

Original Paper

# Protected Health Information on Social Networking Sites: Ethical and Legal Considerations

Lindsay A Thompson<sup>1\*</sup>, MD MS; Erik Black<sup>1,2\*</sup>, PhD; W Patrick Duff<sup>3\*</sup>, MD; Nicole Paradise Black<sup>1\*</sup>, MD; Heidi Saliba<sup>1\*</sup>, BA; Kara Dawson<sup>2\*</sup>, PhD

<sup>1</sup>University of Florida, Department of Pediatrics, Gainesville, FL, United States

<sup>2</sup>University of Florida, College of Education, Gainesville, FL, United States

<sup>3</sup>University of Florida, Department of Medicine, Gainesville, FL, United States

\* all authors contributed equally

**Corresponding Author:**

Lindsay A Thompson, MD MS

University of Florida

Department of Pediatrics

1701 SW 16th Ave

Gainesville, FL, 32608

United States

Phone: 1 352 334 1307

Fax: 1 352 334 1348

Email: [lathompson@peds.ufl.edu](mailto:lathompson@peds.ufl.edu)

## Abstract

**Background:** Social networking site use is increasingly common among emerging medical professionals, with medical schools even reporting disciplinary student expulsion. Medical professionals who use social networking sites have unique responsibilities since their postings could violate patient privacy. However, it is unknown whether students and residents portray protected health information and under what circumstances or contexts.

**Objective:** The objective of our study was to document and describe online portrayals of potential patient privacy violations in the Facebook profiles of medical students and residents.

**Methods:** A multidisciplinary team performed two cross-sectional analyses at the University of Florida in 2007 and 2009 of all medical students and residents to see who had Facebook profiles. For each identified profile, we manually scanned the entire profile for any textual or photographic representations of protected health information, such as portrayals of people, names, dates, or descriptions of procedures.

**Results:** Almost half of all eligible students and residents had Facebook profiles (49.8%, or n=1023 out of 2053). There were 12 instances of potential patient violations, in which students and residents posted photographs of care they provided to individuals. No resident or student posted any identifiable patient information or likeness in text form. Each instance occurred in developing countries on apparent medical mission trips. These portrayals increased over time (1 in the 2007 cohort; 11 in 2009;  $P = .03$ ). Medical students were more likely to have these potential violations on their profiles than residents (11 vs 1,  $P = .04$ ), and there was no difference by gender. Photographs included trainees interacting with identifiable patients, all children, or performing medical examinations or procedures such as vaccinations of children.

**Conclusions:** While students and residents in this study are posting photographs that are potentially violations of patient privacy, they only seem to make this lapse in the setting of medical mission trips. Trainees need to learn to equate standards of patient privacy in all medical contexts using both legal and ethical arguments to maintain the highest professional principles. We propose three practical guidelines. First, there should be a legal resource for physicians traveling on medical mission trips such as an online list of local laws, or a telephone legal contact. Second, institutions that organize medical mission trips should plan an ethics seminar prior the departure on any trip since the legal and ethical implications may not be intuitive. Finally, at minimum, traveling physicians should apply the strictest legal precedent to any situation.

(*J Med Internet Res* 2011;13(1):e8) doi: [10.2196/jmir.1590](https://doi.org/10.2196/jmir.1590)

**KEYWORDS**

Protected health information, medical missions, Internet

**Introduction**

Online social networking applications (eg, Facebook, Flickr, Twitter, and YouTube) have become the fastest-growing mechanism to exchange personal and professional information. With 85%-95% of students on college campuses using these communication mediums, and all age groups, even senior citizens, rapidly adopting their use [1,2], online social networking applications have emerged as a significant means of interaction for sharing everything from casual greetings to displaying wedding photographs and lobbying for humanitarian fundraising.

Medical professionals who use social networking sites have unique responsibilities, since their postings could portray themselves in unprofessional ways [3] or, most important, potentially violate patient privacy [3,4]. Publicized breaches of privacy might stem from careless oversights to malicious, illegal, and blatantly unprofessional behaviors. Most worrisome would be those that involve medical students and residents, since their unprofessional behaviors are known to be linked to lifelong licensure problems with state medical boards [5]. Poignantly, Chretien et al recently demonstrated that a significant number of academic medical institutions have experienced incidents of unprofessional student online postings in which some were severe enough to end in student dismissal, although the reasons for these dismissals were not disclosed [6]. Broadly stated, breaches of patient confidentiality involve the identification or potential identification of a patient in any way. Many laws, including the Health Information Portability and Accountability Act (1996, HIPAA), are in place to defend this principle [7,8]. In this context, this study aimed to document whether medical trainees ever share or discuss their patient interactions in their online profiles.

