, the participants with weight problems received (87.7% vs. 73.3%, p=0.02), opened (41.5% vs. 17.8%, p<0.001), and bought products (18.5% vs. 5.2%, p=0.003) from spam e-mails more often than those without weight problems.

Reliability and validity of health products purchased from spam e-mails

One study of note was conducted investigating the actual process of purchasing health-related products via spam e-mails. During November 2006, Gernburd and Jadad *(99)* received 4153 spam messages in three separate e-mail accounts opened in Canada. Of these messages, 1334 (32%) were health-related. Throughout the last week of the study, the authors received 19 health-related spam e-mails from which they purchased 13 prescription drugs and 6 natural health products. During the ordering process, four web sites stopped working after the credit card information was submitted; no further information was provided to the ostensible customer to indicate if the transaction was successful. While 13 sites did not actually process the order, all of them recorded the full set of personal information provided, arguably the more valuable commodity.

Out of the 19 orders placed by the authors, 5 prescription drugs and 4 natural health products were delivered, although the quality of these products was not examined. Surprisingly, none of the credit card information appeared to be abused. The only fraud that was detected in this study was by one site that took payment for a product that was never delivered. However, based on research conducted with Internet pharmacies (see Section 2.1), it would stand to reason the risks of purchasing medications online through spam would be congruent.

Even if the products purchased were defective or harmful, very little action could be taken against the spammers because of the short half-life of the associated links (i.e. approximately 2 weeks). According to the authors, by the time the products were delivered the spammers had become "virtual ghosts". Since the spammers could largely disappear without a trace, it precluded any real action being taken by law enforcement in the rare cases when consumers tried to report the incidents *(99)*.

Summary

Because of the lack of published studies; this literature review raises more questions than answers. For example:

- How does spam affect consumers' attitudes toward the pharmaceutical industry and online health information?
- Are products purchased through spam links safe and effective? Or are they counterfeit and substandard?
- How much of spam-linked content is valid, and which is part of a phishing scam?
- What are the incidence and effects of viruses and malware contained in health-related spam?
- What type of people open, read, and act upon spam messages and why?
- Are consumers aware of the dangers of spam? Does this knowledge (or lack thereof) affect their behaviour?

Some legislation and other anti-spamming initiatives employed by Member States have shown promise. For example, in Japan, the 38 million customers using DoCoMo, Japan's largest wireless company, received 150 million pieces of spam a day on their cell phones before the passage of anti-spam legislation and just 30 million pieces of spam a day after *(100)*. However, this legislation is largely based on observational work. Hope and greed are powerful motivators, so as more people around the world begin to access the Internet and search for solutions to health and lifestyle problems, the number of e-mails, text messages, and mobile web solutions offering promises, legitimate or otherwise, will undoubtedly increase and customize to match the demand *(99)*. Therefore, without increased research into the motivations of spammers and consumers and enhancing programmatic support, spam will be nearly impossible to eradicate.

2.3 Online safety of children and adolescents

It is normal today for children and adolescents to base their extracurricular activities around the Internet. With access to video games, chat rooms, and social networking, being 'plugged in' is one of the most popular pastimes for children. This is due, in part, to the fact that over 90% of children and adolescents in developed countries have access to the Internet *(101)*. More specifically, the Pew Internet & American Life Project found that 93% of youth (i.e. aged 12–17 years) use the Internet *(102)*. Rising or robust use of the Internet by children and adolescents has also been noted in research in many other countries ranging from Argentina to Guatemala *(103)* and Qatar *(104)* to Turkey *(105)*. Considering the level of their connectivity and a transient lack of supervision and controls in place, children and adolescents are subject to online risk and can also become easy targets for online predators.

Methodology

Medline, EMBASE, Cochrane Database of Systematic Reviews, and EBSCO databases, as well as Google Scholar, were searched for the periods January 1999 to March 2011 using search terms including 'online child* safety, 'online child* health', 'Internet child* safety', 'Internet child* access', 'child* activity Internet', 'adolescent activity Internet', 'teen* activity Internet', and, 'child* OR teen* predators'.

The literature search also included a limited search of references retrieved from included articles but did not extend to searching Internet web sites, grey literature, conference abstracts, or contacting authors for unpublished data. Clinical studies, feasibility studies, survey studies, meta-analyses and review articles published in English and those obtainable in English translation, were considered for inclusion in this review. Lists of articles were deduplicated.

Are children and adolescents at risk when online?

As use of the Internet has greatly increased over the past twenty years, so has its role in becoming a useful forum for child predators. Since children have easy and often unsupervised access to the Internet, they are increasingly targeted for exploitation, sexual and emotional abuse, and maltreatment *(30, 106)*. By being able to disguise their identity, sexual predators have a great advantage of being able to target and approach their young victims in many popular forums such as chat rooms and social media platforms (e.g. Facebook, Twitter) without them ever knowing *(107)*. The single biggest risk in social media circles may be the individual's complete "lack of control over where the information is going, how it will be posted, and who is going to be able to access it" *(108)*.

Children and adolescents online without supervision

Children and adolescents are using their online access without restriction and can be unaware they are putting themselves into compromising situations. Adolescents, in particular, are liable to adopt risky behaviour without considering consequences due to underlying neural and cognitive factors during age-related brain maturation *(109)*. A survey conducted in 2008 by The National Campaign to Prevent Teen and Unplanned Pregnancy found that 22% of teenage girls and 18% of teenage boys (aged 13–19 years), reported sending or posting nude or semi-nude pictures or videos of themselves online. Of these teens,

15% reported that they sent these sexually suggestive images of themselves to someone they only knew online, usually to be "fun or flirtatious" *(110)*. Similarly, due to the increasingly ubiquitous nature of mobile phones among all age groups, there has consequently been an increase in "sexting" among teenagers in which sexually suggestive photos and/or messages are sent via mobile phone *(111)*.

Without knowing the actual identity of perceived friends and relationships forged online, children could be unwittingly encouraging sexual predators. Online predators will attempt to leverage relationships with these vulnerable populations in order to manipulate behaviour *(112)*. However, sexually explicit photos or information shared by children and adolescents online is not limited to placing them in compromising situations with predators; it can also lead to bullying or unwanted sexual advances by their peers. A study in the United Kingdom found that more than a third of the 2000 surveyed secondary school children had been sent messages of a sexual content *(113)*. Another study generated from WHO data on behaviour in children revealed that 13.6% of children were the victim of cyberbullying *(114)*.

The link between children online and child pornography

With children and adolescents accessing the Internet unsupervised and engaging in discussions and pictures of a sexual nature, it is unfortunate, but unsurprising, that they would be highly susceptible to targeting by paedophiles and child pornographers *(115)*.

With little research being done concerning the numbers of children abused by child pornographers online *(116)*, it is difficult to get a clear picture on the severity of this risk. There is also a lack of a consensus regarding an association between predilections to commit real-life offenses and collecting child pornography that may have slowed responses to this issue *(117)*. Hence, the extent and magnitude of children and adolescents targeted by online child pornographers and sexual predators is unknown.

Summary

Based on the evaluation of this literature review concerning the online safety of children and adolescents, this age group can be characterized as at-risk when online. Although there are many benefits to children and adolescents using the Internet for learning or improving skills, there is obviously a need for regulation or restrictions on the sites they are accessing and the amount of personal information they are providing to 'friends' or 'relationships' forged online. Without cautionary guidelines for children who go online, there is an increased probability that they will experience exposure to some sort of exploitation during their usage.

With children and adolescents accessing the Internet unsupervised for lengthy periods of time every day *(118)*, further research needs to be conducted on how many children are actually aware of the dangers of sexual predators online or are aware of the consequences of sending sexually explicit photographs of themselves via the World Wide Web *(119)*.

At the least, Member States should consider fostering awareness of the risks of sending personal information and photos online through school curricula and/or meetings between parents and teachers.

2.4 Digital literacy and online health information quality

After health information started to appear online, along with the promise it offered, concerns about the quality of that information and its potential impact were expressed *(120, 121).* This, in turn, led to the development of hundreds of instruments being created to measure online health information quality *(122, 123).* Tools were created ranging from checklists like DISCERN (http://www.discern.org.uk/) to vetting systems such as the HON Foundation (See Box 1) (http://www.hon.ch) to guidelines from WHO *(123)*. Evaluations of online health information quality have since been conducted for topics such as women's health *(124)*, malaria *(125)*, medications *(126)*, and sexual health *(127)* on web sites in English, French *(128)*, Italian *(129)*, Spanish *(130)*, among others. More recently, with the rise of social media, health information is being shared via blogs, social networking sites, Twitter, and in particular Wikipedia; the quality of these sources is now being examined as well *(131–136).*

The Internet is a quick, convenient and private means for obtaining medical information, and when such information is accurate and appropriate, offers enormous potential for informed decision-making and greater participation of patients in their own care *(137)*. As a result, much emphasis has been placed on the validity, accuracy, and completeness of online health information, with a large number of studies suggesting significant deficiencies in quality for online patient-oriented information covering a variety of medical conditions *(138–143)*. These results have led to calls for improving or certifying the quality of health information online. However, ensuring there is accurate and complete health content available online is not enough; information seekers must be able to find and access it.

Methodology

Medline, EMBASE, Cochrane Database of Systematic Reviews, and EBSCO databases, as well as Google Scholar, were searched for the periods January 1999 to March 2011 using search terms including 'online OR Internet health information', 'online OR Internet health information quality', 'quality online information', 'digital literacy', 'Internet literacy', 'search engine*', 'online OR Internet health information accessibility', 'assess online OR Internet information', and 'evaluate online OR Internet information'.

The literature search also included a limited search of references retrieved from included articles but did not extend to searching Internet web sites, grey literature, conference abstracts, or contacting authors for unpublished data. Clinical studies, feasibility studies, survey studies, meta-analyses and review articles published in English and those obtainable in English translation, were considered for inclusion in this review. Lists of articles were deduplicated.

Searching for health information online: is quality content easily accessible?

A wealth of health information is currently available on the Internet, and as previous studies have shown, the quality of the information presented varies greatly. But with well over 100 000 health-related web sites *(144)*, it is impossible for information seekers to surf through them all. As a result, when confronted with a specific health-related question, nearly all Internet users (more than 95%) use a search engine (145, 146). But do search engines retrieve the highest quality health information? And more importantly, does the way people conduct searches and assess the results provide them with information they can use to make educated health-related decisions?

The role of search engines

Three categories of search engines are available to help health information seekers retrieve information from the Internet: general search engines, meta-search engines, and medical search engines. General search engines such as Google, Yahoo!, and Bing were designed to be user-friendly programs for sourcing information via the Internet. Meta-search engines were developed to perform simultaneous searches within a select group of general search engines and then collate the results *(147)*. Finally, medical search engines are much more specific, as they only catalog online medical information. Such searches generally retrieve fewer, but more relevant, results.

Despite the fact there are search engines specifically designed to retrieve information from selected web sites, general search engines are the most common starting points for health information searches *(102, 145, 146, 148, 149)*. This issue is particularly germane as new research has demonstrated up to one third of online searches for prescription drugs were the subject of search-redirect attacks; in effect the high-ranking links were re-routed to infected host pharmacy sites *(150)*.

While general search engines have vastly improved user access to online health information, the criteria used to identify and rank health-related web sites vary considerably among search engines, and the method for ranking results often is not apparent to users *(151)*. A web site's ranking within the results returned by a search engine depends on its specific algorithm but may include variables such as the number of times a web site has been accessed from the results page, the structure and content of the web site, the search terminology employed by the user, and any use of paid placements *(151)*.

A web site's ranking within search results is extremely important because sites listed on the first page are "significantly more likely to be accessed by health information seekers, with an exponential decline thereafter" *(145, 146, 152)*.

How do health information seekers search for information?

Several studies have investigated the methods different groups of Internet users employ to find answers to health-related questions online. Hansen and colleagues *(146)* examined the search strategies of 68 adolescents and noted they were generally successful in finding correct and useful information to answer a health-related question. The majority of sites the teenagers accessed (87%) came directly from a list of search engine results, of which 10% were from a search engine's list of recommended links. Eighty-three per cent of participants clicked on links that appeared within the first nine results returned by the search engine. A qualitative assessment by the authors revealed that the teenagers used a trial-and-error approach for formulating their searches, randomly scanning pages rather than systematically evaluating them and did not consider the source of the information when answering health-related questions.

Eysenbach & Köhler *(145)* observed similar techniques among adults. The general search strategy of their participants was to try a number of initial search terms and briefly examine the contents of a page before iteratively refining their search. According to the authors, few of the participants noted, and later remembered, from which web sites they had gathered information. Buhi and colleagues *(153)* asserted that users need to be educated about how search engines prioritize and display their results and be trained to systematically evaluate health web sites for reliable information. Another author cautions, however, against too much analysis, which could lead to paralysis and may be consistent with the suggestion that "more is less" *(154)*.

Quality of search engine results

As the majority of health information seekers never get past the first few pages of search engine results, determining the accuracy and reliability of the web sites listed on these pages is important for evaluating the quality of health information available to users *(152)*.

In a study evaluating online information about depression, Lissman and Boehnlein *(155)* observed that the quality of information retrieved by the search engines they utilized was very low. They also found that commercial web sites appeared much more frequently within the top 20 results returned by the search engines than not-for-profit sites. Based on the findings of two more recent studies, this may be because many of the top results are so-called sponsored links, meaning the web site owner has paid the search engine for higher placement *(156, 157)*.

After sponsored links, the next most common site to appear in the first page of health-related search results is often Wikipedia *(158)*. Wikipedia is the world's largest reference web site and is the most successful example of a 'wiki', a site collaboratively written by its users. Since it began in January 2001, more than 3.3 million articles have been generated and edited in English alone by volunteers worldwide, many of which are on medical topics *(159)*. According to a 2009 study conducted by Laurent and Vickers *(160)*, Wikipedia was listed within the first ten results in 71–85% of search engines for health-related keywords they tested. Since anyone, expert or layperson, is able to write and edit Wikipedia entries anonymously, concern has been raised over whether Wikipedia provides accurate information about health and medical topics. Two studies assessing the quality of Wikipedia content are discussed below.

The first, published by Clauson and colleagues *(134)*, investigated the scope, completeness, and accuracy of drug information on Wikipedia in comparison to a free, online, traditionally-edited database, Medscape Drug Reference. Based on the results, Wikipedia had a narrower scope, was less complete, and had more errors of omission than the Medscape Drug Reference. The study also found that the medication entries in Wikipedia improved significantly over time (p=0.024) In the second study, Heilman and colleagues *(159)* reported that Wikipedia's many medical articles contain few factual errors but that improvements need to be made in the depth and readability of individual articles. Both studies concluded that while Wikipedia may be a useful point of engagement, it should not be used as an authoritative source of health information.

Do Internet searches retrieve desired health information?

At least two studies have shown that only a small percentage of sites retrieved by online health keyword searches contain the information being sought. Rose and colleagues *(161)* used 25 commonly-used keywords to search for knee-related information online. The search generated nearly 6000 pages, of which only 395 (6.6%) contained actual knee-related information. McClung and colleagues *(141)* conducted similar searches using keywords such as "diarrhea" and "treatment" and evaluated the first 300 search engine results. Of these results, just 23% (70 sites) contained information relevant to the topic.

However, other studies have shown that patients are easily able to find the information they are searching for online, although their evaluation of the sites may be lacking. Based on the results of Eysenbach and Köhler *(145)*, Internet users successfully found the answers to health-related questions in an average of 5 minutes 42 seconds (median 4 minutes 18 seconds) per question; however, their search techniques were often deemed to be suboptimal.

In a larger Australian study, 227 undergraduate students answered a set of health-related questions before and after using a search engine to retrieve online information from PubMed, MedlinePlus, and HealthInsite *(162)*. The investigators found that searching quality health information sources improved the user's accuracy in answering health-related questions (pre-search 61.2% versus post-search 82.0%, p<.001). However, they also discovered that searching the Internet increased users' confidence in incorrect answers. This may be because a person's prior belief (anchoring bias) may impact their search for information and their confidence in the answers found *(163, 164)*.

Summary

This review suggests the web sites that users are more likely to access for health information are based on their ranking within general search engine results and usually are of lower quality than sites dedicated to health information (e.g. MedlinePlus). Further, it appears users are too rushed, unconcerned, or simply not savvy enough to evaluate the sources of information they use to answer health-related questions. As a result, researchers have recommended a number of ways to improve the overall quality of web sites accessed by health information seekers, as well as educating citizens.

One possible approach is to promote the use of medical search engines such as Healthfinder (www.healthfinder.gov) and HONsearch (www.hon.ch/HONsearch/Patients/index.html; also see Box 1) that only list information from trusted content providers as well as sites that perform similar aggregating functions of trusted resources like MedlinePlus (http://www.nlm.nih.gov/medlineplus/; also see Box 3) or other sites officially hosted by Member States and local institutions such as NHS Patient Choices (http://www.nhs.uk) and CISMeF-patient (http://www.chu-rouen.fr/cismefp/).

