Protection of Patient’s Privacy and Data Security in E-Health Services

Yi Hong¹, ², Timothy B. Patrick², Rick Gillis¹
¹Medical College of Wisconsin and ²University of Wisconsin – Milwaukee
Milwaukee, WI

yhong@mcw.edu, tp5@uwm.edu, rgillis@mcw.edu

Abstract

E-Health involves new forms of patient-physician interaction and poses new ethical challenges and threats to patient privacy. This paper reviews Health On the Net Foundation Code of Conduct (HONcode) accredited e-Health websites that provide online appointment services in the U.S.A for compliance with basic principles of security and privacy. We found that 20 of 30 HON sites we reviewed are secure sites but only 8 of 20 secure sites state that it is secure. Most HON sites require patients to submit confidential data. 12 of 30 websites do not display privacy notice on the web appointment request page. The reading level might be a problem for the patients who have lower educational background to understand the privacy notice. Regulations and guidelines do not ensure that privacy protection and data security is done appropriately or well. More attention to security methods and procedures is needed to safeguard patients’ privacy rights.

1. Introduction

E-Health involves new forms of patient-physician interaction and poses new ethical challenges and threats to patient privacy. This paper reviews Health On the Net Foundation Code of Conduct (HONcode) accredited e-Health websites that provide online appointment services in the U.S.A for compliance with basic principles of security and privacy. We found that 20 of 30 HON sites we reviewed are secure sites but only 8 of 20 secure sites state that it is secure. Most HON sites require patients to submit confidential data. 12 of 30 websites do not display privacy notice on the web appointment request page. The reading level might be a problem for the patients who have lower educational background to understand the privacy notice. Regulations and guidelines do not ensure that privacy protection and data security is done appropriately or well. More attention to security methods and procedures is needed to safeguard patients’ privacy rights.

1. Introduction

E-Health involves new forms of patient-physician interaction and poses new ethical challenges and threats to patient privacy. This paper reviews Health On the Net Foundation Code of Conduct (HONcode) accredited e-Health websites that provide online appointment services in the U.S.A for compliance with basic principles of security and privacy. We found that 20 of 30 HON sites we reviewed are secure sites but only 8 of 20 secure sites state that it is secure. Most HON sites require patients to submit confidential data. 12 of 30 websites do not display privacy notice on the web appointment request page. The reading level might be a problem for the patients who have lower educational background to understand the privacy notice. Regulations and guidelines do not ensure that privacy protection and data security is done appropriately or well. More attention to security methods and procedures is needed to safeguard patients’ privacy rights.

1. Introduction

E-Health involves new forms of patient-physician interaction and poses new ethical challenges and threats to patient privacy. This paper reviews Health On the Net Foundation Code of Conduct (HONcode) accredited e-Health websites that provide online appointment services in the U.S.A for compliance with basic principles of security and privacy. We found that 20 of 30 HON sites we reviewed are secure sites but only 8 of 20 secure sites state that it is secure. Most HON sites require patients to submit confidential data. 12 of 30 websites do not display privacy notice on the web appointment request page. The reading level might be a problem for the patients who have lower educational background to understand the privacy notice. Regulations and guidelines do not ensure that privacy protection and data security is done appropriately or well. More attention to security methods and procedures is needed to safeguard patients’ privacy rights. E-Health can provide healthcare consumers with opportunities to interact with their healthcare systems online and can provide new forms of patient-physician interaction.

Various services may be provided by an e-Health site. It may provide healthcare consumers access to internet-based tools to monitor their health records, view test results, refill prescriptions, schedule appointments, communicate electronically with their personal care physician, and get online reference services from health librarians to help answer their questions. Online appointment services in particular are the most common e-Health services.

Healthcare consumers have the right to expect that their personal data will be kept confidential. Since online appointment services are the most common e-Health services, this study reviews HONcode accredited websites that provide online appointment services for compliance with basic principles of security and privacy.

2. Background: the need for Consumer Protections

Despite its advantages for healthcare consumers, E-Health involves new forms of patient-physician interaction and poses new ethical challenges and threats to patient privacy. This paper reviews Health On the Net Foundation Code of Conduct (HONcode) accredited e-Health websites that provide online appointment services in the U.S.A for compliance with basic principles of privacy and data security. We found that 20 of 30 HON sites we reviewed are secure sites but only 8 of 20 secure sites state that it is secure. Most HON sites require patients to submit confidential data. 12 of 30 websites do not display privacy notice on the web appointment request page. The reading level might be a problem for the patients who have lower educational background to understand the privacy notice. Regulations and guidelines do not ensure that privacy protection and data security is done appropriately or well. More attention to security methods and procedures is needed to safeguard patients’ privacy rights.

E-Health Code of Ethics.