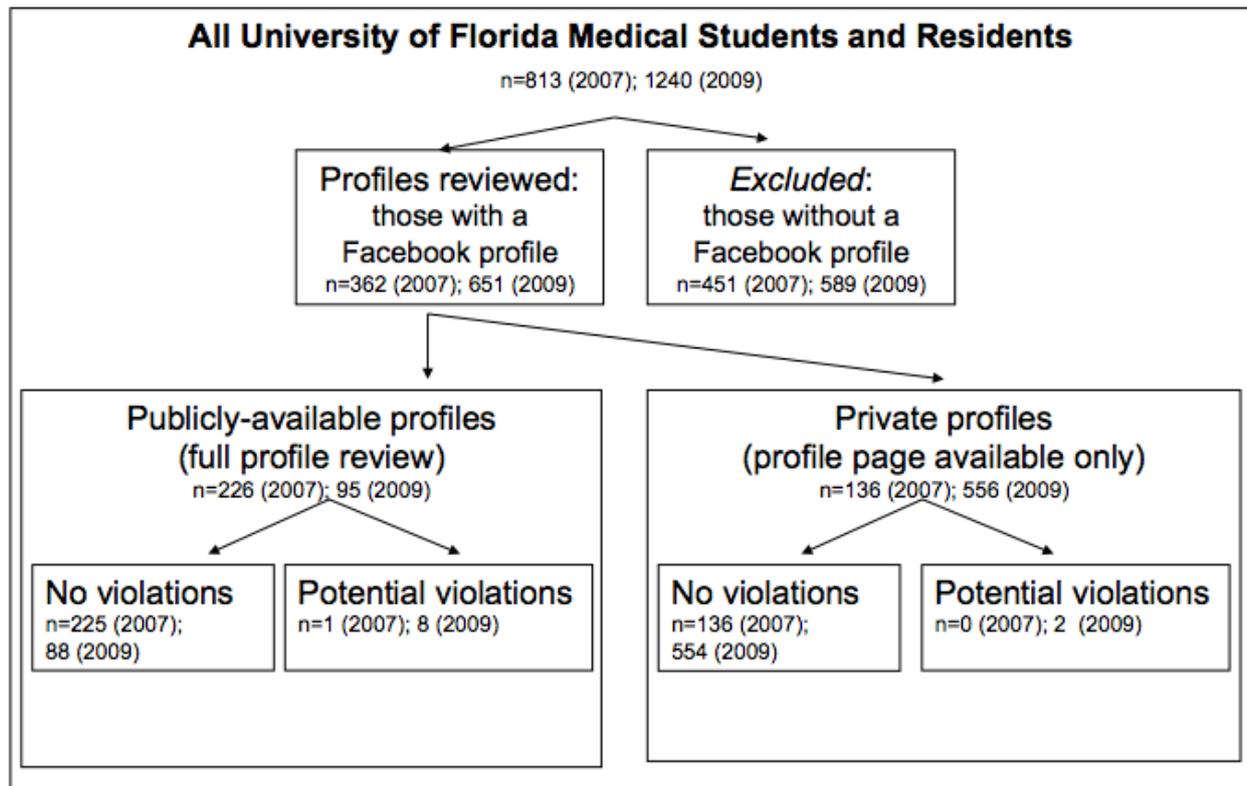
**Methods**

The University of Florida's Institutional Review Board approved as exempt a multidisciplinary team to perform two cross-sectional analyses of Facebook profiles of medical students and residents (2007, 2009). For the purposes of this study, we considered eligible all medical students ( $n = 501$  in 2007, 528 in 2009) enrolled at the University of Florida, Gainesville, and the associated medical residents with available full names ( $n = 312$  in 2007, 712 in 2009) employed by the Shands Hospital. Descriptive findings from each cohort have been published elsewhere [3,9]. In brief, Facebook proceedings allow any registered user of Facebook access to every Facebook profile according to each individual owner's chosen preferences for privacy. To be a Facebook user, an applicant only needs to supply an email address and choose a password. Once a user, one can scan Facebook profiles anonymously, without revealing to the profile owners that their site has been viewed. Drawing on these parameters, the first profile search associated with this study was done from June 7 to June 11, 2007, where three