Three of the studies identified include those that evaluated the efficiency of medical search engines in sourcing relevant health information. All three studies found that, as with other search engines, the search specificity of medical search programs was low, with only about 10% of web sites retrieved being unique and relevant (165, 166, 147). However, the studies diverged on whether the overall quality of web sites retrieved by medical search engines was higher than general ones. Maloney and colleagues *(147)* assessed the quality of osteoarthritis information retrieved through general, medical, and meta-search engines and concluded that while the overall quality of the results was poor, the medical search engines identified higher-quality web sites. Conversely, medical search engines did not provide higher quality information about androgen deficiency in the ageing male or prostate cancer screening *(165, 166).*

A second suggestion that has been posed is to encourage more health-care providers to specifically direct their patients to high-quality online health resources. Although less than 5% of patients currently use web sites recommended by their health-care providers when searching for health information, a handful of randomized controlled trials have shown that such advice does increase the use of recommended sites *(167–169).*

The variation among search engine listings and the prevalence of sponsored or recommended sites on the first page of results suggests that patients are often being directed to health-related web sites on commercial, rather than informative, grounds. Therefore, users need to become more educated about how search engines prioritize and display their results and learn to systematically evaluate health web sites before making any decisions based on information they find online. Health-care professionals also need to accept the growing role the Internet has in patient care and take responsibility for helping patients locate comprehensive and accurate online health information.

A strategic alternative to addressing these issues is the dot health (.health) proposal. The ambitious idea of creating .health as an Internet top-level domain (TLD) was first advanced in 2000. A TLD is the highest hierarchical level of a web address and is structurally analogous to .com, .org, and .edu (ICANN, 2000). Creation of the .health TLD under the auspices of an international organization would contribute significantly to the protection of the public's health through the global adoption of quality standards for health-related information and practices on the Internet. In leveraging the .health TLD, WHO could promote consensus building and broad adoption of quality standards for health-related information on the Internet. In addition to the generation of value, a .health TLD could be used to help protect information quality as well as privacy and safety of Member States' citizens.

3 Analysis and discussion of survey results



Responses to the questions in Section 6 of the second global survey on eHealth have been categorized into the following four areas:

1. Internet pharmacies
2. Internet security
3. Online safety of children and adolescents
4. Digital literacy and online health information quality

In this section, analyses and observations relating to each of these areas will be presented and the key trends and patterns will be discussed.

Full details of the survey methods including survey instrument development, data collection and processing, response rate and survey limitations are included in Appendix 1.

3.1. Internet pharmacies

In order to ascertain the current legal status and regulation of Internet pharmacies in Member States, responding countries were asked a series of four questions and invited to elaborate on their responses. These questions covered the general regulation of Internet pharmacy operations within their country as well as the online ordering of pharmaceuticals from other countries.

Regulation of Internet pharmacy operations

Key findings

- The majority of responding countries (66%) have no legislation either allowing or prohibiting Internet pharmacy operations.
- Developed countries were more likely to have established legal policies than developing countries.
- Existing legislation prohibits Internet pharmacy operations more often than permitting it (19% versus 7%).

With the significant increase in the number of Internet pharmacies over the past decade, concern over the safety of the prescription medication dispensed online has also grown. While some online pharmacies are tightly controlled, like web-based enterprises managed by well-known corporate brands, there is also a growing number of rogue pharmacies dispensing prescription-only medications without valid prescriptions, providing counterfeit drugs of questionable quality, and failing to properly inform their customers about potential side-effects and dangerous drug interactions.

National and local governments have traditionally regulated the sale and dispensing of prescription drugs by pharmacies. However, when it comes to the online sale of these medications, regulation appears to be lagging. The majority of responding countries (66%) have no legislation either allowing or prohibiting Internet pharmacy operations (Figure 1). However, in those countries that do have regulations, the general trend appears to be for their prohibition (19% versus 7%).

As shown in Figure 2, when classified by World Bank income group, significantly more countries prohibit Internet pharmacy operations than allow them in every category except the low-income group. The same holds true when responding countries were divided into their respective WHO regions. In fact, the European, Americas, and Western Pacific Regions were the only constituencies with countries that formally allow Internet pharmacy operations (Figure 3).

Figure 1. Global legislation of Internet pharmacy operations, globally

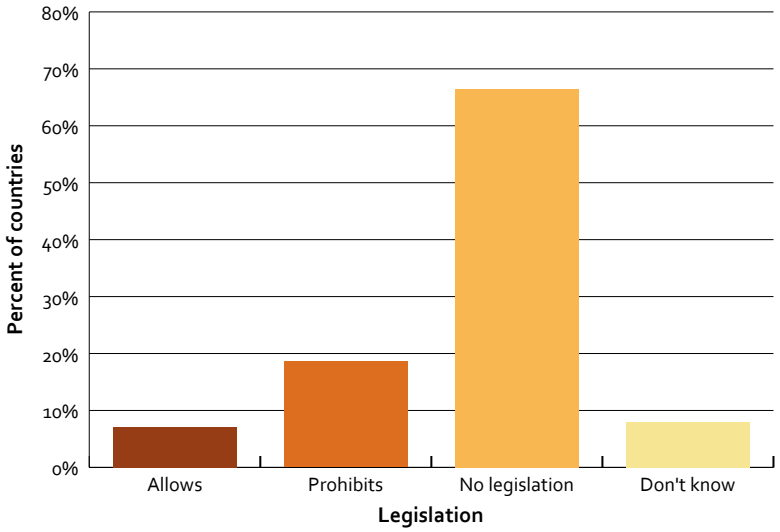


Figure 2. Legislation of Internet pharmacy operations, by World Bank income group

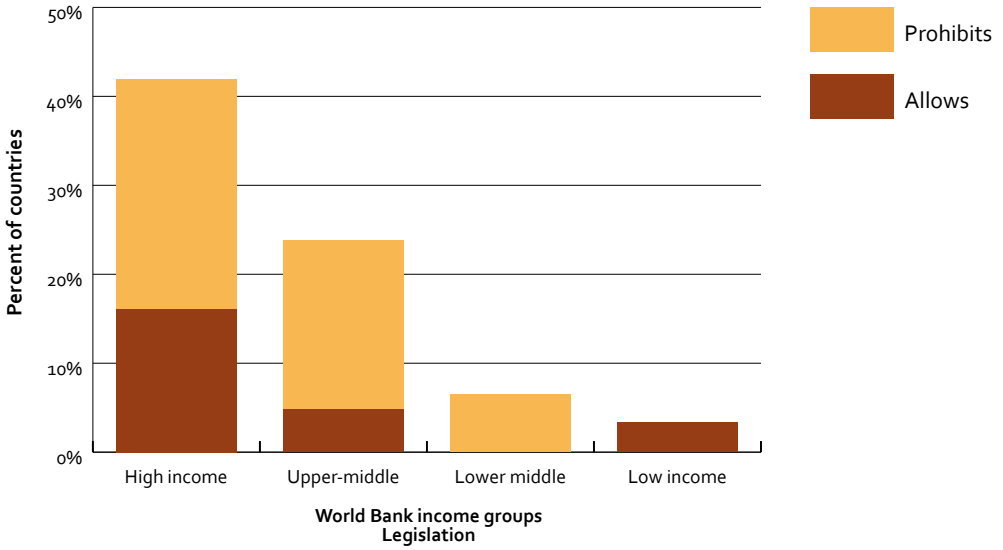
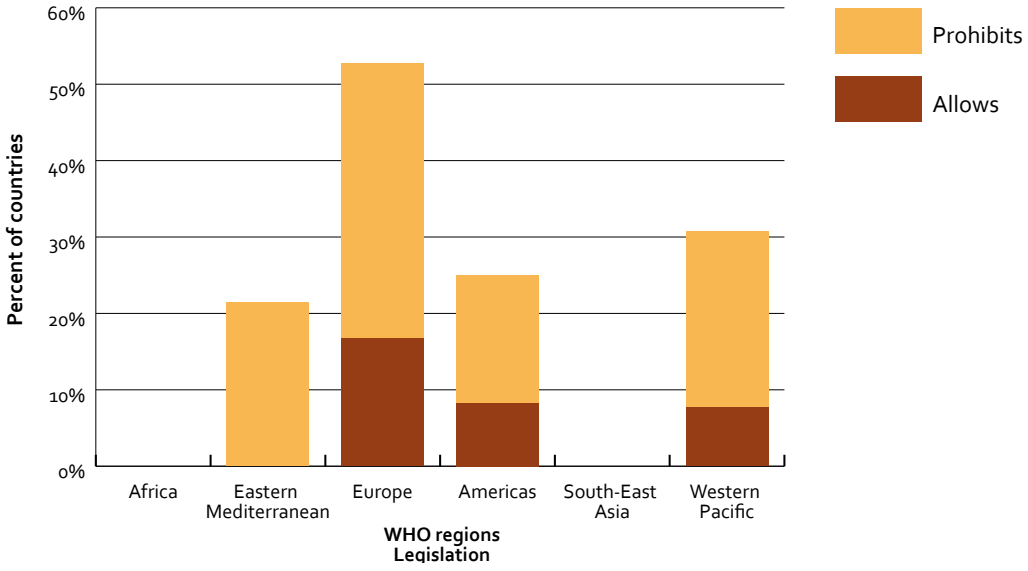


Figure 3. Legislation of Internet pharmacy operations, by WHO region



Respondents were also asked if their country regulates, accredits, or certifies Internet pharmacy sites. As with Internet pharmacy legislation, the vast majority of responding countries (86%) do not regulate, accredit, or certify Internet pharmacy sites.

Of the 7% of responding countries that do regulate, accredit, or certify Internet pharmacy sites, the vast majority are located in the European Region (Figure 4) and all are high- or upper-middle income countries (Figure 5).

Figure 4. Regulation, accreditation, and certification by WHO region

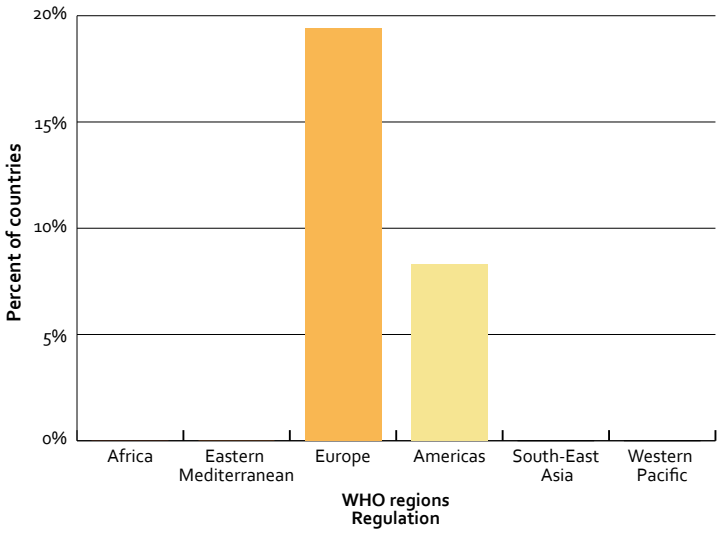
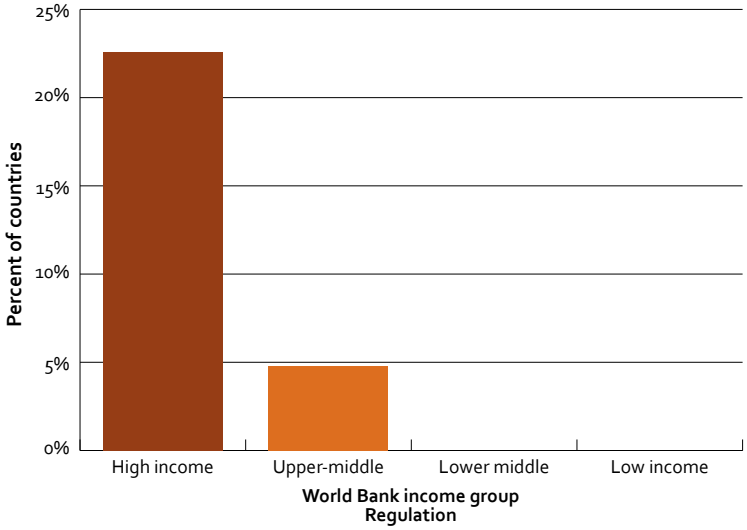


Figure 5. Regulation, accreditation, and certification by World Bank income group



Regulation of online purchase of pharmaceuticals from abroad

Key findings

- Globally, the online purchase of medications from other countries is largely unregulated, with 75% of responding countries having no legislation permitting or prohibiting the practice.
- The European Region has the largest percentage of countries with some type of legislation.
- Nearly 80% of responding countries do not have, do not know, or did not respond if there were consequences for breach of laws regulating online purchases of pharmaceuticals.

The Internet is truly a borderless medium. As such, regulating e-commerce like Internet pharmacies within the physical jurisdiction of a sovereign state is extremely difficult and such regulation becomes even more problematic when the pharmacies originate outside of a nation's jurisdiction. The difficulty of this task is echoed in the survey results, as 75% of responding countries have no legislation permitting or prohibiting the online purchase of medications from other countries.

Figure 6 shows the proportion of responding countries with policies concerning the online purchase of pharmaceuticals from abroad, categorized according to WHO region. The European Region was by far the most likely to have legislation, with nearly 53% of responding countries having some form of policy. It was the only region in which countries legally permit the online purchase of medications originating non-domestically. Notably, Norway responded that it has legislation which prohibits Internet pharmacy operations based in its own country, but allows purchase from other countries.

Figure 6. Legislation of online purchase of pharmaceuticals from abroad, by WHO region

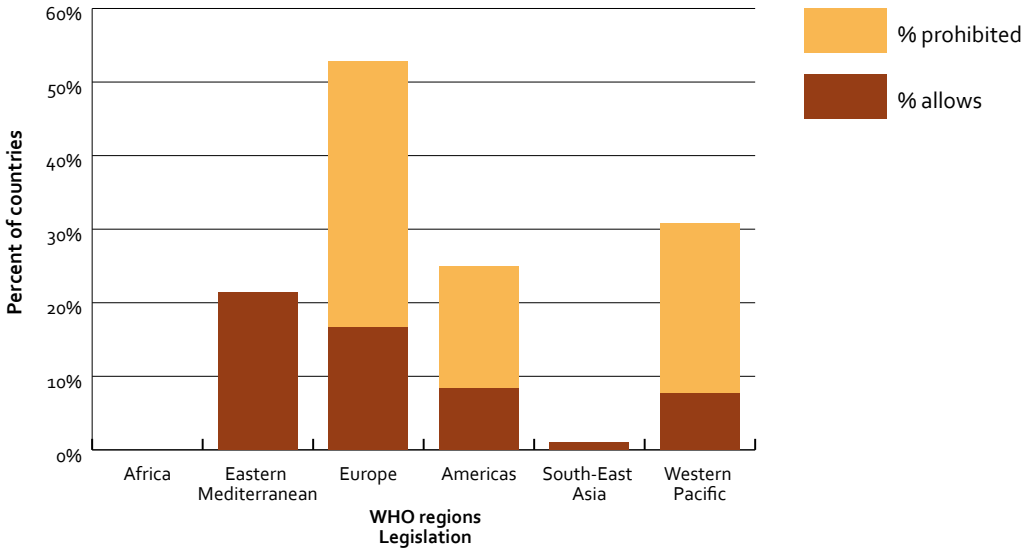
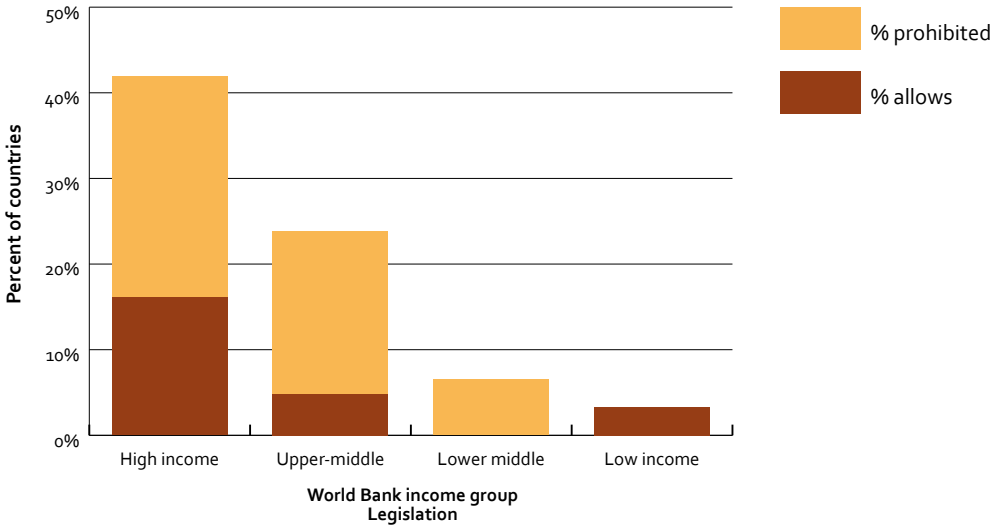


Figure 7 shows the percentage of countries reporting legislation that allows or prohibits online medication purchases from abroad based on World Bank income groups. The results reflect a common trend with high-income countries being more likely to have such a policy than those countries in the upper-middle, lower-middle, and low-income brackets.