To protect consumers’ privacy and personal data, the e-Health Code of Ethics requires e-Health websites to clearly disclose potential user privacy risks and clearly indicate what data are being collected when users visit the site, who is collecting the data, how the data will be used, and whether the site will share data (with whom and for what purpose).

HIPAA.

While the e-Health Code of Ethics requires e-Health sites to adopt reasonable mechanisms to provide online appointment services for compliance with basic principles of security and privacy.
security of patients’ personal data, HIPAA regulations aim to inform and educate patients about their privacy rights and establish standards for the privacy and security of health information.

The HIPAA Privacy Rule protects all “individually identifiable health information” in any form or media. This information is called “protected health information (PHI)”, and includes many common identifiers (e.g. name, address, birth date, Social Security Number (SSN)).

The Privacy Rule requires covered entities to provide patients with a Notice of Privacy Practices. The Notice must describe the ways in which the covered entity may use and disclose protected health information.

According to HIPAA, a covered entity must maintain reasonable and appropriate administrative, physical and technical safeguards to prevent intentional or unintentional use or disclosure of PHI in violation of the Privacy Rule. [4]

The HONcode. The Health On the Net Foundation (HON) is another effort to protect consumers. HON was founded in 1995 to promote “…the effective and reliable use of the new technologies for telemedicine in healthcare around the world.” The HONcode was developed …to help standardize the reliability of medical and health information available on the World-Wide Web. [5]

Currently there are more than 120,000 health-related websites that are HONcode accredited. [6] The HONcode principle regarding privacy and confidentiality states that

Your site must describe how you treat confidential, private or semi-private information such as email addresses and the content of emails received from or sent to your visitors. You must inform your visitors whether their data will be recorded in your own database, who can access this database (others, only you, nobody), if this information is used for your own statistics (anonymous or not), or if these statistics are used by third party or other companies.

A statement or a privacy policy page regarding confidentiality of data must be clearly displayed. [7]

3. Methods

We searched for HONcode accredited sites using the HON search engine [8] with the query “web appointment request” on November 16 2007. The search retrieved 170 HONcode accredited sites. We reviewed the 30 USA websites that actually provided online appointment services. The 30 sites are listed in Table 1.

We reviewed each of the 30 sites to determine:
(1) Is it a secure site?
(2) Does it include a statement regarding its status as a secure site?
(3) Does it request confidential data elements from the user making an appointment?
(4) Does it include a privacy notice or statement of privacy policy?
(5) What is the reading level of the privacy notice or statement of privacy policy?

We considered a site to be secure if it used HTTPS, which is a “…combination of a normal HTTP interaction over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) transport mechanism.” [9]

We used the SMOG Calculator [10] to assess the educational level needed to fully understand the text of the privacy notice or statement of privacy policy. We coded SMOG grade <12 (high school level) as low level (l), SMOG grade 12-16 (college level) as medium level (m), SMOG grade >16 (university degree) as high level (h).

4. Results

Table 1 shows the results of the review.

4.1. Is it a secure site?

Among the 30 HON sites, 20 sites are secure sites, 10 are not.

4.2. Does it include a statement regarding its status as a secure site?

Among the 20 secure sites, only 9 of them state that they are secure.

4.3. Does it request confidential data elements from the user making an appointment?

Most of the HON sites require patients to submit confidential data such as Social Security Number,
date of birth, medical record number, medical information, insurance information, etc. Almost all of them require patients to provide birth date information.

Table 1 Review of the HONcode accredited websites for compliance with basic principles of security and privacy