researchers used personally created Facebook accounts to manually search for the study subjects' online profiles using a university-generated list of names of students and residents. The second cohort was searched from September 2 to October 7, 2009, where only one study author (EB) used a personal account to manually search for the study subjects' online profiles using the 2009 university lists. Given that the study began in 2007, it did not use any face-recognition software, since it was not available at the time, and our study protocol did not include searching "friends' sites" for the study subjects. We likewise could not discern how often a profiler used Facebook, nor could we tell the duration that a profiler had the account. We could not discern the frequency with which a subject accessed Facebook. This study was part of a larger study on trends of social networking site use among medical students and residents [3,9]. We first determined whether each student or resident had a Facebook account and whether that account was "private" or "public," a designation that each user can activate to limit some, or all, of a site's content. Sites were deemed private if the following message appeared on the site of interest: "\_\_\_\_ only shares certain information with everyone. If you know \_\_\_\_, add him/her as a friend on Facebook." Three study authors (EB, LT, KD) compared their individual analyses of the content. We found a high degree of interrater reliability using intraclass correlation (type 1,  $df = 6$ ) = 0.9, for the public profiles of medical students and residents in characterizing material with complete unanimity for the comparisons of potential patient privacy violations [9]. We searched a total of 1023 profiles ( $n = 372$  profiles in 2007 and 651 in 2009; see Figure 1 for flowchart of subjects and profiles reviewed).

For the purposes of this study, we reviewed sites for possible privacy violations to explicitly examine how students are using sites according to legal and ethical professional norms. Once a profile related to a study subject was found, any potential violation within a site was counted as one, even if a profile had multiple representations. For private sites, where optional Facebook privacy settings can limit non-"friends" from viewing part or most of the site, study authors reviewed only the profile photograph(s) and available content on their front page, where Facebook users can choose to list information such as name, address, and favorite hobbies. For publicly available profiles ( $n = 233$ , 62.6% in 2007;  $n = 95$ , 14.6% in 2009), we manually scanned all information, including all scrolled wall posts in text form and extensive albums for photographs, for patient information, such as names, dates, and procedures, photographs of patients or procedures, or any mention of patients. We also recorded available demographic information of the subjects (gender, year in training, relative age of subject). At the end of the study, in September 2010, we reviewed the sites that had potential privacy violations; all sites were now private and could not be reviewed. We performed our analyses using SPSS PASW Statistics, version 17 (Chicago, IL), and we accepted a level of significance of  $P < .05$  using a Student  $t$  test for comparison [10].

**Figure 1.** Enrollment of medical students and residents' Facebook profiles



## Results

A significant proportion (49.8%) of medical students and residents had profiles (n = 1023 out of 2053 eligible students and residents). Students and residents increased their use of Facebook, with 44.5% using Facebook in 2007 (n = 362 of 813), compared to 52.5% in 2009 (n = 651 of 1240,  $P < .0001$ ). By 2009, a majority (85.4%) of profiles were made private by their owners compared to 37.6% in 2007 ( $P < .001$ ). However, we found significant and increasing evidence of potential privacy violations (n = 12; 1 of 372 in 2007, 10 of 651 in 2009;  $P = .03$ ). Medical students were more likely than residents to have these violations (10 students, 1 resident;  $P = .04$ ). In each instance, all of which were photographic patient information, the profile owners illustrated themselves providing health care to individuals (see deidentified examples, [Figures 2-5](#); authors added the face blockouts). We did not find any textual evidence

of patient information or likeness that could potentially violate patient privacy.

In each of these groups of photographs, the profile owner was apparently on a medical mission trip, performing health care in another county. These photographs were placed in photo albums that the profile owner explicitly labeled (eg, “mission trip” or “Dominican Republic”), giving the viewer a context for understanding where they are from. Among “private” profiles (n = 701), two displayed themselves on their profile picture with identifiable patients, which is the information first available on any profile when a user peruses Facebook profiles. For those with publicly available Facebook profiles (n = 328 total, 233 in 2007; 95 in 2009), 10 additional sites had potential privacy violations within their profile’s photo albums. Photographs included trainees interacting with identifiable patients or performing medical examinations or procedures such as vaccinations. Of note, in each photograph, the recipient of the care was a child.