Figure 7. Legislation of online purchase of pharmaceuticals from abroad, by World Bank income group



Countries with policies prohibiting the online ordering of pharmaceuticals from other countries were also asked to describe the consequences for breach of the law. The particular penalties included in the survey were:

- Seizure of goods
- Consumer fine or prosecution
- No consequences
- Other

Only 20% of responding countries provided a specific consequence associated with ordering pharmaceuticals from foreign countries over the Internet. Of the remaining countries, 20% said there were no consequences for breaching the law, 28% did not know if there were consequences and 31% did not answer (Figure 8).

Figure 8. Consequences for breach of law

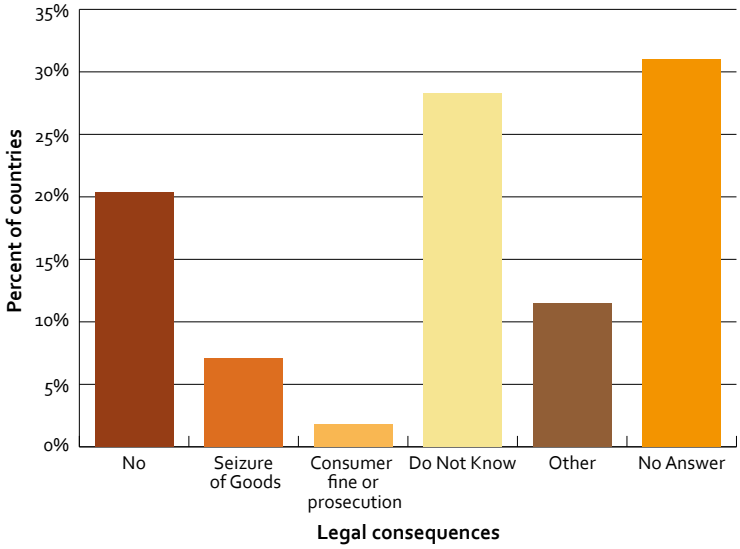


Table 6 summarizes the consequences for breach of law, including a description of any penalty described by responding Member States as "other". It is important to note that some countries stating there was no legislation, or even that their government allows the online purchase of pharmaceuticals from foreign countries, provided examples of consequences under "other".

For example, among the countries that responded there was legislation allowing Internet pharmacy sales purchased online from other countries, three later responded that the consequence for breach of law was seizure of goods and/or consumer fine or prosecution. In the same way, four countries which responded "no legislation" (Azerbaijan, Iceland, India, Malaysia), gave seizure of goods as a consequence for breach of law.

These seemingly contrary replies appeared to occur most often in countries which allow online ordering of pharmaceuticals (e.g. Germany responded "allows" for question 6.16), but only from a limited number of other countries (and thus entered a consequence for breach of law in question 6.17). It is quite possible that the legislative situation within countries is not straightforward, which would lead to reasonable explanations for why so many responses to this series of questions seemed inconsistent on the surface, as exemplified by Germany.

Table 6. Summary of legislation and consequences for breach of law

Country	Legislation	Consequence	Description of "other"
Greece	Allows	Seizure of goods	—
Finland	Allows	Consumer fine or prosecution	—
Germany	Allows	Other	According to the country list of the German Federal Ministry of Health (BMG), currently mail order pharmacies of the following three countries are allowed to send pharmaceuticals to German customers: the United Kingdom, the Netherlands (only if a community pharmacy exists in addition to the mail order pharmacy), and the Czech Republic (only allowed for non-prescription drugs).
Norway	Allows	Other	Consequences for breach of the law are seizure of goods and consumer fine or prosecution.
Poland	Allows	Other	All of above refers only to drugs available without a prescription. Prescription drugs can be purchased only from brick-and-mortar pharmacies (not online).
Croatia	Prohibits	Seizure of goods	—
Estonia	Prohibits	Seizure of goods	—
Morocco	Prohibits	Seizure of goods	—
Jordan	Prohibits	Consumer fine or prosecution	—
New Zealand	Prohibits	Other	Some drugs are only available to consumers by presenting a written prescription; there is more general legislation covering the importation of goods, and a licence is required to import in some circumstances.
Turkey	Prohibits	Other	Medicines are only allowed to be sold in pharmacies. Ministry of health policy is to forbid any selling initiatives except through pharmacies. This policy is formally empowered with related legislations.
Azerbaijan	None	Seizure of goods	—
Iceland	None	Seizure of goods	—
India	None	Seizure of goods	—
Malaysia	None	Seizure of goods	—
Austria	None	Other	If requirements of Doc-Morris-Judgment (C-322/01) are not fulfilled.
Bangladesh	None	Other	—
Canada	None	Other	—
Cyprus	None	Other	Seizure and prosecution
Denmark	None	Other	—
Malta	None	Other	No consequences as long as the ordered medicinal products are for personal use.
Pakistan	None	Other	—
Singapore	None	Other	—

— indicates field not completed by Member State.

Implications

As detailed in Section 2, many of the risks associated with online pharmaceutical purchases are compounded when Internet pharmacies located in foreign countries. This is because without suitable harmonized legislation, treaties, and cooperative agreements between Member States, rogue Internet pharmacies can evade stringent regulation by operating their web sites within jurisdictions having the least restrictive regulatory framework. The lack of legal statutes and inconsistent consequences for breach of law globally and within WHO regions reflects the need for greater development of governance mechanisms to facilitate the creation of political and legal frameworks for the online sale of pharmaceuticals.

3.2 Internet security

As outlined in the GOe survey, preservation of trust online is an important element as eHealth matures. The issue of unsolicited electronic messages sent in bulk, known as spam, is growing exponentially and threatens to undermine this trust. In recent years spam has evolved from disruptive, malicious messages or irritating advertising into a global business linked to crime, fraud, and identity theft.

To establish how Member States are dealing with escalating Internet security issues, countries were asked to describe what actions were being taken to reduce spam.

Key findings

- Overall, technology filters are the most common method for combating spam among responding countries.
- Government intervention, educational programmes, and mechanisms to report abuse are much more likely to occur in high-income countries.
- Local filters at the organizational/business level are the primary way to prevent spam in all WHO regions.

Figure 9 illustrates that technology filters at both the Internet service provider (ISP) level (67%) and the organizational/business level (75%) are the most popular methods for combating spam. Government intervention (e.g. laws, regulations), educational programmes for consumers and professionals, and mechanisms to report abuse also exist but on a much smaller scale.

Figure 10 shows that government interventions (55%), education (52%), and reporting (55%) are much more frequently used in high-income countries than in low-income countries. Unsurprisingly, developed countries also report a higher use of technology to combat spam than developing ones.

When divided into WHO regions (Figure 11), filters at the local (i.e. organizational/business) level ranked as the number one preventive action in the African (63%), Eastern Mediterranean (71%), and Americas (92%) Regions and shared this ranking with ISP filters in the European (81%) and South-East Asia (88%) Regions.

Despite the reliance on technological solutions, several countries indicated that a multi-pronged strategy was needed in order to combat the threats posed by spam. Singapore has developed a programme that combines the benefits of a public education programme, appropriate technology measures, industry self-regulation, spam control legislation, and international cooperation to curb spam.

Canada has also undertaken a number of efforts and initiatives to help deal more effectively with spam. The Working Group on Anti-Spam Technology and Network Management began in 2004 to bring various industry groups together to encourage the broad adoption of best practices among ISPs, other network operators, and large enterprise users *(170)*. The Anti-Spam Action Plan for Canada was also introduced at that time *(171)*. In December 2010, Canada passed extensive anti-spam legislation (i.e. Fighting Internet and Wireless Spam Act) *(172)* that includes formation of a Spam Reporting Centre, which will come into force following a Governor in Council order *(173)*. Parallel and temporally similar efforts were also made with the introduction of the so-called CAN-SPAM Act (i.e. Controlling the Assault of Non-Solicited Pornography and Marketing) *(174)*. Finally, the efforts of The Spamhaus project, detailed in Section 1, also deserve mention.

Figure 9. Actions to reduce spam, globally

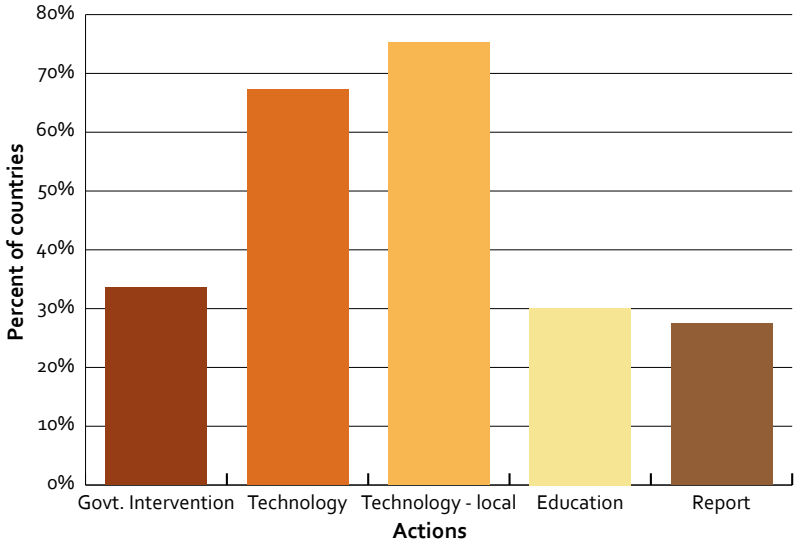


Figure 10. Actions to reduce spam, by World Bank income group

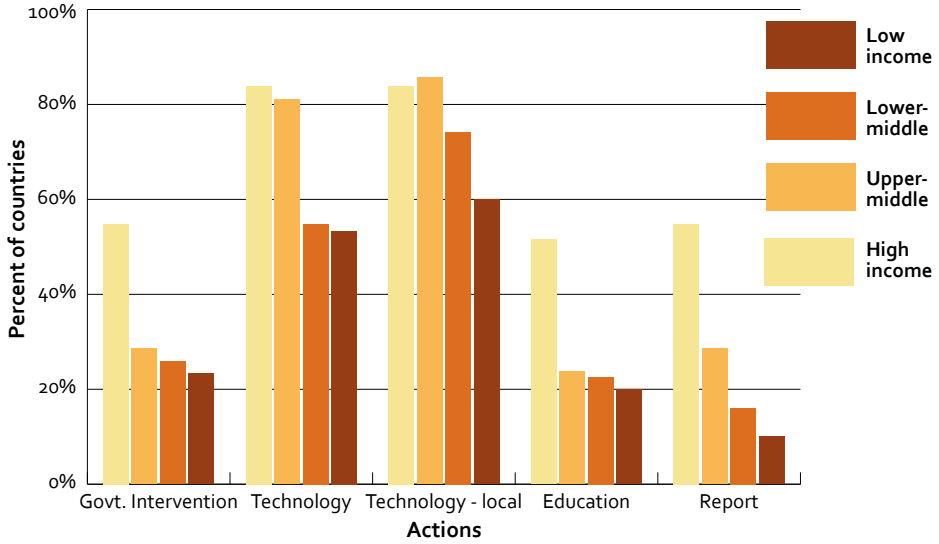
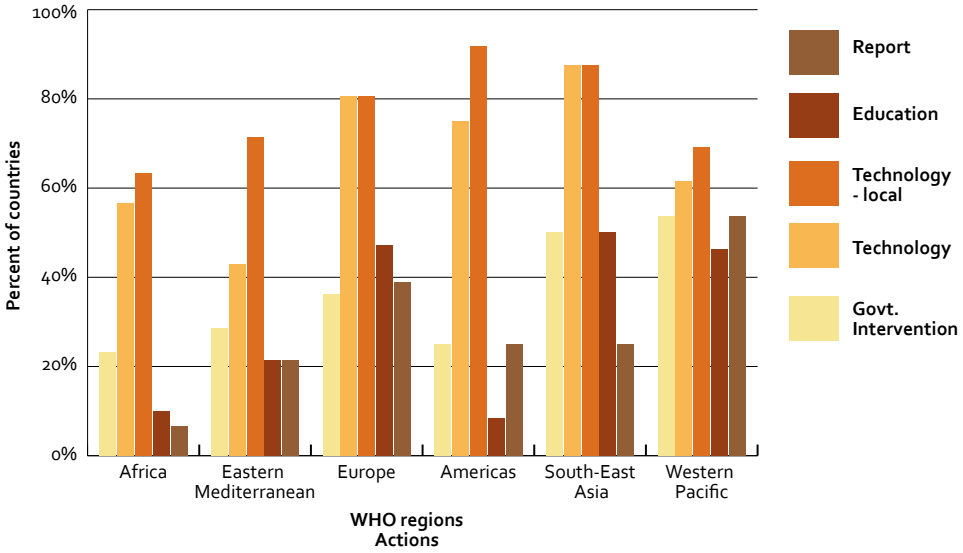


Figure 11. Actions to reduce spam, by WHO region



Implications

Based on the results of the survey it would appear that many Member States have either actively or passively decided to leave the matter of safeguarding against spam to individual businesses, organizations, and citizens. This may be, in part, as most popular e-mail clients have built-in spam filters that pre-sort incoming e-mail messages and can block up to 98% of spam messages, ensuring that the majority of the messages found in an individual's inbox is genuine e-mail *(175)*. However, local spam filters have no effect at all in combating the *distribution* of spam messages.

According to survey responses, only 34% of responding Member States have government laws or regulations in place to stem the tide of spam. To compound the issue, few developing nations have other types of law, such as consumer protection laws, privacy or network security laws, or computer crime regulations that could be used to prosecute spammers. As a result, many Member States are not only restricted in their ability to keep spammers from exploiting their citizens but also in preventing spammers from using their countries as a base for sending spam to other countries.

Spam is a global problem; therefore, international cooperation is key. It is clear from these results that further promotion and development of an international, multi-pronged approach to reducing spam is needed.

3.3 Online safety of children and adolescents

The development of the Internet has created a communication medium that exists apart from the confines and structure of the 'real world', as well as away from the prying eyes of parents. While children and adolescents relish the freedom that the Internet and online anonymity can bring, it also carries with it hidden dangers, like sexual predators and the threat of cyberbullying.

Information and education about Internet safety

Key findings

- Less than half of responding countries have government-sponsored web sites or official initiatives educating citizens about Internet safety and literacy.
- Seventy-five per cent of governments responding from the South-East Asia Region sponsored online education initiatives; substantial efforts were also made in the European and Americas Regions (67%).
- Ninety-three per cent of countries with government-sponsored online education programmes had efforts aimed specifically at children.
- The Regions of South-East Asia, Europe, and the Americas had the highest rates of initiatives directed at raising awareness of Internet safety specifically among children and teenagers.

Although there are many stakeholders responsible for the safety of children and teenagers online, countries were asked to focus on their government's efforts in this area. According to the survey results, 47% of responding countries have government-sponsored web sites or official initiatives that provide appropriate information and education about Internet safety and literacy (Figure 12). Following a common trend, the highest percentage (81%) was found in high-income countries (Figure 13).

When aggregated by WHO region, 75% of responding countries from the South-East Asia Region had these web sites and official initiatives, while inroads had also been made in countries of the European (67%) and Americas (67%) Regions (Figure 14).

Figure 12. Existence of official web sites or initiatives, globally

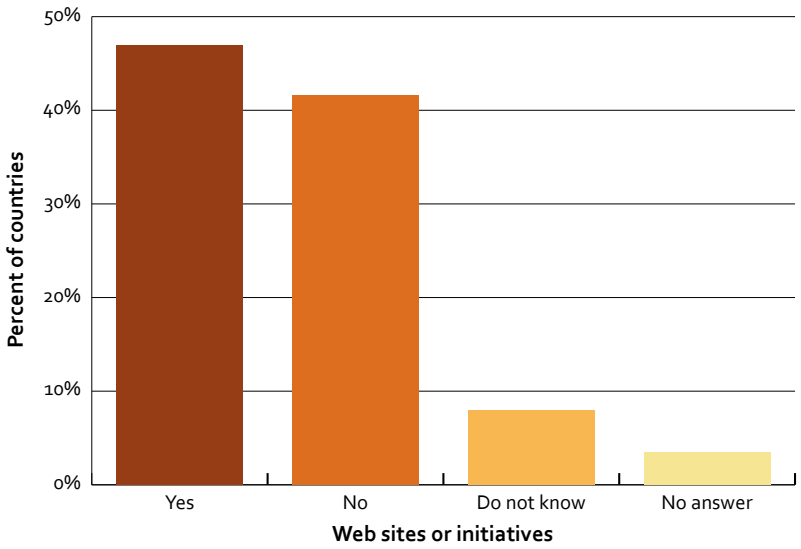


Figure 13. Web sites or initiatives by World Bank income group

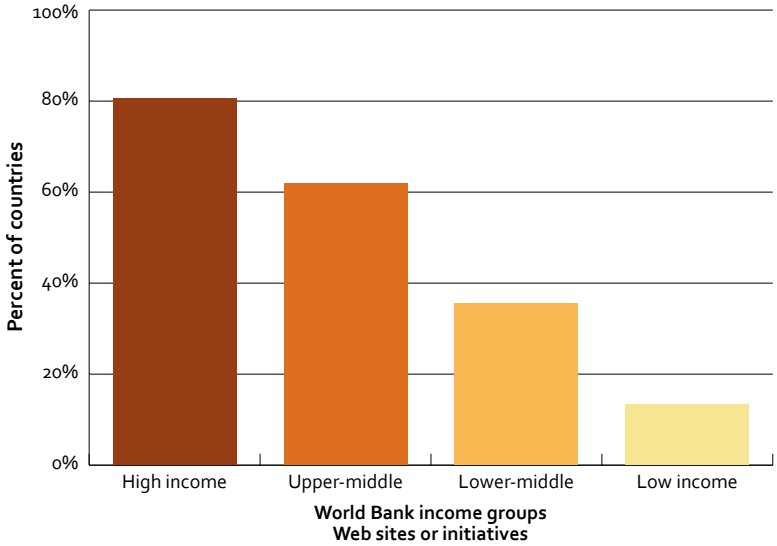
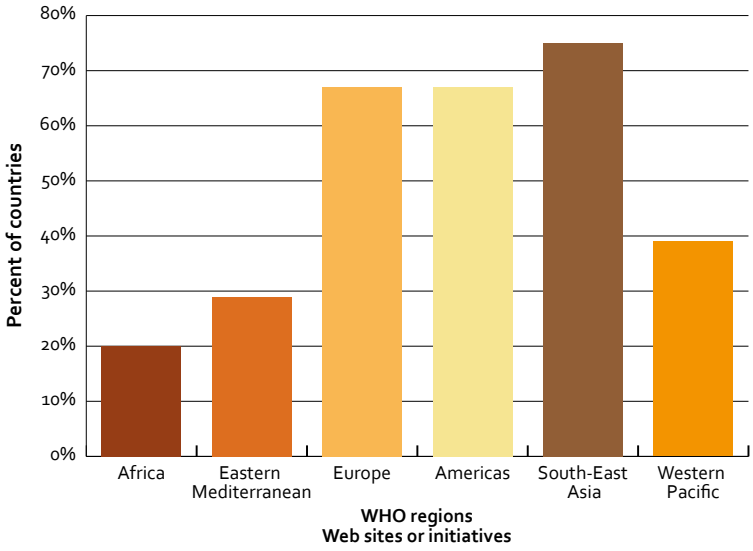


Figure 14. Web sites or initiatives by WHO region



Responding countries indicating that there were government-sponsored web sites or official initiatives in their countries were then asked whether any of these efforts were aimed specifically at protecting children. The vast majority (93%) responded in the affirmative (Figure 15).