<table>
<thead>
<tr>
<th>Online Appointment Site</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://epatient.muhealth.org/UMCWeb/idxpol/pslogin.asp">https://epatient.muhealth.org/UMCWeb/idxpol/pslogin.asp</a> (Click “Visit as a Guest” to access to the secure Web appointment access form)</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td><a href="https://forms.mayoforms.org/forms/up/mc408606.cfm">https://forms.mayoforms.org/forms/up/mc408606.cfm</a> (Access to the secure site through: <a href="http://www.mayoclinic.org/patientinfo/appointments.html">http://www.mayoclinic.org/patientinfo/appointments.html</a>)</td>
<td>y y n y m</td>
</tr>
<tr>
<td><a href="https://secure.childrensmemorial.org/kids_doc/apptForm.asp">https://secure.childrensmemorial.org/kids_doc/apptForm.asp</a></td>
<td>y n y y h</td>
</tr>
<tr>
<td><a href="https://secure.mcw.edu/appt_form.htm">https://secure.mcw.edu/appt_form.htm</a></td>
<td>y y y y l</td>
</tr>
<tr>
<td><a href="https://secure01.cqservices.com/guthrie/FindAPhysician/Physicians/Default.asp?mode=new">https://secure01.cqservices.com/guthrie/FindAPhysician/Physicians/Default.asp?mode=new</a></td>
<td>y n y y h</td>
</tr>
<tr>
<td><a href="https://transact.med.yale.edu/ynhhphysiciandata/apptrequestform.asp?inst=ynhh">https://transact.med.yale.edu/ynhhphysiciandata/apptrequestform.asp?inst=ynhh</a></td>
<td>y n y y m</td>
</tr>
<tr>
<td><a href="https://www.brighamandwomens.org/forms/RequestAppointment.aspx">https://www.brighamandwomens.org/forms/RequestAppointment.aspx</a></td>
<td>y y y y m</td>
</tr>
<tr>
<td><a href="https://www.clevelandclinic.org/myappointment/form.asp">https://www.clevelandclinic.org/myappointment/form.asp</a></td>
<td>y n y n na</td>
</tr>
<tr>
<td><a href="https://www.dfci.harvard.edu/pat/becoming/request/Default.asp">https://www.dfci.harvard.edu/pat/becoming/request/Default.asp</a></td>
<td>y n y y m</td>
</tr>
<tr>
<td><a href="https://www.forsberg.com/sparrowsecure/preregister1.asp">https://www.forsberg.com/sparrowsecure/preregister1.asp</a></td>
<td>y n y n na</td>
</tr>
<tr>
<td><a href="https://www.geisinger.org/patients/appts/appt_form.html">https://www.geisinger.org/patients/appts/appt_form.html</a></td>
<td>y y y y m</td>
</tr>
<tr>
<td><a href="https://www.jeffersonhospital.org/cgi-bin/jeffnowappt/apptfrmloc.cgi?tjuh++++0">https://www.jeffersonhospital.org/cgi-bin/jeffnowappt/apptfrmloc.cgi?tjuh++++0</a></td>
<td>y n y n na</td>
</tr>
<tr>
<td><a href="https://www.marshfieldclinic.org/patients/pages/default.aspx?page=apptrequest">https://www.marshfieldclinic.org/patients/pages/default.aspx?page=apptrequest</a></td>
<td>y n y y m</td>
</tr>
<tr>
<td><a href="https://www.meei.harvard.edu/db/appoint.php">https://www.meei.harvard.edu/db/appoint.php</a></td>
<td>y n y y m</td>
</tr>
<tr>
<td><a href="https://www.munchealth.com/patients_visitors/eservices/request_appointment/request_appointment.htm">https://www.munchealth.com/patients_visitors/eservices/request_appointment/request_appointment.htm</a></td>
<td>y y y y m</td>
</tr>
<tr>
<td><a href="https://www.secure01.cqservices.com/guthrie/FindAPhysician/Physicians/Default.asp?mode=new">https://www.secure01.cqservices.com/guthrie/FindAPhysician/Physicians/Default.asp?mode=new</a></td>
<td>y n y y h</td>
</tr>
<tr>
<td><a href="https://www.utphysicians.org/Appointment/forms/default.htm">https://www.utphysicians.org/Appointment/forms/default.htm</a></td>
<td>y y y n na</td>
</tr>
<tr>
<td><a href="https://www.ucsfhealth.org/adult/patient_guide/request_primary_care.html">https://www.ucsfhealth.org/adult/patient_guide/request_primary_care.html</a></td>
<td>y y y n na</td>
</tr>
<tr>
<td><a href="http://www.mnhphysicians.photobooks.com/Appointment.asp?disclaimer=Continue">http://www.mnhphysicians.photobooks.com/Appointment.asp?disclaimer=Continue</a></td>
<td>n na y y h</td>
</tr>
<tr>
<td><a href="http://www.dentalgentlecare.com/make_appointment.htm">http://www.dentalgentlecare.com/make_appointment.htm</a></td>
<td>n na n n na</td>
</tr>
<tr>
<td><a href="http://www.dedepediatrics.com/appointment.php">http://www.dedepediatrics.com/appointment.php</a></td>
<td>n na n n na</td>
</tr>
<tr>
<td><a href="http://www.englewoodortho.com/new_pt_form.htm">http://www.englewoodortho.com/new_pt_form.htm</a></td>
<td>n na n n na</td>
</tr>
<tr>
<td><a href="http://www.evped.com/onlineappt.htm">http://www.evped.com/onlineappt.htm</a></td>
<td>n na y y m</td>
</tr>
<tr>
<td><a href="http://www.healthgrades.com/consumer/index.cfm?fuseaction=mod&amp;modtype=prc&amp;module=appointment&amp;hgid=HGPY01C99FF3875647053&amp;type=emailphone&amp;tv=Report_EmailLink&amp;TVID=BTN_Apt">http://www.healthgrades.com/consumer/index.cfm?fuseaction=mod&amp;modtype=prc&amp;module=appointment&amp;hgid=HGPY01C99FF3875647053&amp;type=emailphone&amp;tv=Report_EmailLink&amp;TVID=BTN_Apt</a></td>
<td>n na y n na</td>
</tr>
<tr>
<td><a href="http://www.jhintl.net/forpatients/page.aspx?id=2338">http://www.jhintl.net/forpatients/page.aspx?id=2338</a></td>
<td>n na n n na</td>
</tr>
<tr>
<td><a href="http://www.mscenerg.org/content/category/1/1/15/">http://www.mscenerg.org/content/category/1/1/15/</a></td>
<td>n na y y h</td>
</tr>
<tr>
<td><a href="http://www.ssdental.com/appointments/appointments_dw.asp">http://www.ssdental.com/appointments/appointments_dw.asp</a></td>
<td>n na n n na</td>
</tr>
<tr>
<td><a href="http://www.vasectomy.com/Appointment.asp?DoctorId=1967">http://www.vasectomy.com/Appointment.asp?DoctorId=1967</a></td>
<td>n na n n na</td>
</tr>
</tbody>
</table>