**Figure 2.** Example of a potential violation of patient privacy

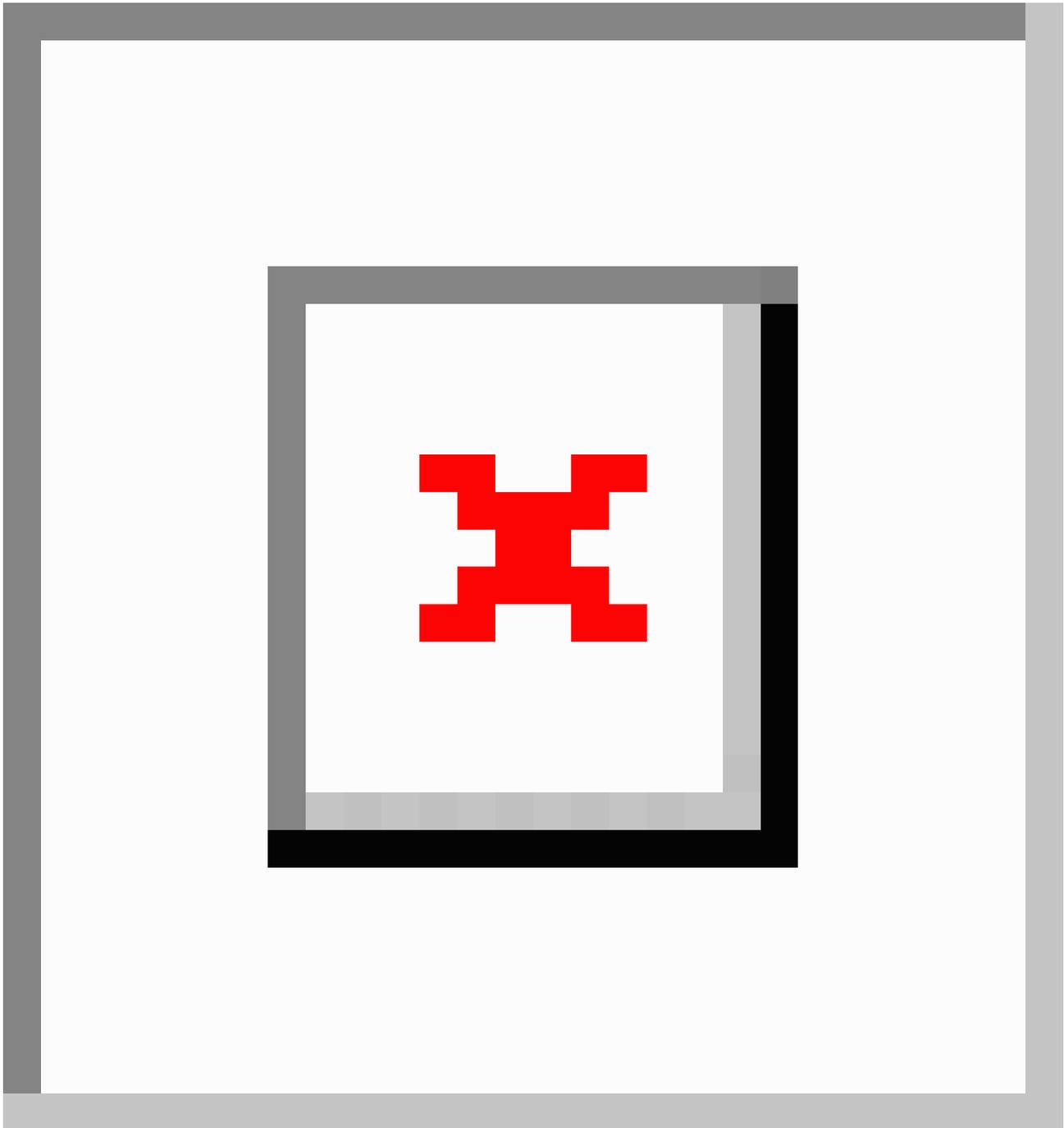


Figure 3. Example of a potential violation of patient privacy



**Figure 4.** Example of a potential violation of patient privacy

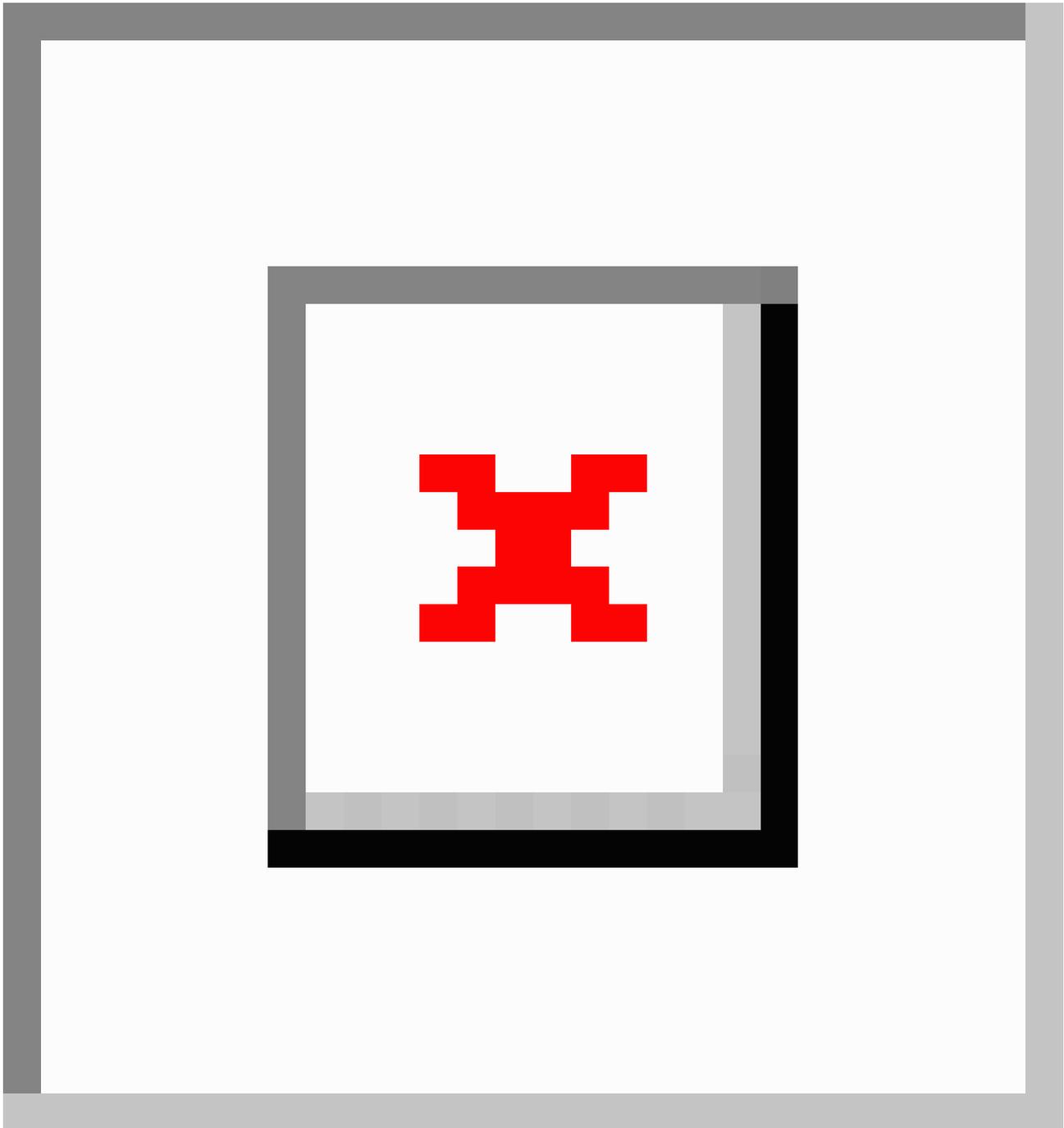


Figure 5. Example of a potential violation of patient privacy



## Discussion

This study reveals that students and residents place protected health information on their publicly available social networking sites. This exposes significant concerns with the ethical and legal aspects of patient portrayals, a problem well debated with cyberspace issues [11,12], but one that has been magnified by the recent phenomenon of online social networking [13]. As an unanticipated outcome, these violations seem only to be in the context of medical mission trips. Medical missions, defined as a “group of people traveling from a developed country to a developing country for a short period of time” [14] with the purpose of providing needed health care, are viewed as highly professional, benevolent acts [15]. Nonetheless, posting photographs or information from such events challenges US and international laws of patient privacy, regardless of whether content is posted to a publicly available or private profile. Imagery of humanitarian trips is common, even supported in medical settings [15]; perhaps the reason why this online imagery is not only common but increasing. It is likely, given the increasing frequency of these portrayals, that medical students and residents believe they are representing themselves in a prosocial manner on their online profile, forgetting or ignoring that this can conflict with their professional responsibilities. Nonetheless, any single incident of an online depiction represents the tension between personal pride in compassionate acts and unethical and potentially illegal representations and descriptions of individuals receiving medical care.

Medical mission trips offer an opportunity to trainees and doctors alike to learn to practice medicine outside of the highly technical US hospitals and to gain personal satisfaction in treating patients who may otherwise not have access to care. However, these acts of compassion or benevolence should not be available for public or private discussion or viewing