Figure 16 shows responses to this question by World Bank income group. While the majority of countries with official informative web sites and initiatives have ones specifically directed at children and teenagers, these are mostly high-income countries. Taken as a whole, 48% of high-income countries, 24% of upper-middle income countries, 20% of lower-middle income countries, and 8% of low-income countries have initiatives explicitly designed to educate children and teenagers about online safety.

It is interesting to note the WHO regional lines (Figure 17) upon which age-targeted efforts were developed. The European (44%), Americas (14%), South-East Asia (12%), and African Regions were the most proactive in implementing initiatives specifically directed at raising awareness among children and teenagers, while the existence of such initiatives in the Western Pacific (8%), Eastern Mediterranean (8%) Regions were low.

Figure 15. Existence of efforts aimed specifically at protecting children, globally

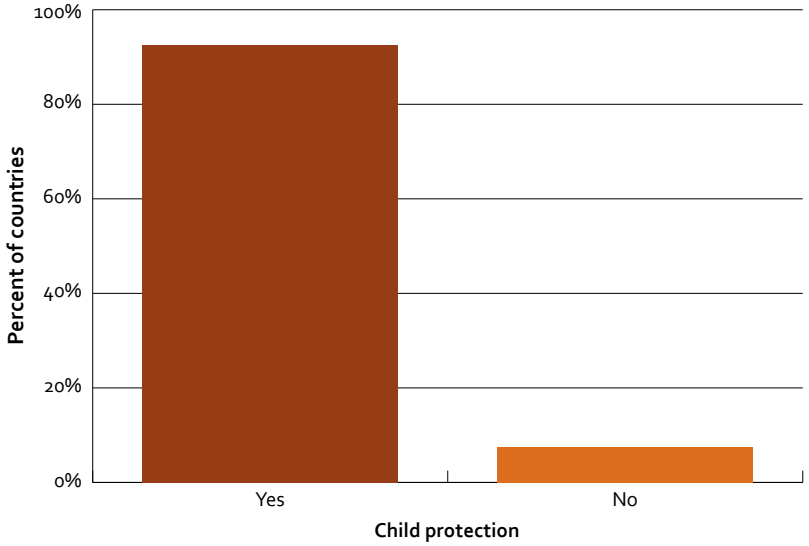


Figure 16. Specific web sites or initiatives to protect children, by World Bank income group

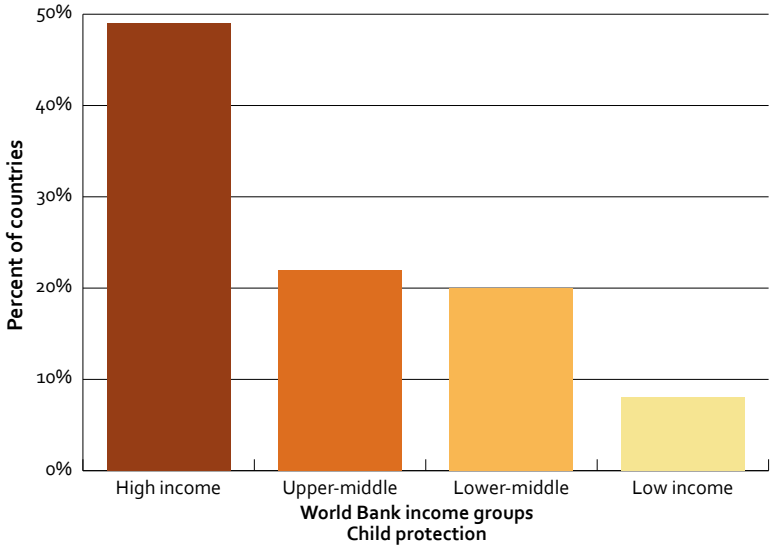
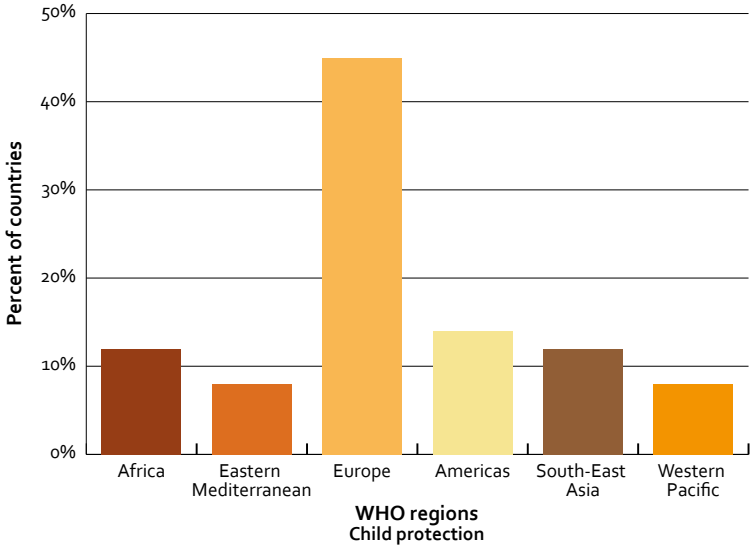


Figure 17. Specific web sites or initiatives to protect children, by WHO region



Safety and security requirements

While social and educational strategies are important for empowering children and adolescents to make responsible choices and avoid potentially dangerous situations online, technology solutions and public policy are equally important. To determine the current regulatory environment, countries were asked whether safety tools and security technologies were required by law for schools, libraries, and other public places with Internet facilities used by children.

Key findings

- Less than a quarter (22%) of responding countries legally require the use of safety tools and security technologies in public places where children access the Internet.
- Even in high-income countries only 26% have legal requirements for these safety features in public Internet facilities used by children.
- The Regions of the Americas and Europe have higher percentages of countries with legislation than other WHO regions.

Nearly half (48%) of responding countries do not legally require safety tools and security technologies in public places where children access the Internet (Figure 18). Even when stratified by income the percentages were still low, with just 26% of high-income and 43% of upper-middle income countries requiring such technologies (Figure 19). The disproportionately large gap between upper-middle income countries and high-income countries is notable; no correlation is observed between high-income countries and technology-focused legislation for this question.

Figure 20 shows the prevalence of legal requirements for the use of safety tools and security technologies in public Internet facilities used by children, by WHO region. The results show that the Regions of the Americas (67%) and Europe (28%) have a higher percentage of countries with legislation than other regions.

However, just because there is no legal requirement for safety tools and security technologies does not mean that countries responding negatively do not have protective measures in place in public places where children access the Internet. For example, in Paraguay security keys/passwords are generally used to limit access to web sites inappropriate for children. There are no specific legal requirements, simply filter systems.

Figure 18. Legal requirements for safety tools and security systems, globally

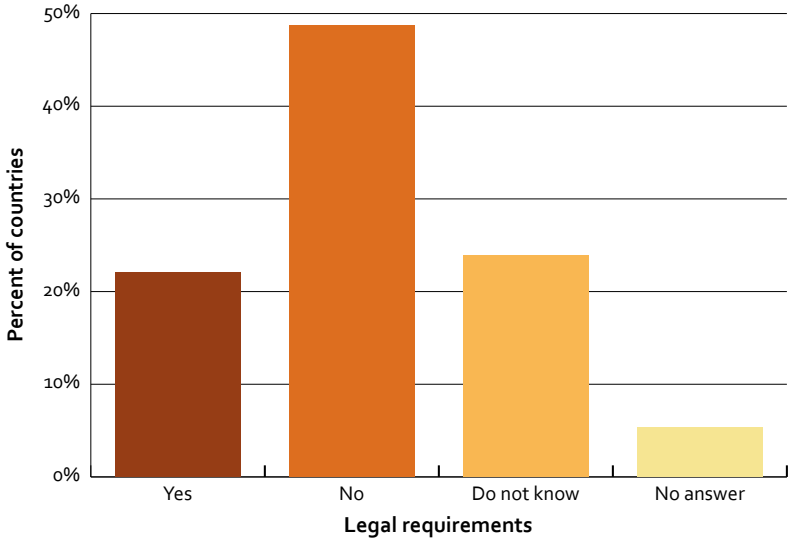


Figure 19. Legal requirements for safety tools and security systems, by World Bank income group

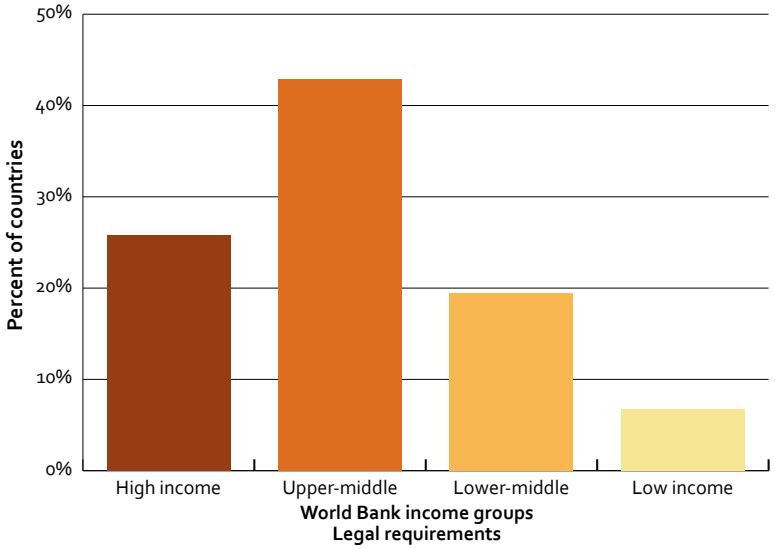
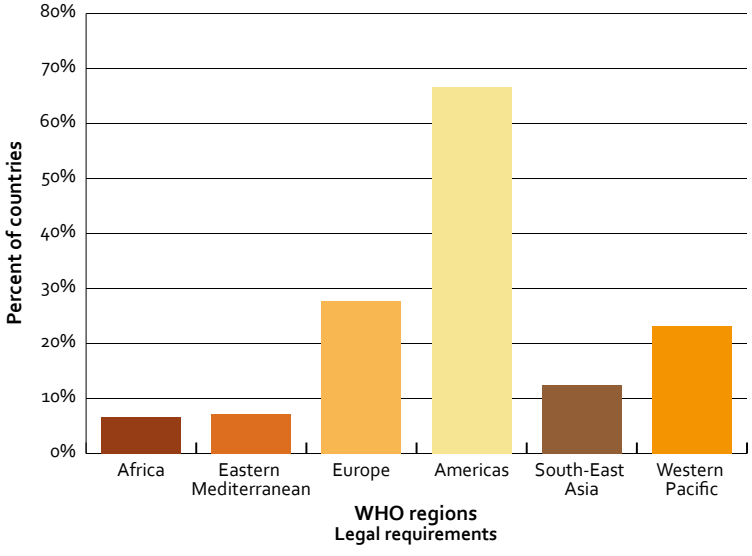


Figure 20. Legal requirements for safety tools and security systems, by WHO region



Implications

Social and educational strategies are central to the development of responsible decision-making and appropriate online behaviour in children and adolescents in order to protect them from the many dangers that lurk online. Because online content is increasingly 'user-driven,' users are becoming progressively more accountable for their personal well-being online. Their individual choices and behaviours on the Internet can help determine whether their online experiences are positive or negative. As a result, safety education for children, adolescents, teachers, parents, and other caregivers is becoming increasingly important.

Unfortunately, online education initiatives seem to be linked to income level, with much higher percentages of high- and upper-middle income countries backing initiatives dedicated to educating children and teenagers about online safety. While this may be partly because fewer children and teenagers have Internet access on demand in developing nations, there is still the potential for significant child exploitation online.

As different children in different regions of the world are subject to varying levels of risk, Member States need to evaluate and identify potential online hazards for children and adolescents living within their borders and develop a targeted approach to education, prevention, and intervention.

3.4 Digital literacy and online health information quality

The quality of health information on the Internet has been the subject of debate for a decade. While there are a number of high-quality, well researched, clinically informed eHealth sites available, health information of dubious quality, widespread fraud, potentially dangerous claims and a high risk of exposure to harm also exist online. As with all information found through search engines and other methods, the user must be able to critically evaluate the source and its claims before taking action, highlighting the importance of digital literacy.

To evaluate current government eHealth quality control practices, survey participants were asked to give details about their country's approaches for ensuring the quality of health-related content on the Internet. The particular mechanisms included in the survey were:

- voluntary compliance by content providers or web site owners to quality criteria for health-related sites;
- technology (e.g. filters and controls);
- education programmes for consumers and professionals;
- official approval (e.g. certification, accreditation, seals of approval, quality seals); and
- other.

Key findings

- Voluntary compliance (55%) was the most common quality control mechanism indicated by responding countries in all regions and income levels.

Figure 21 gives an overview of the overall use of the aforementioned quality control mechanisms. Voluntary compliance was the most commonly reported climate of control, with 55% of responding countries indicating it for their country. Technology (28%), government intervention (26%), and education programmes (23%) were also used by responding countries, while official approval or other methods were utilized by a small percentage (16% and 5% respectively).

Figure 22 shows the use of the various quality control measures based on World Bank income group. While the pattern of results is consistent for all income levels, the highest levels recorded for voluntary compliance and the lowest levels for official approval and other methods show that the magnitude of utilization is appreciably different between developed and developing countries. For example, nearly 70% of high- and upper-middle income countries employ voluntary compliance, while only 33% of low-income countries do so.

Figure 23 provides an additional perspective, displaying the same countries by WHO region. It is interesting to note that 100% of an albeit small number of responding countries (eight) in the South-East Asia Region report voluntary compliance, with significantly lower levels of government interventions, technology, education, and other mechanisms (between 0 and 38%). In the African Region approximately 20% of countries affirm voluntary compliance, government intervention and technology mechanisms.