Legend
n = no; y = yes; na = not applicable; l = low; m = medium; h = high

Criteria:
1: Is it a secure site?
2: Does it include a statement regarding its status as a secure site?
3: Does it request confidential data elements from the user making an appointment?
4: Does it include a privacy notice or statement of privacy policy?
5: What is the reading level of the privacy notice or statement of privacy policy? (SMOG grade)
6 of them require Social Security Number along with birthday. The secure sites require more confidential data than non-secure sites.

4.4. Does it include a privacy notice or statement of privacy policy?

12 of 30 websites do not display a privacy notice or statement of privacy policy, or a link to such a statement, on the web appointment request page.

4.5. What is the reading level of the privacy notice or statement of privacy policy?

Among 18 websites that have a privacy notice or statement of privacy policy on their appointment page, 13 of them have a medium or college reading level, 4 of them have a high reading level, and only one has a low reading level.

5. Discussion

There is an obvious need for secure websites to ensure visitors’ privacy and prevent personal health information. A considerable challenge arises from trying to balance the desire to make information freely available to users of the Internet, while at the same time protecting people’s privacy and confidentiality. [11]

People who use the Internet for health-related reasons have the right to expect that personal data they provide will be kept confidential and also have the right to be informed that personal data may be gathered, and to choose whether they will allow their personal data to be collected and whether they will allow it to be used or shared.

However, Non-medical professionals involved in providing online medical services may be unaware of the unique standards they must adhere to when dealing with online healthcare consumers and may need to be educated about the obligation not to exploit patients or clients and to respect issues of privacy and confidentiality. [12] Few healthcare consumers have any idea what is done with their personal data and health information on the Internet. Even though a health website claims it respects patients’ privacy and takes steps to protect patients’ personal data, a patients’ data may not be safe during the transaction process. The study of HONcode accredited medical and health websites reveals the gap between ideal and reality. In our sample, one third of the HONcode accredited sites that provide online appointment services are not secure.

Including a privacy notice or statement of privacy policy on a site is very important. Even though a site adopts security procedures and displays a privacy policy, users might still not trust it or may be misled unless there is a brief and understandable statement of security and privacy displayed on the site. In our study, we regarded the websites that have “https” within their URLs as secure sites since information exchanged with any address beginning with https is encrypted using Secure Sockets Layer (SSL) before transmission. However, very few lay users realize the difference between “http” and “https”. It is thus necessary to show that the website is secure by either displaying a secured seal or a brief statement. This is especially important for the users with lower educational background, particularly when the site requires users to submit confidential data such as SSN, date of birth, medical record number, medical information, or insurance information.

6. Conclusion

Security, privacy, and confidentiality are major concerns in e-Health services. HIPAA regulations, e-Health Code of Ethics, HON principles, and other guidelines do not ensure that privacy protection and data security are done appropriately or well. There is a gap between ideal and reality. More attention to the spirit of existing measures and procedures is needed to safeguard patients’ privacy rights.

To deal with the challenges to manage and ensure individual privacy, the following steps should be taken to maintain the e-Health site visitor’s rights to privacy and the confidentiality of personal information:

6.1. Ensure personal data security with user ID and password or using SSL Certificate Encryption and display the Secured Seal to let the user know that his or her transactions are secure.

6.2. Provide a statement or a link to the privacy policy of the e-Health site on the home page or the site navigational bar that is easily accessible and understandable to the user.

6.3. Do not collect name, birthday, phone number, e-mail address, or any other personal information unless voluntarily provided by the visitor after the visitor is informed about the potential use of such information.

6.4. Do not collect SSN, personal medical information (medical conditions, health-seeking
behaviors and questions, and use of or requests for information about drugs, therapies, or medical devices) and other sensitive personal information without the express consent of the site visitor, and only after explanation of the potential uses of such information.

7. References