outside the context of the doctor-patient relationship. Medical trainees and providers at all levels need to apply legal and ethical practices of patient privacy at all times of their working careers. We believe that photographs of patients from medical mission trips are unethical and unprofessional, yet, due to variances in established international and emerging Internet law, they are only a possible privacy violation.

HIPAA (1996) [7,8] and other laws such as the Health Information Technology for Economic and Clinical Health Act demonstrate that the legal aspects of protecting patient identities in the digital age are complex [16-18]. In this study, students and residents do not appear to violate patient privacy at their own US institutions through online postings, but they seem to not equate this standard to medical mission trips in other countries. The Hippocratic Oath, HIPAA, and individual state and international laws all articulate different regulatory standards of patient privacy to which health care providers, as “covered entities,” must adhere. While extensive and at times confusing, they are nonetheless the law. Medical mission trips within the United States, for example, would characterize written patient health information on the Internet as HIPAA violations [7,8], but potentially not a photograph if it is not a “full-face photographic image” [19]. Other countries, such as Argentina,

have stricter patient privacy laws that may include any photography [20]. Further, state laws in the United States may dictate higher standards than the federal HIPAA law for their licensed practitioners. In Florida, for example, all physicians are required to always maintain patient confidentiality regardless of where they are. To date, there is no legal precedent for the adjudication of these potential online violations, nor guidance from the medical literature on how to maintain high standards of patient privacy in the age of online social networking. To the contrary, in fact, one publication (predating online user-generated content) *advocated* the use of digital photography, ostensibly for its ease of transmission and reproduction [21]. It is yet unknown who, outside of the individual patient, could claim a violation when viewing online content. Nonetheless, awaiting legal action is ill advised.