Figure 21. Quality control mechanisms for health information, globally

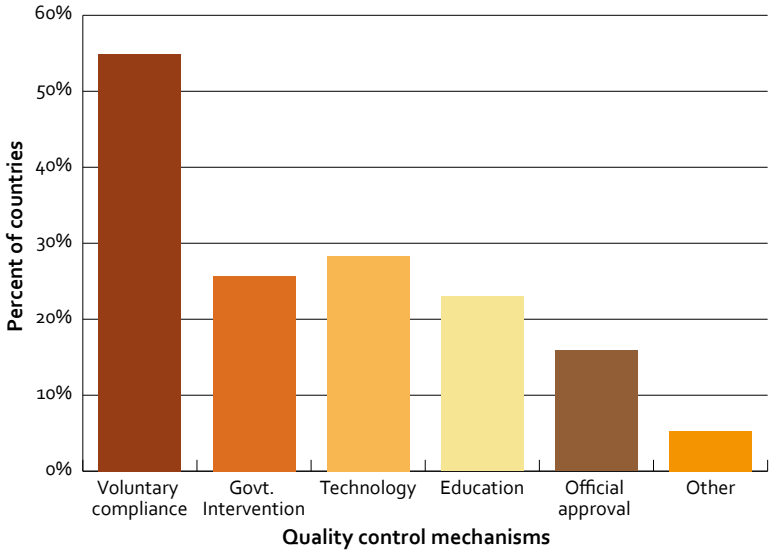


Figure 22. Quality control mechanisms for health information, by World Bank income group

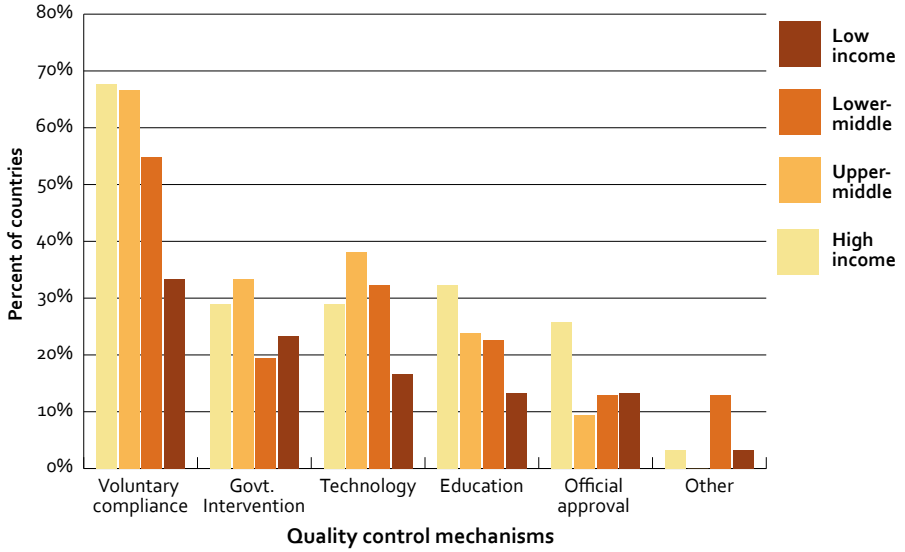
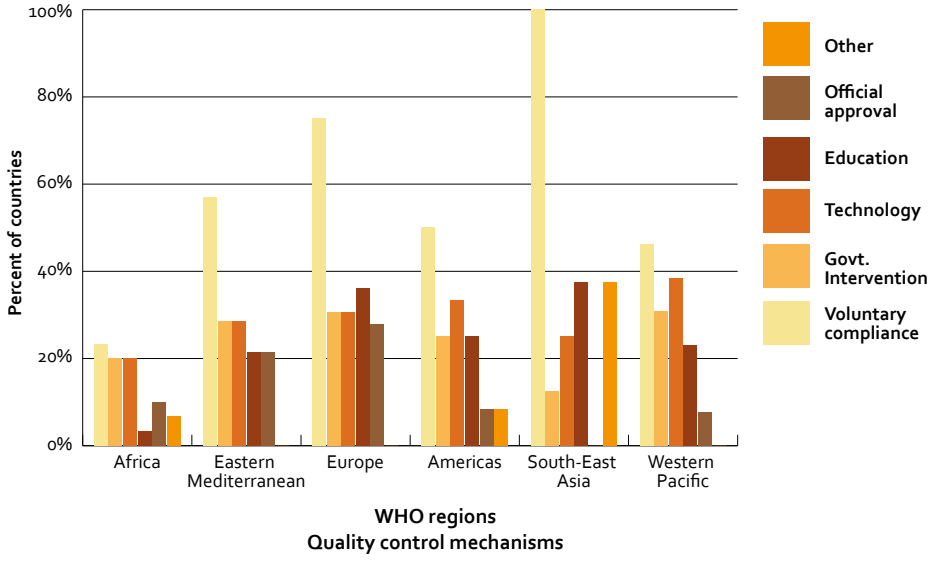


Figure 23. Quality control mechanisms for health information, by WHO region



Responding countries who replied with "other" were asked to elaborate on the methods employed. Table 7 summarizes the responses.

Table 7. Other quality controls employed by Member States

Country	Elaboration of the "other" response
Bangladesh	Permission needed from appropriate authority for uploading information on pharmaceutical products.
Bhutan	Some verbal caution is given to consumers regarding authenticity of health-related information on the Internet.
Cameroon	Informal.
Canada	Governments at various levels in Canada, including the federal government, have themselves provided considerable health information on their own web sites. Surveys have indicated that the Health Canada web site is a frequently used source of health information. Provincial ministries of health also post health information on their web sites.
India	Sites are developed where the processes ensure quality of information (e.g. www.nhicindia.org). IT law laid down by the Department of Information Technology, Ministry of Communications & IT, Government of India.
Sri Lanka	Awareness creation among the public using medical students.
Nigeria	Disclaimer notices.

Implications

Despite the fact that a large number of people base important health decisions on information they find on the Internet, there is very little being done to ensure the accurate reporting of health information online. Currently, it is the responsibility of the individual site to determine the quality of health-related content. As a significant amount of time, effort, and money would be required to establish governance mechanisms to facilitate the development and implementation of policy and legal frameworks, a better option may be to invest in educational programmes to increase digital literacy.

Erroneous and deceitful health information is particularly dangerous if acted upon unquestioningly. By improving the public's critical evaluation of health information, citizens will be empowered to make better, more informed decisions about the health content found online.

Government-sponsored eHealth sites providing authoritative content can also serve as a complement to digital literacy initiatives. Such sites would provide a benchmark of quality by which other online health information can be judged.

Box 3. How one medical student 'crowd-sourced' curation of quality online health information in 17 languages

A young man named Bertalan Mesko attending medical school in Debrecen, Hungary was using his blog as a platform to collect and share information on 'Medicine 2.0' and network with others from all over the world. Noting the difficulty that even fairly Internet savvy health-care professionals and patients had in identifying, managing, and organizing reputable sources of health information online and keeping abreast of new medical developments, he elected to develop a new aggregation tool called PeRSSonalized medicine *(176)*.

This tool functions similarly to existing RSS (Really Simple Syndication) in that it aggregates 'feeds' of information that could be set to automatically push to the end-user. However, it removed what little complexity that did exist by making it more similar to choosing items from a menu than configuring a tool. This menu of medical information was based on the interests of the individual patient or provider and included conditions such as depression, specialties like cardiology, and other categories such as a customized feed for the Pan American Health Organization (PAHO).

Image Courtesy of Dr Bertalan Mesko. PeRSSonalized Medicine: http://www.webicina.com/perssonalized/.

As this resource evolved, the capacity for any one individual to hand-select all the feeds was exceeded and the now Dr Bertalan Mesko capitalized on the collaborative nature of Web 2.0. He began to 'crowd-source' information by putting out a call to his social networks for items to be included and eventually PeRSSonalized medicine grew to encompass 80 different medical specialties and conditions that are curated today. Similarly, he started to solicit additional contributions, which resulted in health information resources being aggregated in 17 different languages including English, Spanish, Hungarian, French, German, Chinese, Japanese, and Indonesian.

> *I realized how hard it is for either medical professionals or empowered patients to keep themselves up-to-date in a medical specialty or condition…Later it was clear we need to develop national versions as well, that is why 17 languages are available in PeRSSonalized Medicine now (178).*
>
> —Dr Bertalan Mesko

While PeRSSonalized medicine now stands as a massive resource that is freely available to anyone, it is more a testament to the potential for one person to help make a difference, especially when that person taps into the cognitive philanthropy of the crowd.

9 The practice of obtaining needed services, ideas, or content by soliciting contributions from a large group of people and especially from the online community rather than from traditional employees or suppliers.

10 Used by actors in health care including doctors, patients, and scientists, Medicine 2.0 / Health 2.0 is a specific set of Web tools (blogs, podcasts, tagging, search, wikis, etc.) – founded on principles of open source and user generated content, as well as the power of networks – to personalize health care, collaborate, and promote health education *(177)*.

11 http://www.webicina.com/perssonalized/?cat=35.

4 Conclusions



The Internet pharmacy has moved beyond its nascent stage into a more widely adopted and legislated extension as a potentially trusted source of medications and pharmaceutical care. However, rogue pharmacies – increasingly advertised through spam messages – still plague those using the Internet. Due to a dearth of vetted, high-quality online health information, people mostly have access to untrustworthy health information online, and are putting themselves at risk of virus programs and phishing scams. Spam also continues to be the bane of e-mail users worldwide.

Is the answer to Internet pharmacies a blanket ban? Unconditional, unrestricted access? Or the juxtaposition of intelligent legislation, good practices, and coordinated vigilance? How can we best capitalize on freely available Internet-based health information to empower patients for the evolving participatory medicine model? What protections need to be in place to safeguard citizens and their children from Internet-based threats? This publication has provided a snapshot of current practices, responses to issues by Member States, and case studies examining the transformation of cautionary tales to tales of success. The information contained within this volume is provided for stakeholders including policy-makers, practitioners, and patients in the interest of a sustainable provision of equitable health care. The summary conclusions that follow are intended to assist stakeholders in informing their decision-making processes regarding Internet pharmacies and online safety and information quality. These conclusions are derived from feedback supplied by Member States in responding to a subset of items on the 2009 global survey on eHealth administered by WHO.

Overall, the results describe an atmosphere of uncertainty regarding Internet pharmacy. Despite existing as a business and practice model in some parts of the world for over ten years, Internet pharmacy remains legislatively unaddressed by the majority of responding countries (Figure 1). As policies were likely reactionary and temporally related to the emergence of this model of pharmacy, developed countries correspondingly were more likely than developing countries to have general legislation and specific policies in place. However, even among the minority of countries who have broached the topic, as a matter of policy they have elected to simply prohibit their operations rather than permit them (Figure 1). Regardless of the stance, Member States should adopt formal positions regulating Internet pharmacy to protect public health and, when feasible, create an alternative but secure distribution channel for delivery of essential medicines. Member States with existing legislation identified in this volume (China, Czech Republic, Finland, Germany, Latvia, Poland, Portugal, USA) can be a valuable point of contact and data for other countries wishing to move forward in this arena. Organizations and institutions including the FIP as well as boards of pharmacy in each respective Member State also merit consulting based on their work in these areas.

In concert with, or following determination of, a basic domestic legislative approach, regulating the external online sale of pharmaceuticals should be considered a priority. Even fewer Member States have policies in place determining whether or not medications from other countries are legally permitted or restricted (Figures 6 and 7). Significantly, almost 80% of responding countries did not have consequences for breach of law using Internet pharmacies, were not aware of such consequences, or did not respond to the question. The key to addressing this deficit is in developing and enacting enforceable legislation that supports public health while satisfying any harmonization requirements that may be in place with neighbouring countries or trade partners. International pharmacy law experts and Member States with current legislation may again serve as resources.

Spam – unsolicited messages sent to e-mail and mobile devices in bulk – and other types of Internet security threats continue to be a scourge: costing citizens and Member States significant resources to bolster Internet and e-mail security, as well as mitigate the effects of successful attacks. Technology filters both at the local (e.g. business) and ISP levels (Figure 9) remain the primary line of defence for Member States against spam. While governmental intervention and educational programmes are also mechanisms used to combat it, these tactics are more prevalent in World Bank designated high-income countries.

A two-pronged approach is recommended to counter distribution and receipt of spam based on the findings in this volume, including continued international support of non-profit-making efforts (e.g. Spamhaus), as well as consolidation of fragmented educational efforts. It may also behove Member States to develop stronger definitions, penalties, and enforcement for spam along with aligning with the cybersecurity efforts of the International Telecommunication Union (ITU). Some responding countries indicated that legislative acts addressing spam had been created, but had never been enacted into law and/or a lack of media coverage stifled awareness about its existence thereby compromising capacity for enforcement. Additionally, findings suggest reallocating existing resources – currently diluted in multiple ways – to educational programmes to help avoid the more serious threats that can accompany spam (e.g. viruses, spyware) and specifically increase vigilance regarding medical identity theft in upper-middle and high-income countries.

While security issues such as spam create problems numbering in the billions of any currency, the most polarizing public health threat presented by the Internet may be as a means to intentionally or unwittingly jeopardize the safety of children and adolescents. Threats from this medium encompass those from predatory adults, cyberbullying from peers, and poor personal judgment by teens that elect to engage in activities like 'sexting' without thought of consequence. Despite this state of affairs, less than a quarter of responding countries legally require the use of safety tools and security technologies in public places where children access the Internet (Figure 18). Among high- and upper-middle income countries, however, a collective 69% have those legal requirements in place to protect children (Figure 19). Overall the most progressive WHO region in implementing these measures is the Region of the Americas (Figure 20).

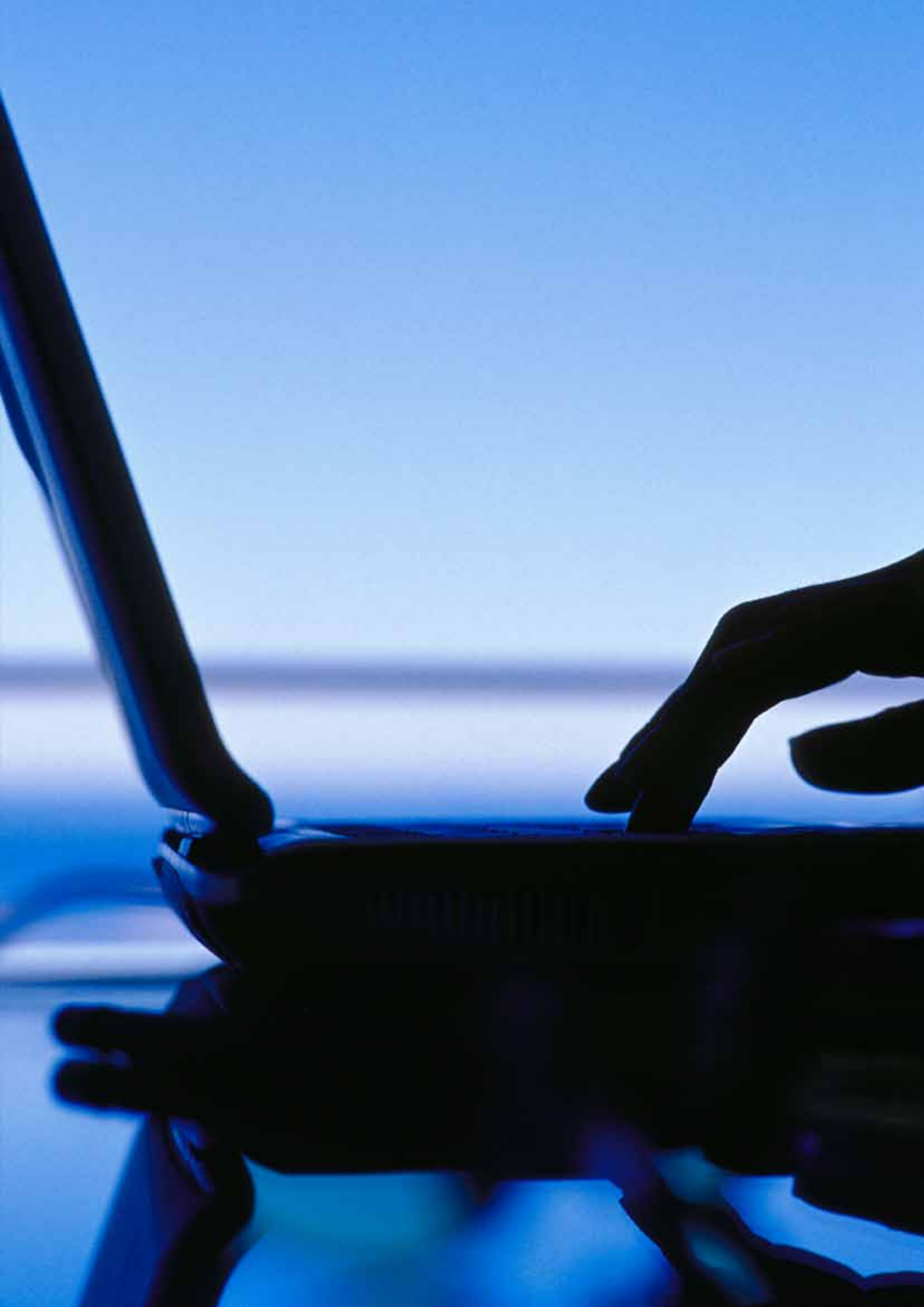
For those Member States contemplating introduction, prioritization, or strengthening of such legislation, libraries, schools, and community centres granting Internet access to children and teenagers are natural foci for directing legislative and intervention efforts to enhance child safety. Guidance in these efforts may be sought in the form of the Family Online Safety Institute (FOSI). Given the sometimes slow wheels of the legislative process and for deriving maximum benefit, child safety programmatic initiatives should also be considered in a similarly geographically-targeted manner.

Moving into the next decade, Internet safety and literacy present enormous challenges, considering basic and health literacy are still hurdles to be overcome in most Member States. Currently, less than half of responding countries utilize government-sponsored web sites or official initiatives to educate citizens about Internet safety and literacy. Paralleling its proclivity for early adoption of technology and innovation, government sponsored initiatives are seen most commonly in the South-East Asia Region; there are also strong programmes in the European and Americas Regions (Figure 14). Echoing these findings, the European Region and – to a much lesser extent – the Region of the Americas have the highest rates of initiatives specifically directed at protecting children and adolescents (Figure 17). Countries in other regions should consider prioritizing this area; lower rates of Internet penetration insulated the youth of those areas to an extent previously, but with the explosion of mobile accessibility as reported in *mHealth: new horizons for health through mobile technologies (179)*, the face of Internet access has changed. Universally, Member States would benefit both from existing efforts and could explore formalizing or codifying educational practices to integrate digital literacy and awareness of online safety issues into requisite schooling and adult education.