Like the legal aspects, the ethics involved are multifaceted. In speaking to the responsibilities of health care providers who place patient information online, social networking sites challenge the difference between public and private information. In fact, one might argue that, while these sites are public, users are likely operating under the expectations of privacy [22]. However, users of social networking sites not only choose to have profiles with photos, text, and other self-created content, they also have control over whether such content is available to everyone (publicly available) or whether their profile and its content are private to some or all. Of note, since this study was performed, Facebook has changed its privacy features (December 2009), requiring users to actively select what it describes as “simplified privacy settings.” However, its default settings allow for unrestricted public access, much to the consternation of Internet privacy and security experts [23]. It remains unknown how medical professionals will respond to this privacy option. Additionally, current academic discussions describe the exact nature of what is public versus private, or identified versus deidentified on the Internet as not dichotomous [24], and that privacy is ultimately a function of social context, meaning that displays and disclosure of information may be appropriate in some contexts but not in others [13]. Profiles and postings of any type—public or private—are ultimately the responsibility of the creators, who in this case are practicing medical trainees and/or professionals who have completed HIPAA and confidentiality training. Unique to the fields of health care, these roles and their attendant responsibilities continue beyond the end of a shift and into all spheres of their lives, including when traveling abroad.

Additional ethical considerations may question what duty that we, as authors, have in collecting and analyzing data obtained from public online social networking sites [12,13,16]. Foremost, as medical professionals, we are bound to report potential abuses of children [25]. We do not feel this has occurred. Additionally, it could be argued that research on social networking sites is voyeuristic, hence inappropriate. Leading researchers, however, have likened social network research to research on newspaper personal ads [26], removing much of the mystery surrounding its potential. We believe that medical educators need to be particularly sensitive to educating our students and residents about patient privacy with clear and salient guidance on the various aspects of professionalism as it pertains to online

postings. Given the overwhelming popularity of social networking applications such as Facebook, and their convenient and compelling means by which to exchange personal information, educators must better inform students that posting patient information may lead to serious, unintended, and irreversible consequences.

### Practical Recommendations

We make the following recommendations. First, there should be a legal resource for physicians traveling on medical mission trips such as an online list of local laws, or a telephone legal contact. To our knowledge, this does not exist. Second, we believe institutions that organize medical mission trips should plan this type of ethics seminar prior to the departure of any trip, since the legal and ethical implications may not be intuitive. Further, while an understanding of local privacy laws prior to departure on a medical mission trip would be ideal, it is nonetheless, at minimum, advisable to be cautious and apply the strictest legal precedent to any situation. For example, physicians should never write any patient information in text form or use a full-face photograph of a patient receiving any treatments. If photographs of individuals are desired, written consent should be obtained (although the wording of such documents may still not be legally defensible in that country). Additionally, subjects should only be shown in profile or in shadows, or physicians/medical professionals should use photo editing software to deidentify patients' faces (see [Figures 2-5](#) for the authors' examples of ways to deidentify patients and trainees). While photographs can play a central role for both physicians (eg, in dermatology) and patients (eg, the birth of a child), they are one of the most difficult legal and ethical considerations in online portrayals and as such demand careful attention.

### Study Limitations

This study has several limitations. First, this study was performed at a single institution, where it is possible that the

students and residents with patient portrayals did in fact receive permission from the individuals that they photographed. However, no acknowledgement or supportive information regarding this consideration was available on the individual profiles. Second, while it appears that medical students are more likely than residents to post content that may violate patient privacy, this likely is a function of the structure of medical school in which students in their fourth year have the most time for trips overseas and their younger age [27]. Finally, we cannot comment on profiles that have been made private. It is likely, perhaps even more likely, that photographs or even text that may violate patient privacy exists on private sites, since profile owners may feel their audience is not public. However, given the large number of profile friends Facebook users have (sometimes thousands), the notion of privacy is again contextual [26]. Yet patient privacy is not contextual. It is concrete and unyielding to electronic and other innovations for social networking.

### Conclusions

As a profession, we have made considerable strides to protect patient privacy. We have not, however, adequately impressed upon students and residents that online social networking sites and blogs are, in essence, broad communities with a public audience. They are arenas, such as medical mission trips, in which patient information must be guarded just as it would be in any health care situation. Future studies should explore the motivations behind such postings, but we believe the observations found in this study merit swift action, since the nature of social networking sites allows for immediate assumptions by the observer, whether or not these assumptions are formed within the context that the profiler intended. Medical mission trips require the same high professional standards of patient privacy that all medical situations require, whether in a highly technical US tertiary care center or in a rural medical clinic in another country.

---

### Acknowledgments

We would like to thank the Office of Privacy at the University of Florida, specifically Susan Blair and B Dianne Farb, JD, for their careful review of this manuscript. Publication of this article was funded in part by the University of Florida Open-Access Publishing Fund.

---

### Conflicts of Interest

None declared

---

### Authors' Contributions

All of the authors are responsible and qualified for the reported research. They have all participated in the concept and design, analysis and interpretation of data, and drafting and revision of the manuscript and approve the manuscript as submitted. All of the authors have had full access to all the data in the study and take responsibility for the integrity of the data and the accuracy of the data analysis. None of the authors, to our knowledge, have any undisclosed affiliations, conflicts of interests, or financial arrangements with any organizations mentioned in the manuscript.

---

### References

1. Corbett P. iStrategyLabs. 2009. Facebook demographics and statistics report: 513% growth in the 55+ year old users. College and high school drop 20% URL: <http://www.istrategylabs.com/2009/07/2009-facebook-demographics-and-statistics-report-513-growth-in-55-year-old-users-college-high-school-drop-20/> [accessed 2010-11-24] [[WebCite Cache ID 5uUHjd8Ys](#)]