The capacity for digital literacy is intertwined with accessibility to, and quality of, online health information. It is anticipated that the importance of these issues will become even more prominent as a greater percentage of the global public gains ready access to the Internet and health information seekers grow more likely to take action based upon what they find. Thus far, voluntary compliance by web site operators and content providers is the most commonly cited control mechanism by Member States to help ensure the quality of health information online (Figure 21). However, within this approach there is great variability based on World Bank classifications: nearly 70% of high- and upper-middle income countries employ voluntary compliance, whereas only 33% of low-income countries take such action (Figure 22). Interestingly, strategies to address health quality online by Member States were wide-ranging, as indicated by the spectrum of answers received to the "other" category for this survey item (Table 7).

Solutions for managing the quality of health information proposed were inclusive of town, state, provincial, and country levels. Technological approaches such as medically focused search engines have been explored and 'seals of approval' conferred by a third party regardless of geography or government (like the HONcode seal; Box 1) have also been examined. These tools have limited utility considering the rapid global expansion of the Internet. The most holistic and ambitious plan proposed to date is the creation of the dot health (.health) TLD. Development of a dot health TLD as a recognizable label for quality health-related information sources on the Internet would raise awareness of health information quality issues. It would overcome a serious shortcoming of existing codes of conduct by enabling codes to be enforced; however, it would not regulate, restrict or censure health content on the Internet.

Developing countries would benefit from being able to use a domain where standards are not the problem of governments alone to solve. The standards would protect consumers with measures for privacy and security, as well as benefit national health systems as they increasingly integrate the Internet into their operations. Dot health's operational model is most likely to be a consortium led by an appropriate international organization and with a membership of high-level stakeholders with interests in public health.



5 References

1. Atkin DJ, Jeffres LW, Neuendorf KA. Understanding Internet adoption as telecommunications behavior. *Journal of Broadcasting and Electronic Media*, 1998, 42(4):475–90.
2. Barbosa GT. *Internet use 1990*. Sheffield, University of Sheffield, 2006 (www.worldmapper.org/posters/worldmapper_map335_ver5.pdf, accessed 2 March 2011).
3. Internet usage statistics. Internet World Stats, 2011 (http://www.Internetworldstats.com/stats.htm, accessed 13 October 2011).
4. Davis D. Global e-commerce sales head for the $1 trillion mark. Chicago, Vertical Web Media, 2011 (http://www.Internetretailer.com/2011/01/04/global-e-commerce-sales-head-1-trillion-mark, accessed 9 October 2011).
5. The cost of cybercrime. A Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office. Surrey, Detica Limited, 2011. (http://www.cabinetoffice.gov.uk/sites/default/files/resources/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf, accessed 10 October 2011).
6. Flannery MA. Building a retrospective collection in pharmacy: a brief history of the literature with some considerations for U.S. health sciences library professionals. Bulletin of the Medical Library Association, 2001, 89(2):212–221.
7. George C. Internet pharmacies: Global threat requires a global approach to regulation. Hertfordshire Law Journal, 2006, 4(1):12–25.
8. Weiss AM. Buying prescription drugs on the Internet: promises and pitfalls. Cleveland Clinic Journal of Medicine, 2006, 73(3):282–288.
9. Ovaskainen H. Internet pharmacies: advantages and risks. WHO Drug Information, 2001, 15(3/4):149–151.
10. Anand A et al. Internet pharmacy: need to be implemented in India. Chronicles of Young Scientists, 2010, 1(1):16–25. Palumbo FB et al. Policy implications of drug importation. *Clinical Therapeutics*, 2007, 29(12):2758–2767.
11. Palumbo FB et al. Policy implications of drug importation. *Clinical Therapeutics*, 2007, 29(12):2758–2767.

12. Anderson C et al. The WHO UNESCO FIP Pharmacy Education Taskforce. *Human Resources for Health*, 2009, 7:45.

13. Littlejohn C et al. Internet pharmacies and online prescription drug sales: a cross-sectional study. *Drugs Education Prevention & Policy*, 2005, 12(1):75–80.

14. Spamhaus Project. The definition of spam. Available from: http://www.spamhaus.org/definition.html.

15. *Symantec.cloud MessageLabs Intelligence: May 2011 intelligence report*. Mountain View, Symantec, 2011 (http://www.symanteccloud.com/mlireport/MLI_2011_05_May_FINAL-en.pdf, accessed 10 October 2011).

16. Kanich C et al. Spamalytics: an empirical analysis of spam marketing conversion. *Communications of the ACM*, 2009, 52(9):99–107.

17. Fogel J, Shlivko S. Weight problems and spam e-mail for weight loss products. *Southern Medical Journal*, 2010, 103(1):31–36.

18. Kako-Batt Y. *Pharmacy spam: pharmaceutical websites fall into two distinct operations*. Mountain View, Symantec, 2010 (http://www.symantec.com/connect/blogs/pharmacy-spam-pharmaceutical-websites-fall-two-distinct-operations, accessed 10 October 2011).

19. Hu H et al. WiFi networks and malware epidemiology. *Proceedings of the National Academy of Sciences of the United States of America*, 2009, 106(5):1318–1323.

20. *Symantec.cloud MessageLabs Intelligence: February 2011 intelligence report*. Mountain View, Symantec 2011 (http://www.symanteccloud.com/mlireport/MLI_2011_02_February_FINAL-en.PDF, accessed 10 October 2011).

21. *Cyber banking fraud. Global partnerships lead to major arrests*. Washington, DC, Federal Bureau of Investigation, 2010 (http://www.fbi.gov/news/stories/2010/october/cyber-banking-fraud, accessed 10 October 2011).

22. Mancilla D, Moczygemba J. Exploring medical identity theft. *Perspectives in Health Information Management*, 2009, 6:1e.

23. Booz Allen Hamilton. *Medical identity theft final report.* Washington, DC, United States Department of Health and Human Services, 2009 (http://www.hhs.gov/healthit/documents/MedIdTheftReport011509.pdf, accessed 10 October 2011).

24. Ramasubramanian S. *Task Force on Spam. Spam issues in developing countries.* Paris, Organisation for Economic Co-Operation and Development, 2005 (www.oecd.org/dataoecd/5/47/34935342.pdf, accessed 10 October 2011).

25. Strasburger VC, Jordan AB, Donnerstein E. Health effects of media on children and adolescents. *Pediatrics*, 2010, 125(4):756–767.

26. Stanley J. *Child abuse and the Internet*. Melbourne, National Child Protection Clearinghouse, 2001 (http://www.aifs.gov.au/nch/pubs/issues/issues15/issues15.html, accessed 10 October 2011).

27. Marsh L et al. Brief report: text bullying and traditional bullying among New Zealand secondary school students. *Journal of Adolescence*, 2010, 33(1):237–240.

28. Dowdell EB, Bradley PK. Risky Internet behaviors: a case study of online and offline stalking. *Journal of School Nursing*, 2010, 26(6):436–442.

29. UNIS-UN. *The web: wiring our world*. 35th Annual International Student Conference 3–4 March 2011. A Working Paper. New York, United Nations, 2011.

30. Mishna F et al. Cyber bullying behaviors among middle and high school students. *The American Journal of Orthopsychiatry*, 2010, 80(3):362–374.

31. Jones-Kavalier BR, Flannigan SL. Connecting the digital dots: literacy of the 21st Century. *Educause Quarterly*, 2006, 29(2).

32. Gilster P. *A primer on digital literacy*. Mississauga, Ontario, John Wiley & Sons, 1997.

33. Ivanitskaya L, O'Boyle I, Casey AM. Health information literacy and competencies of information age students; results from the interactive online Research Readiness Self-Assessment (RRSA). *Journal of Medical Internet Research*, 2006, 8(2):e6.

34. Norman CD, Skinner HA. eHealth literacy: essential skills for consumer health in a networked world. *Journal of Medical Internet Research*, 2006, 8(2):e9.

35. Eshet-Alkalai Y, Chajut E. Changes over time in digital literacy. *Cyberpsychology and Behavior*, 2009, 12(6):713–715.

36. Ivanitskaya L et al. Dirt cheap and without prescription: how susceptible are young US consumers to purchasing drugs from rogue Internet pharmacies? *Journal of Medical Internet Research*, 2010, 12(2):e11.

37. Fox S. *The social life of health information 2011*. Washington, DC, Pew Internet & American Life Project, 2011 (http://pewinternet.org/~/media/Files/Reports/2011/PIP_Social_Life_of_Health_Info.pdf, accessed 26 October 2011).

38. *The growing influence and use of health care information obtained online*. NY, NY, Harris Interactive, 2011 (http://www.harrisinteractive.com/vault/HI-Harris-Poll-Cyberchondriacs-2011-09-15.pdf, accessed 26 October 2011).

39. *Cybercitizen Health Europe. Connecting with Europeans online for health: digital marketing strategies for building consumer relationships*. NY, NY, Manhattan Research, LLC, 2008.

40. McDaid D, Park A. *BUPA Health Pulse 2010. Online health: untangling the web*. London, The London School of Economics and Political Science, 2011.

41. Fox S. *Online health search 2006*. Washington, DC, Pew Internet & American Life Project, 2006 (http://www.pewInternet.org/Reports/2006/Online-Health-Search-2006.aspx, accessed 10 October 2011).

42. *Report on objective 11-4: estimating the proportion of health related web sites disclosing information that can be used to assess their quality*. Washington, DC, Department of Health and Human Services, 2006. (http://www.health.gov/communication/healthypeople/obj1104/default.htm, accessed 9 October 2011).

43. Fox S, Purcell K. *Chronic disease and the Internet*. Washington, DC, Pew Internet & American Life Project, 2010 (http://pewinternet.org/~/media//Files/Reports/2010/PIP_Chronic_Disease_with_topline.pdf, accessed 26 October 2011).

44. Akerkar SM et al. Use of the Internet as a resource of health information by patients: A clinic-based study in the Indian population. *Journal of Postgraduate Medicine*, 2005, 51:116–118.

45. Sarasohn-Kahn J. *Health citizens in emerging countries seek health information online even more than their peers in developed economies*. Philadelphia, Health Populi, 2011 (http://healthpopuli.com/2011/01/06/health-citizens-in-emerging-countries-seek-health-information-online-even-more-than-their-peers-in-developed-economies/, accessed 10 October 2011).

46. Boyer C et al. The Health On the Net code of conduct for medical and health web sites. *Computers in Biology and Medicine*, 1998, 28(5):603–610.

47. Boyer C, Geissbuhler A. A decade devoted to improving online health information quality. *Studies in Health Technology and Informatics*, 2005,116:891–896.

48. Boyer C, personal communication, 2011.

49. Nabarette H et al. Certification des sites dédiés à la santé en France. [Certification of health-related web sites in France]. *Presse Medicale*, 2009, 38(10):1476–1483.

50. Berland GK et al. Health information on the Internet: accessibility, quality, and readability in English and Spanish. *The Journal of the American Medical Association*, 2001, 285(20):2612–2621.

51. Kommalage M, Thabrew A. Use of websites for disseminating health information in developing countries: an experience from Sri Lanka. In: *Proceedings of the 2nd International Conference on Theory and Practice of Electronic Governance*. Cairo, 2nd International Conference on Theory and Practice of Electronic Governance, 2008.

52. Prachusilpa S, Oumtanee A, Satiman A. A study of dissemination of health information via Internet. *Studies in Health Technology and Informatics*, 2006, 122:775.

53. Maxwell SR, Webb DJ. Internet pharmacy: a web of mistrust? *British Journal of Clinical Pharmacology*, 2008, 66(2):196–198.

54. Holmes ER, Tipton DJ, Desselle SP. The impact of the Internet on community pharmacy practice: a comparison of a Delphi panel's forecast with emerging trends. *Health Marketing Quarterly*, 2002, 20(2):3–29.

55. Fittler A, Bosze G, Botz L. Attitude of patients and customers toward on-line purchase of drugs--a Hungarian survey by community pharmacies. *Orv Hetil*, 2010, 151(48):1983–1990.

56. Orizio G et al. "Save 30% if you buy today". Online pharmacies and the enhancement of peripheral thinking in consumers. *Pharmacoepidemiology and Drug Safety*, 2010, 19(9):970–976.

57. Mutschler J, Diehl A, Kiefer F. Illegal purchase of psychotropic drugs from the Internet. *Nervenarzt*, 2007, 78(7):818–820.

58. Armstrong K, Schwartz JS, Asch DA. Direct sale of sildenafil (Viagra) to consumers over the Internet. *The New England Journal of Medicine*, 1999, 341(18):1389–1392.

59. Bate R, Hess K. Assessing website pharmacy drug quality: safer than you think? *PLoS One*, 2010, 5(8):e12199.

60. Forman RF et al. The availability of web sites offering to sell opioid medications without prescriptions. *American Journal of Psychiatry*, 2006, 163:1233–1238.

61. Gallagher CT, Chapman LE. Classification, location and legitimacy of web-based suppliers of Viagra to the UK. *International Journal of Pharmacy Practice*, 2010, 18(6):341–345.

62. Mahe E et al. Shopping for psoriasis medications on the Internet. *Journal of the European Academy of Dermatology and Venereology*, 2009, 23(9):1050–1055.

63. Memmel LM, Miller L, Gardner J. Over-the-Internet availability of hormonal contraceptives regardless of risk factors. *Contraception*, 2006, 73(4): 372–375.

64. Miller L, Nielsen C. Internet availability of contraceptives. *Obstetrics & Gynecology*, 2001, 97(1):121–126.

65. Raine C, Webb DJ, Maxwell SRJ. The availability of prescription-only analgesics purchased from the Internet in the UK. *British Journal of Clinical Pharmacology*, 2008, 67(2):250–254.

66. Orizio G et al. Online consultations in cyberpharmacies: completeness and patient safety. *Telemedicine and e-Health*, 2009, 15, 10:1022–1025.

67. Veronin MA, Nguyen NT. Comparison of simvastatin tablets from the US and international markets obtained via the Internet. *The Annals of Pharmacotherapy*, 2008, 42(5):613–620.

68. Inciardi JA et al. Prescription drugs purchased through the Internet: who are the end users? *Drug and Alcohol Dependence*, 2010, 110(1–2):21–29.

69. Bloom BS, Iannacone RC. Internet availability of prescription pharmaceuticals to the public. *Annals of Internal Medicine*, 1999, 131:830–833.

70. Orizio G et al. Cyberdrugs: a cross-sectional study of online pharmacies characteristics. *European Journal of Public Health*, 2009, 19(4):375–377.

71. *Medicines: counterfeit medicines*. Geneva, World Health Organization, 2010 (http://www.who.int/mediacentre/factsheets/fs275/en/, accessed 12 October 2011).

72. European Alliance for Access to Safe Medicines. *The counterfeiting superhighway*. Surrey, Medicom Group Ltd, 2008. (http://v35.pixelcms.com/ams/assets/312296678531/455_EAASM_counterfeiting%20report_020608.pdf, accessed 9 October 2011).

73. Westenberger BJ et al. Quality assessment of Internet pharmaceutical products using traditional and non-traditional analytical techniques. *International Journal of Pharmaceutics*, 2005, 306(1–2):56–70.

74. WHO. Growing threat from counterfeit medicines. *Bulletin of the World Health Organization*, 2010, 88(4):241–320.

75. Veronin M. Packaging and labeling of pharmaceutical products obtained from the Internet. *Journal of Medical Internet Research*, 2011, 13(1):e22.

76. Becher E, Glina S. Erectile dysfunction in Latin America and treatment with sildenafil citrate (Viagra): introduction. *International Journal of Impotence Research*, 2002, 14(Suppl 2):S1–S2.

77. Khalaf IM, Levinson IP. Erectile dysfunction in the Africa/Middle East Region: epidemiology and experience with sildenafil citrate (Viagra). *International Journal of Impotence Research*, 2003, 15(Suppl 1):S1–S2.

78. Solomon H et al. Viagra on the Internet: unsafe sexual practice. *International Journal of Clinical Practice*, 2002, 56(5):403–404.

79. Boyer EW, Wines JD Jr. Impact of Internet pharmacy regulation on opioid analgesic availability. *Journal of Studies on Alcohol and Drugs*, 2008, 69(5):703–708.

80. Liang BA, Mackey T. Searching for safety: addressing search engine, web site, and provider accountability for illicit online drug sales. *American Journal of Law and Medicine*, 2009, 35(1):125–184.

81. Dupuits FM. The effect of the Internet on pharmaceutical consumers and providers. *Disease Management and Health Outcomes*, 2002, 10:679–691.

82. Ukens C. Canada adopts VIPPS for on-line pharmacies. *Drug Topics*, 2002, 23:85.

83. National Association of Boards of Pharmacy. *Internet Drug Outlet Identification Program progress report for state and federal regulators*. Mount Prospect, IL, National Association of Boards of Pharmacy, 2011 (http://www.nabp.net/news/assets/IDOIReportJuly11.pdf, accessed 20 October 2011).

84. Catizone C, personal communication, 2011.

85. Crawford SY. Internet pharmacy: issues of access, quality, costs, and regulation. *Journal of Medical Systems*, 2003, 27(1):57–65.

86. Law E, Youmans SL. Combating counterfeit medications: The California pharmacist perspective. *Journal of Pharmacy Practice*, 2010, 24:114–121.

87. Grech V, Hugo AM. Email spam: a single user's perspective. *Journal of Visual Communication in Medicine*, 2008, 31(3):110–112.

88. Cerf VG. Spam, spim, and spit. *Communications of the ACM*, 2005, 48(4):39–43.

89. Liszka KJ et al. *Detecting pharmaceutical spam in microblog messages*. Akron, University of Akron, 2010 (http://www.cs.uakron.edu/~chan/DataMining/References/Detecting Pharma Spam --Liszka et al.pdf, accessed 10 October 2011).

90. *False claims in spam. A report by the FTC's Division of Marketing Practices.* Washington, DC, Federal Trade Commission, 2003 (http://www.ftc.gov/reports/spam/030429spamreport.pdf, accessed 10 October 2011).

91. Morimoto M, Chang S. Consumers' attitudes toward unsolicited commercial e-mail and postal mail direct mail marketing methods: Intrusiveness, perceived loss of control, and irritation. *Journal of Interactive Advertising*, 2006, 7(1):8–20.

92. Grimes GA, Hough MG, Signorella ML. E-mail end users and spam: relations of gender and age group to attitudes and actions. *Computers in Human Behavior*, 2007, 23:318–332.

93. Grimes GA. Online behaviors affected by spam. *Social Science Computer Review*, 2006, 24(4):507–515.

94. Fallows D. *Spam*. Washington, DC, Pew Internet and American Life Project, 2007 (http://www.pewInternet.org/~/media//Files/Reports/2007/PIP_Spam_May_2007.pdf.pdf, accessed 10 October 2011).

95. Forrester Research. *Consumer attitudes toward spam in six countries*. Washington, DC, Business Source Alliance, 2004 (http://www.bsa.org/country/Research%20and%20Statistics/~/media/87F4037F2B7044ECBF448A227B84BE86.ashx, accessed 10 October 2011).

96. *Results of the SpamCatcher attitude survey*. San Francisco, Mailshell, 2003 (http://www.mailshell.com/mail/client/oem2.html/step/pr/article/17, accessed 10 October 2011).

97. Marshal. *Sex, drugs and software lead spam purchase growth.* Irvine, M86 Security, 2008 (http://www.marshal.com/pages/newsitem.asp?article=748&thesection =news, accessed 10 October 2011).

98. Fogel J, Shlivko S. Consumers with sexual performance problems and spam e-mail for sexual performance products. *Journal of Internet Banking and Commerce*, 2010, 15(1):1–10.

99. Gernburd P, Jadad AR. Will spam overwhelm our defenses? Evaluating offerings for drugs and natural health products. *PLoS Medicine*, 2007, 4(9):e274.

100. Holt R. *Legislative efforts to combat spam. Joint hearing before the Subcommittee on Commerce, Trade, and Consumer Protection and the Subcommittee on Telecommunications of the Internet of the Committee on Energy and Commerce House of Representatives, 108th Congress, First Session*. Washington, DC, U.S. Government Printing Office, 2003 (http://energycommerce.house.gov/108/action/108-35.pdf, accessed 10 October 2011).

101. Dobbins M et al. School-based physical activity programs for promoting physical activity and fitness in children

and adolescents aged 6-18. *The Cochrane Database of Systematic Reviews*, 2009, (1):CD007651.

102. Fox S, Jones S. *The social life of health information*. Washington, DC, Pew Internet & American Life Project, 2009 (http://www.pewInternet.org/Reports/2009/8-The-Social-Life-of-Health-Information/01-Summary-of-Findings.aspx, accessed 10 October 2011).

103. Melamud A et al. Internet usage in households with children between 4 and 18 years old. Parent's supervision. Results of a national survey. *Archivos Argentinos de Pediatría*, 2009, 107(1):30–36.

104. Bener A et al. Do excessive Internet use, television viewing and poor lifestyle habits affect low vision in school children. *Journal of Child Health Care*, 2010, 14(4):375–385.

105. Kayiran SM, Soyak G, Gürakan B. Electronic media use by children in families of high socioeconomic level and familial factors. *The Turkish Journal of Pediatrics*, 2010, 52(5):491–499.

106. Mitchell KJ et al. Internet-facilitated commercial sexual exploitation of children: findings from a nationally representative sample of law enforcement agencies in the United States. *Sexual Abuse: A Journal of Research and Treatment*, 2011, 23(1):43–71.

107. Fuld GL. Social networking and adolescents. *Adolescent Medicine: State of the Art Reviews*, 2009, 20(1):57–72, viii.

108. McCrea B. Managing social media risks. *The Journal*, 2009.

109. Kelley AE, Schochet T, Landry CF. Risk taking and novelty seeking in adolescence: introduction to part I. *Annals of the New York Academy of Sciences*, 2004, 1021:27–32.

110. National Campaign To Prevent Teen and Unplanned Pregnancy. *Sex and tech: results from a nationally representative survey of teens and young adults*. Washington, DC, 2008 (http://www.thenationalcampaign.org/sextech/, accessed 10 October 2011).

111. Katzman D. Sexting: Keeping teens safe and responsible in a technologically savvy world. *Paediatrics and Child Health*, 2010, 15(1):41–45.

112. Marcum CD. Interpreting the intentions of Internet predators: an examination of online predatory behavior. *Journal of Child Sexual Abuse*, 2007, 16(4):99–114.

113. BeatBullying.org. *Truth of sexting amongst UK teens. Leading children's charity Beatbullying uncovers true extent of 'sexting' amongst UK teens*. London, Rochester House, 2009 (http://www.beatbullying.org/dox/media-centre/press-releases/press-release-040809.html, accessed 9 October 2011).

114. Wang J, Iannotti RJ, Nansel TR. School bullying among adolescents in the United States: physical, verbal, relational, and cyber. *The Journal of Adolescent Health: Official Publication of the Society for Adolescent Medicine*, 2009, 45(4):368–375.

115. Deirmenjian JM. Pedophilia on the Internet. *Journal of Forensic Sciences*, 2002, 47(5):1090–1092.

116. Nielssen O et al. Child pornography offenders detected by surveillance of the Internet and by other methods. *Criminal Behaviour and Mental Health*, 2011, 21(3):215–224.

117. Neutze J et al. Predictors of child pornography offenses and child sexual abuse in a community sample of pedophiles and hebephiles. *Sexual Abuse: A Journal of Research and Treatment*, 2011, 23(2):212–242.

118. Rideout VJ, Foehr UG, Roberts DF. *GenerationM2. Media in the lives of 8- to 18-year olds*. Menlo Park, Henry J. Kaiser Family Foundation, 2010 (http://www.kff.org/entmedia/upload/8010.pdf, accessed 10 October 2011).

119. Wolak J. Online 'predators' and their victims: myths, realities and implications for prevention. *The American Psychologist*, 2008, 63(2):111–128.

120. Silberg WM, Lundberg GD, Musacchio RA. Assessing, controlling, and assuring the quality of medical information on the Internet: caveat lector et viewor—let the reader and viewer beware. *The Journal of the American Medical Association*, 1997, 277(15):1244–1245.

121. Karp S, Monroe AF. Quality of healthcare information on the Internet: caveat emptor still rules. *Managed Care Quarterly*, 2002, 10(2):3–8.

122. Risk A, Dzenowagis J. Review of Internet health information quality initiatives. *Journal of Medical Internet Research*, 2001, 3(4):E28.

123. Bernstam EV et al. Usability of quality measures for online health information: Can commonly used technical quality criteria be reliably assessed? *International Journal of Medical Informatics*, 2005, 74(7–8):675–683.

124. Wootton JC. The quality of information on women's health on the Internet. *Journal of Women's Health*, 1997, 6(5):575–581.

125. Bazaz R, Green E, Green ST. Quality of malaria information provided on Internet travel operator websites. *Travel Medicine and Infectious Disease*, 2010, 8(5):285–291.

126. Ghoshal M, Walji MF. Quality of medication information available on retail pharmacy websites. *Research in Social and Administrative Pharmacy*, 2006, 2(4):479–498.

127. Buhi ER et al. Quality and accuracy of sexual health information web sites visited by young people. *The Journal of Adolescent Health: Official Publication of the Society for Adolescent Medicine*, 2010, 47(2):206–208.

128. Smarrito S et al. Do we need a chart of quality for websites related to cosmetic surgery? *Annales de chirurgie plastique et esthétique*, 2003, 48(4):222–227.

129. Pandolfini C, Clavenna A, Bonati M. Quality of cystic fibrosis information on Italian websites. *Informatics for Health and Social Care*, 2009, 34(1):10–17.

130. Conesa Fuentes MC, Aguinaga Ontoso E, Hernández Morante JJ. An evaluation of the quality of health web pages using a validated questionnaire. *Atención Primaria*, 2011, 43(1):33–40.

131. Guardiola-Wanden-Berghe R, Sanz-Valero J, Wanden-Berghe C. Eating disorders blogs: testing the quality of information on the Internet. *Eating Disorders*, 2010, 18(2):148–152.

132. Weitzman ER et al. Social but safe? Quality and safety of diabetes-related online social networks. *Journal of the American Medical Informatics Association* (in press).

133. Scanfeld D, Scanfeld V, Larson EL. Dissemination of health information through social networks: twitter and antibiotics. *American Journal of Infection Control*, 2010, 38(3):182–188.

134. Clauson KA et al. Scope, completeness, and accuracy of drug information in Wikipedia. *The Annals of Pharmacotherapy*, 2008, 42(12):1814–1821.

135. Mühlhauser I, Oser F. Does Wikipedia provide evidence-based health care information? A content analysis. *Zeitschrift für Evidenz, Fortbildung und Qualität im Gesundheitswesen*, 2008, 102(7):441–448.

136. Fiore F. Medications in Wikipedia. Comparison of reliability. *Perspective Infirmière: Revue Officielle de l'Ordre des Infirmières et Infirmiers du Québec*, 2009, 6(5):11.

137. Goldsmith J. How will the Internet change our health system? *Health Affairs*, 2000, 19:148–156.

138. Eysenbach G et al. Empirical studies assessing the quality of health information for consumers on the World Wide Web: a systematic review. *The Journal of the American Medical Association*, 2002, 287(20):2691–700.

139. Impicciatore P et al. Reliability of health information for the public on the World Wide Web: systematic survey of advice on managing fever in children at home. *British Medical Journal*, 1997, 314:1875–1879.

140. Jiang YL. Quality evaluation of orthodontic information on the World Wide Web. *American Journal of Orthodontics and Dentofacial Orthopedics*, 2000, 118:4–9.

141. McClung HJ, Murray HD, Heitlinger LA. The Internet as a source for current patient information. *Pediatrics*, 1998, 101:1–4.

142. Prusti M et al. The quality of online antidepressant drug information: An evaluation of English and Finnish language web sites. *Research in Social and Administrative Pharmacy: RSAP* (In press).

143. Reynolds J, Griffiths K, Christensen H. Anxiety and depression - online resources and management tools. *Australian Family Physician*, 2011, 40(6):382–386.

144. Illman J. WHO's plan to police websites rejected. *British Medical Journal*, 2000, 321(7272):1308.

145. Eysenbach G, Köhler C. How do consumers search for and appraise health information on the World-Wide-Web? Qualitative study using focus groups, usability tests and in-depth interviews. *British Medical Journal*, 2002, 324:573–577.

146. Hansen D et al. Adolescents searching for health information on the Internet: an observational study. *Journal of Medical Internet Research*, 2003, 5:e25.

147. Maloney S, Ilic D, Green S. Accessibility, nature and quality of health information on the Internet: a survey on osteoarthritis. *Rheumatology*, 2005, 44(3):382–385.

148. Eysenbach G, Köhler C. What is the prevalence of health-related searches on the World Wide Web? Qualitative and quantitative analysis of search engine queries on the Internet. *AMIA Annual Symposium Proceedings*, 2003:225–229.

149. Dickerson S et al. Patient Internet use for health information at three urban primary care clinics. *Journal of the American Medical Information Association*, 2004, 11(6):499–504.

150. Leontiadis N, Moore T, Christin N. Measuring and analyzing search-redirect attacks in the illicit online prescription drug trade. In: Proceedings of the 20th USENIX Security Symposium. 2011 (https://db.usenix.org/events/sec11/tech/full_papers/Leontiadis.pdf, accessed 10 October 2011).

151. Greenberg L, D'Andrea G, Lorence D. Setting the public agenda for online health search: a white paper and action agenda. *Journal of Medical Internet Research*, 2004, 6(2):e18.

152. Jansen BJ, Spink A. How are we searching the World Wide Web? A comparison of nine search engine transaction logs. *Information Processing & Management*, 2006, 42(1):248–263.

153. Buhi ER et al. An observational study of how young people search for online sexual health information. *Journal of American College Health*, 2009, 58(2):101–111.

154. Oulasvirta A, Hukkinen JP, Schwartz B. When more is less: the paradox of choice in search engine use. SIGIR '09. In: Proceedings of the 32nd international ACM SIGIR conference on research and development in information retrieval. The 32nd international ACM SIGIR conference on research and development in information retrieval, Boston, 2009:516–523.

155. Lissman TL, Boehnlein JK. A critical review of Internet information about depression. *Psychiatric Services*, 2001, 52(8):1046–1050.

156. Kaimal AJ et al. Google obstetrics: who is educating our patients? *American Journal Obstetrics & Gynecology*, 2008, 198(6):682.e1–5.

157. Walji M et al. Searching for cancer-related information online: unintended retrieval of complementary and alternative medicine information. *International Journal of Medical Informatics*, 2005, 74(7–8):685–693.

158. Law MR, Mintzes B, Morgan SG. The sources and popularity of online drug information: an analysis of top search engine results and web page views. *The Annals of Pharmacotherapy*, 2011, 45(3):350–356.

159. Heilman JM et al. Wikipedia: a key tool for global public health promotion. *Journal of Medical Internet Research*, 2011, 13(1):e14.

160. Laurent MR, Vickers TJ. Seeking health information online: does Wikipedia matter? *Journal of the American Medical Informatics Association*, 2009, 16(4):471–479.

161. Rose S, Bruce J, Maffulli N. Accessing the Internet for patient information about orthopedics. *Journal of the American Medical Association*, 1998, 280:1309–1310.

162. Lau AY, Coiera EW. Impact of web searching and social feedback on consumer decision making: a prospective online experiment. *Journal of Medical Internet Research*, 2008, 10(1):e2.

163. Lau AY, Coiera EW. Do people experience cognitive biases while searching for information? *Journal of the American Medical Informatics Association*, 2007, 14(5):599–608.

164. Lau AY, Coiera EW. Can cognitive biases during consumer health information searches be reduced to improve decision making? *Journal of the American Medical Informatics Association*, 2009, 16(1):54–65.

165. Ilic D et al. Specialized medical search engines are no better than general engines in sourcing consumer information about androgen deficiency. *Human Reproduction*, 2003, 18:557–561.

166. Ilic D, Risbridger G, Green S. Searching the Internet for information on prostate cancer screening: an assessment of quality. *Urology*, 2004, 64:112–116.

167. Coberly E et al. Linking clinic patients to Internet-based, condition-specific information prescriptions. *Journal of the Medical Library Association*, 2010, 98(2):160–164.

168. D'Alessandro DM et al. A randomized controlled trial of an information prescription for pediatric patient education on the Internet. *Archives of Pediatrics & Adolescent Medicine*, 2004, 158(9):857–862.

169. Ritterband LM et al. Using the Internet to provide information prescriptions. *Pediatrics*, 2005, 116(5):e643–e647.

170. Industry Canada. Working Group on Anti-Spam Technology and Network Management. http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00292.html#TechnologyWG, accessed 29 October 2011.

171. Industry Canada. *An anti-spam action plan for Canada*. http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/h_gv00246.html, accessed 29 October 2011.

172. Parliament of Canada. House of Commons. *Bill C-28*. Third Session. Fortieth Parliament, 59 Elizabeth II, 2010 (http://www.parl.gc.ca/HousePublications/Publication.aspx?Docid=4547728&file=4, accessed 25 October 2011).

173. Leduc A. *Canada's anti-spam legislation*. 2011 (http://www.colloque-rsi.com/files/2011/presentations/A-Leduc.pdf, accessed 29 October 2011).

174. United States of America. 108th Congress. Public Law 108-177. *Controlling the Assault of Non-Solicited Pornography and Marketing*. 15 USC 7701. 117 STAT2699. December 16, 2003 (http://uscode.house.gov/download/pls/15C103.txt, accessed 25 October 2011).

175. Craddock D. Inside Windows Live: fighting the war on spam. Blog post from 12 January 2010 (http://windowsteamblog.com/windows_live/b/windowslive/archive/2010/01/12/fighting-the-war-on-spam.aspx, accessed 25 October 2011).

176. Clauson KA, Seamon MJ, Fox BI. Pharmacists' duty to warn in the age of social media. *American Journal of Health-System Pharmacy*, 2010, 67(15):1290–1293.

177. Hughes B, Joshi I, Wareham J. Health 2.0 and Medicine 2.0: tensions and controversies in the field. *Journal of Medical Internet Research*, 2008, 10(3):e23

178. Mesko B, personal communication, 2011.

179. *mHealth: new horizons for health through mobile technologies*. Geneva, World Health Organization, 2011

Appendix 1. Methodology of the second global survey on eHealth

Purpose

The World Health Organization's eHealth resolution WHA 58.28 was adopted in 2005 and focused on strengthening health systems in countries through the use of eHealth (1); building public-private partnerships in ICT development and deployment for health; supporting capacity building for the application of eHealth in Member States; and the development and adoption of standards. Success in these areas is predicated on a fifth strategic direction: monitoring, documenting and analysing trends and developments in eHealth and publishing the results to promote better understanding. In direct response to the eHealth resolution, the Global Observatory for eHealth (GOe) was established to monitor and analyse the evolution of eHealth in countries and to support national planning through the provision of strategic information.

The GOe's first objective was to undertake a global survey on eHealth to determine a series of benchmarks at national, regional and global levels in the adoption of the necessary foundation actions to support the growth of eHealth. The aim was to provide governments with data that could be used as benchmarks for their own development as well as a way to compare their own progress with that of other Member States. The survey is part of the mandate defined during the GOe's inception – to provide Member States with reliable information and guidance on best practices, policies and standards in eHealth.

The second global survey on eHealth was conducted in late 2009 and was designed to build upon the knowledge base generated by the first survey. While the first survey conducted in 2005 was more general and primarily asked high-level questions at the national level, the 2009 survey was thematically designed and presented more detailed questions. The thematic design of the survey has provided the GOe with a rich source of data that is being used to create a series of eight publications – The Global Observatory for eHealth Series – due for publication during 2010 and 2011.

Each publication in the series is primarily targeted to ministries of health, ministries of information technology, ministries of telecommunications, academics, researchers, eHealth professionals, nongovernmental organizations involved in eHealth, donors, and private sector partners.

Survey implementation

Based on the experience of the first global survey, the GOe benefited from many of the lessons learned in creating the second survey, disseminating the instrument in digital format, working with WHO regional offices and Member States to encourage survey completion, as well as processing the data and analysing the results.

Survey instrument

The instrument focused on issues relating to processes and outcomes in key eHealth areas. Objectives for the survey were to identify and analyse trends in the:

- Uptake of eHealth foundation policies and strategies, building on the 2005 results
- Deployment of mHealth initiatives in countries
- Application of telemedicine solutions
- Adoption of eLearning for health professionals and students
- Collection, processing and transfer of patient information
- Development of legal and ethical frameworks for patient information in digital format
- Action concerning online child safety, Internet pharmacies, health information on the Internet, and spam
- Governance and organization of eHealth in countries.

Table A1 shows the seven themes of the survey.

Theme	Action
mHealth	Identify the diverse ways mobile devices are being used for health around the world and the effectiveness of these approaches. Highlight the most important obstacles to implementing mHealth solutions. Consider whether mHealth can overcome the digital divide.
Telemedicine	Identify and review the most frequently used telemedicine approaches across the globe as well as emerging and innovative solutions. Propose necessary actions to be taken to encourage the global growth and acceptance of telemedicine, and particularly in developing countries.
Management of patient information	Describe the issues relating to the management of patient information at three levels – local health care facility, regional/ district, national levels. Analyse the trends in transition from paper to digital records. Identify actions to be taken in countries to increase the uptake of digital patient records.
Legal and ethical frameworks for eHealth	Review the trends in the introduction of legislation to protect personally identifiable data and health-related data in digital format as well as the right to access and control one's own record. Identify and analyse the control of online pharmacies by Member States. Review government action to provide for child safety on the Internet.
eHealth policies – a systematic review	Identify the uptake of eHealth policies across the globe and analyse by WHO region as well as World Bank income groups to establish possible trends. Systematically review the content and structure of existing strategies highlighting strengths and weaknesses. Propose model approaches for the development of eHealth policies including scope and content.
eHealth foundation actions	Review trends in the uptake of foundation actions to support eHealth at the national level including: eGovernment, eHealth, ICT procurement, funding approaches, capacity building for eHealth, and multilingual communications.
eLearning	Analyse the extent of use and effectiveness of eLearning for the health sciences for students and health professionals.
eHealth country profiles	Presentation of all participating Member States eHealth data aggregated by country to act as ready reference of the state of eHealth development according to selected indicators.

Table A1. Survey themes

Survey development

The survey instrument was developed by the GOe with broad consultation and input from eHealth. Planning for the 2009 global survey started in 2008 with the review of the 2005/2006 survey results, instrument and feedback from participating countries. One of the constraints identified in the first survey was on the management of data and its availability for compilation and analysis. In order to facilitate data collection and management, Data Collector (DataCol)[12] was used to make the survey instrument available online and therefore streamlining the collection and processing of data.

A set of questions was developed and circulated in the first quarter of 2009 for comments to selected partners in all regions through virtual teleconferences. The range of partners included those from government, WHO regional and country offices, collaborating centres and professional associations. Over 50 experts worldwide were involved in the process. Collaborative efforts extended to other WHO programmes as well as international organizations, such as the International Telecommunications Union (ITU) and Organisation for Economic Co-Operation and Development (OECD). An online forum to discuss the survey instrument and survey process was developed and hosted by the Institute for Triple Helix Innovation based at the University of Hawaii at Manoa in the United States of America.[13]

A draft questionnaire was developed and posted online for review by the partners and was pilot tested in March 2009 in five countries: Canada, Lebanon, Norway, Philippines, and Thailand. The final version of the survey instrument was enhanced based on the comments and observations received from the pilot testing. In order encourage countries to respond, the survey questions, instructions and data entry procedures were translated into all WHO official languages plus Portuguese.

Data Collector

Data Collector, DataCol, is a web-based tool that simplifies online form creation for data collection and management and is designed, developed and supported by WHO. The collected data are stored in a SQL database maintained by WHO database administrators, and can be exported as a Microsoft Excel file for further analysis using other statistical software.

This is the first time that DataCol has been used as the primary method of implementing an online survey of over 40 pages of text and questions. Significant preparation and testing was required to ensure that the system was robust and able to accommodate the data entry process from around the world, as well as the volume of data entered and stored online.

The various language versions of the survey instrument and supporting documentation were entered into DataCol by language. In addition, individual country login names and passwords were assigned to ensure that only one entry was submitted per country rather than multiple entries. Country coordinators were responsible for completing the forms after obtaining agreement from the expert informant group.

12 Web-based tool for online creation of forms in surveys developed by WHO.
13 http://www.triplehelixinstitute.org/.

Preparation to launch the survey

One of the most important tasks in executing an international survey is to build a network of partners at the regional level who can liaise directly with countries.

Due to differing priorities across WHO regions, not all regional offices have staff whose responsibilities included eHealth activities. For this reason many regional offices had to assign staff to assist in coordinating the survey process with countries in their respective region. Instructions for the survey procedures were circulated and were followed by a series of teleconferences.

One significant outcome during the survey implementation was the development of strong and productive working relationships with regional counterparts, without whom it would not have been possible to successfully undertake such a task. The success of the survey implementation can also be attributed to the assistance of regional and national office colleagues who worked directly with national counterparts in completing the questionnaire.

Figure A1. GOe survey and report process

Survey

The survey was launched on 15 June 2009, and due to the high level of interest, did not close until 15 December 2009. Regional focal points worked to encourage Member States to participate. In some cases this was easy; in others it required extensive discussions, not all of which were successful in achieving participation. Conducting a global survey is like conducting a campaign: the purpose and rewards of participation have to be conveyed to national coordinators and then to survey expert informants. It is important to build momentum and to maintain enthusiasm.

At the national level, coordinators managed the task. Their responsibilities included finding experts in all of the areas addressed by the survey, and organizing and hosting a full-day meeting where the survey could be collectively completed by the entire group. The number of expert informants, per country, ranged from 5 to 15. The survey process helps build the GOe network of informants around the globe and now consists of over 800 eHealth experts.

Limitations

Member States were limited to one response per country; thus, the expert informants were required to come up with a single response for each question that was most representative of the country as a whole. Coming to a consensus could be difficult in cases where the situation varies widely within the country, or where there were significant differences in opinion. The survey does not attempt to measure localized eHealth activity at the subnational level.

The survey responses were based on self-reporting by the expert informant group for each participating Member State. Although survey administrators were given detailed instructions to maintain consistency, there was significant variation across Member States in the quality and level of detail in the responses, particularly to for the descriptive, open-ended questions. While survey responses were checked for consistency and accuracy, it was not possible to verify the responses for every question.

The scope of the survey was broad, and survey questions covered diverse areas of eHealth – from policy issues and legal frameworks to specific types of eHealth initiatives being conducted in-country. Every effort was made to select the best national experts to complete the instrument; however, it is not possible to determine whether the focus groups had the collective eHealth knowledge to answer each question. While the survey was circulated with a set of detailed instructions and terminological definitions, there is no guarantee that these were used when responding.

Data processing

On receipt of the completed questionnaires, all non-English responses were translated into English. Survey responses were checked for consistency and other errors, and countries were contacted for follow-up to ensure accurate reporting of results. Data were exported from DataCol in Microsoft Excel format and the data analysis was performed using R statistical programming language.[14]

Data were analysed by thematic section. For closed-ended questions, percentages were computed for each possible response to obtain the global level results. In addition, the data were aggregated and analysed by WHO region and World Bank income group to see trends by region and by income level. Preliminary analysis based on aggregation by ICT Development Index showed similar results as for World Bank income group (2). This is due to the high correlation between ICT Development Index and GDP per capita (Spearman ρ=0.93, p=10-16). Therefore, these results were not included in this report. Cross-question analysis was performed where two or more questions were thought to be related, and the results were probed in greater depth as warranted. External health and technology indicators, such as mobile phone penetration, were introduced into the analysis for comparison purposes where relevant.

Results from the current survey were compared to those from the previous survey wherever possible; however, as the subject matter covered by the 2009 survey was considerably broader, and the survey questions were worded somewhat differently, there was little scope for this sort of analysis. In addition, the percentages were often not directly comparable, particularly at the regional level, as the sets of responding countries were different, and the expert informants in each iteration of the survey were also different.

Table A2 shows the advantages and disadvantages of the groupings used in the survey.

Country grouping	Advantages	Disadvantages
WHO region	WHO regional approach integrated into WHO strategic analysis and planning, and operational action.	Limited country commonality from an economic, health care, or ethnic perspective. Less useful for other agencies or institutions wishing to interpret or act on GOe data.
World Bank income group	Clear economic definition based on GNI per capita. Consistent application of criteria across all countries. Simple four-level scale.	Does not account for income disparity, ongoing armed conflicts, health of the population, or population age.

Table A2. Advantages and disadvantages of the country groupings

14 See for more information http://www.r-project.org/.

Response rate

The "Internet safety and security" section of the survey, which this publication is based on, was completed by a total of 114 countries (59% of all WHO Member States). Figure A2 shows the responding Member States for this module of the survey. Tables A3 and A4 show the distribution of the responding countries by WHO region and World Bank income group.

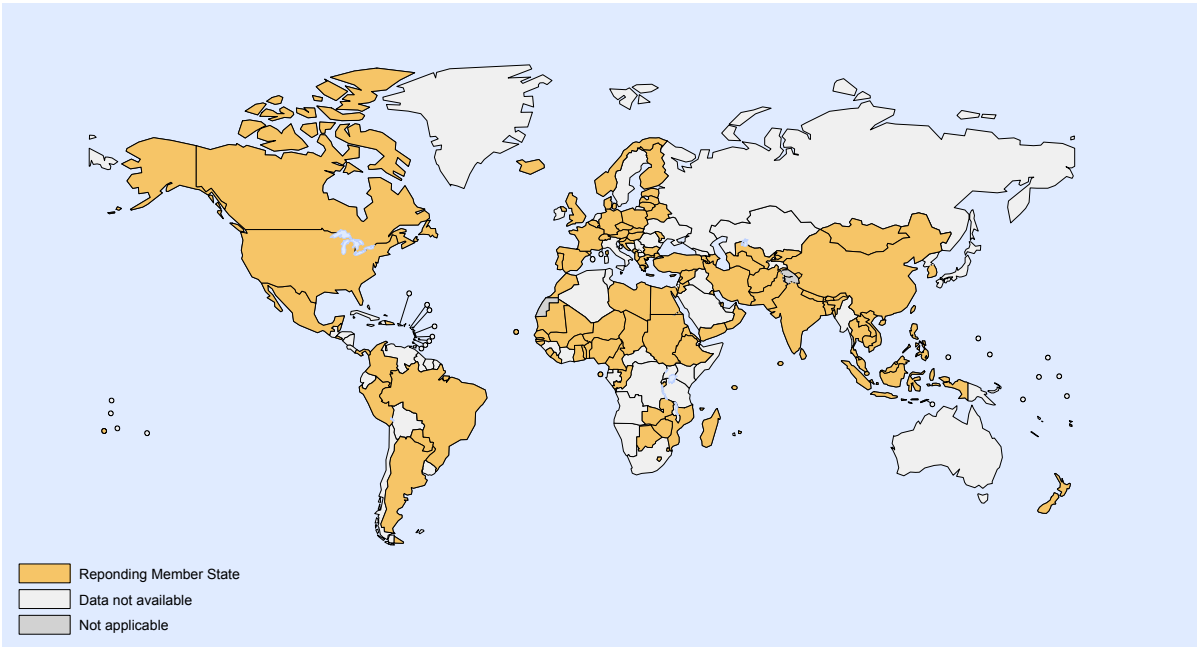


Figure A2. Responding Member States

Response rate by WHO region

Administratively WHO is made up of six geographical regions, which are quite heterogeneous: Member States differ with respect to size, economy, and health care challenges. Nevertheless, it is still important to present high-level eHealth analyses at the regional level as this reflects the organizational structure and operational framework of WHO.

A breakdown by WHO regional responses is presented in Table A3. It shows considerable variation ranging from 34% for the Americas to 73% for the South-East Asia Region. Numerous Member States, particularly those in the Region of the Americas, indicated that they would not be able to participate in the 2009 survey due to resources being diverted to prepare and respond to the H1N1 pandemic or due to other urgent public health issues such as conflict situations. The Western-Pacific Region has many small island Member States of which only a few responded to the survey, yielding a response rate of 48% for the region. The response rates for the Eastern Mediterranean, African and European Regions were over 60%. This was particularly encouraging for regions consisting of a large number of Member States such as the African and European Regions. Results from regions with low response rates should be interpreted with care as they may not be representative of the entire region.

	WHO region					
	African	Americas	South-East Asia	European	Eastern Mediterranean	Western Pacific
Total number of countries	46	35	11	53	21	27
No. of responding countries	29	12	8	36	14	13
Response rate	63%	34%	73%	68%	67%	48%

Table A3. Response rate by WHO region

For the South-East Asia Region, although the number of responding countries was the lowest, the response rate was the highest since the region consists of a total of 11 Member States. Self-selection of the sample often occurs in surveys of this nature, where responding countries are more likely to have a high level of interest and/or activity in eHealth. Table A4 shows that response rates in low and lower-middle income brackets were high. Past surveys have shown that countries in these groups generally have less eHealth activity in comparison to high and upper middle-income brackets. Thus, in some cases, Member States participating in the survey may reflect a commitment to moving forward with eHealth.

Response rate by World Bank income group

The World Bank classifies all economies with a population greater than 30 000 into four income groups based on gross national income (GNI) per capita.[15] The classification is as follows: low income (US$ 975 or less), lower-middle income (US$ 976–3,855), upper-middle income (US$ 3856–11 905), and high income (US$ 11 906 or more). These income groups are a convenient and practical basis for analysis, enabling a review of trends in the survey results based on income level. Classification by income does not correspond exactly to level of development; however, low and middle-income countries are sometimes referred to as 'developing' economies and high-income countries as 'developed', for convenience.

Table A4 shows the survey response rate by World Bank income group. Low-income countries had the highest response rate (70%), closely followed by high-income countries (63%). In terms of raw numbers, the distribution of responding countries was remarkably even, with 30 to 31 countries responding from the high-income, lower-middle income, and low-income groups, and a slightly lower number of countries from the upper-middle income group.

	World Bank income group			
	High income	Upper-middle income	Lower-middle income	Low income
Total no. Countries	49	44	53	43
No. of responding countries	31	21	30	30
Response rate	63%	48%	57%	70%

Table A4. Response rate by World Bank income group

References

1. Resolution WHA 58.28. eHealth. In: Fifty-eighth World Health Assembly, Geneva, [insert dates of meeting]. Geneva, World Health Organization, 2005 (http://apps.who.int/gb/ebwha/pdf_files/WHA58/WHA58_28-en.pdf, accessed 18 May 2011).
2. Measuring the information society – the ICT Development Index. Geneva, International Telecommunications Union, 2009 (http://www.itu.int/ITU-D/ict/publications/idi/2009/index.html, accessed 17 May 2011).

15 http://data.worldbank.org/about/country-classifications

Safety and security on the Internet

Challenges and advances in Member States

Based on the findings of the second global survey on eHealth

Global Observatory for eHealth series - Volume 4

ISBN 978 92 4 156439 7