2. Lampe C, Ellison N, Steinfeld C. Changes in the use and perception of Facebook. 2008 Presented at: ACM Conference on Computer Supported Cooperative Work; 2008; San Diego, CA, USA.
3. Thompson LA, Dawson K, Ferdig R, Black EW, Boyer J, Coutts J, et al. The intersection of online social networking with medical professionalism. *J Gen Intern Med* 2008 Jul;23(7):954-957. [doi: [10.1007/s11606-008-0538-8](https://doi.org/10.1007/s11606-008-0538-8)] [Medline: [18612723](https://pubmed.ncbi.nlm.nih.gov/18612723/)]
4. Lagu T, Kaufman EJ, Asch DA, Armstrong K. Content of weblogs written by health professionals. *J Gen Intern Med* 2008 Oct;23(10):1642-1646. [doi: [10.1007/s11606-008-0726-6](https://doi.org/10.1007/s11606-008-0726-6)] [Medline: [18649110](https://pubmed.ncbi.nlm.nih.gov/18649110/)]
5. Papadakis MA, Teherani A, Banach MA, Knetter TR, Rattner SL, Stern DT, et al. Disciplinary action by medical boards and prior behavior in medical school. *N Engl J Med* 2005 Dec 22;353(25):2673-2682 [FREE Full text] [doi: [10.1056/NEJMSa052596](https://doi.org/10.1056/NEJMSa052596)] [Medline: [16371633](https://pubmed.ncbi.nlm.nih.gov/16371633/)]
6. Chretien KC, Greysen SR, Chretien JP, Kind T. Online posting of unprofessional content by medical students. *JAMA* 2009 Sep 23;302(12):1309-1315 [FREE Full text] [doi: [10.1001/jama.2009.1387](https://doi.org/10.1001/jama.2009.1387)] [Medline: [19773566](https://pubmed.ncbi.nlm.nih.gov/19773566/)]
7. Office for Civil Rights. Standards for privacy of individually identifiable health information: final rule. *Fed Regist* 2002 Aug 14;67(157):53182-53273 [FREE Full text]
8. U.S. Department of Health and Human Services. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule URL: <http://www.hhs.gov/ocr/privacy/> [accessed 2010-11-24] [WebCite Cache ID 5uUDEnV1r]
9. Black EW, Thompson LA, Duff WP, Dawson K, Saliba H, Black NM. Revisiting social network utilization by physicians-in-training. *J Grad Med Educ* 2010;2(2):289-293. [doi: [10.4300/JGME-D-10-00011.1](https://doi.org/10.4300/JGME-D-10-00011.1)]
10. Cohen J. Statistical power analysis. *Current Directions in Psychological Science* 1992;1(13):98-101. [doi: [10.1111/1467-8721.ep10768783](https://doi.org/10.1111/1467-8721.ep10768783)]
11. Rodrigues R. Ethical and legal issues in interactive health communications: a call for international cooperation. *J Med Internet Res* 2000;2(1):E8 [FREE Full text] [doi: [10.2196/jmir.2.1.e8](https://doi.org/10.2196/jmir.2.1.e8)] [Medline: [11720927](https://pubmed.ncbi.nlm.nih.gov/11720927/)]
12. Eysenbach G, Till JE. Ethical issues in qualitative research on internet communities. *BMJ* 2001 Nov 10;323(7321):1103-1105 [FREE Full text] [Medline: [11701577](https://pubmed.ncbi.nlm.nih.gov/11701577/)]
13. Eysenbach G. Medicine 2.0: social networking, collaboration, participation, apomediation, and openness. *J Med Internet Res* 2008;10(3):e22 [FREE Full text] [doi: [10.2196/jmir.1030](https://doi.org/10.2196/jmir.1030)] [Medline: [18725354](https://pubmed.ncbi.nlm.nih.gov/18725354/)]
14. Bradke AJ. The Ethics of Medical Brigades in Honduras: Who Are We Helping? [master's thesis]. Pittsburgh, PA: University of Pittsburgh; 2007.
15. Hanson L, Harms S, Plamondon K. Undergraduate international medical electives: some ethical and pedagogical considerations. *J Studies Int Educ* 2010. [doi: [10.1177/1028315310365542](https://doi.org/10.1177/1028315310365542)]
16. Hrynaskiewicz I, Norton ML, Vickers AJ, Altman DG. Preparing raw clinical data for publication: guidance for journal editors, authors, and peer reviewers. *BMJ* 2010;340:c181. [Medline: [20110312](https://pubmed.ncbi.nlm.nih.gov/20110312/)]
17. Parsell M. Pernicious virtual communities: identity, polarisation and the Web 2.0. *Ethics Inf Technol* 2008;10:41-56. [doi: [10.1007/s10676-008-9153-y](https://doi.org/10.1007/s10676-008-9153-y)]
18. Weitzman ER, Kaci L, Mandl KD. Sharing medical data for health research: the early personal health record experience. *J Med Internet Res* 2010;12(2):e14 [FREE Full text] [doi: [10.2196/jmir.1356](https://doi.org/10.2196/jmir.1356)] [Medline: [20501431](https://pubmed.ncbi.nlm.nih.gov/20501431/)]
19. American Health Information Management Association. Practice brief. Patient photography, videotaping, and other imaging (updated). *J AHIMA* 2001 Jun;72(6):64M-64Q. [Medline: [12793246](https://pubmed.ncbi.nlm.nih.gov/12793246/)]
20. Gakh M. Argentina's protection of personal data: initiation and response. *ISJLP* 2006;2:781.
21. Davolt DA. The use of digital photography to support a medical mission to Honduras. *J Biocommun* 2000;27(2):22-24. [Medline: [11050711](https://pubmed.ncbi.nlm.nih.gov/11050711/)]
22. Kleinberg J. Challenges in mining social network data: processes, privacy, and paradoxes. 2007 Presented at: 3rd ACM SIGKDD international conference on knowledge discovery and data mining; August 12-15, 2007; San Jose, CA, USA.
23. Prince B. 3Week.com. 2009 Dec 20. Facebook privacy: Just how much do users want? URL: [http://www.eweek.com/index2.php?option=content&task=view&id=58084&pop=1&hide\\_ads=1&page=0&hide\\_js=1](http://www.eweek.com/index2.php?option=content&task=view&id=58084&pop=1&hide_ads=1&page=0&hide_js=1) [accessed 2009-12-23] [WebCite Cache ID 5uMZKDSnt]
24. Bos N, Karahalios K, Musgrove-Chavez M, Poole E, Thomas JC, Yardi S. Research ethics in the Facebook era: privacy, anonymity, and oversight. In: 27th International Conference's Extended Abstracts on Human Factors in Computing. 2009 Presented at: ACM Conference on Human Factors in Computing Systems; 2009; New York, NY, USA.
25. Office on Child Abuse and Neglect. U.S. Department of Health and Human Services. 2003 Jun 25. The Child Abuse Prevention and Treatment Act URL: [http://www.acf.hhs.gov/programs/cb/laws\\_policies/cblaws/capta03/capta\\_manual.pdf](http://www.acf.hhs.gov/programs/cb/laws_policies/cblaws/capta03/capta_manual.pdf) [accessed 2010-11-24] [WebCite Cache ID 5uUQRqJGS]
26. Nissenbaum H. Privacy as contextual integrity. *Washington Law Rev* 2004;79:1.
27. Chou WY, Hunt YM, Beckjord EB, Moser RP, Hesse BW. Social media use in the United States: implications for health communication. *J Med Internet Res* 2009;11(4):e48 [FREE Full text] [doi: [10.2196/jmir.1249](https://doi.org/10.2196/jmir.1249)] [Medline: [19945947](https://pubmed.ncbi.nlm.nih.gov/19945947/)]

## Abbreviations

**HIPAA:** Health Information Portability and Accountability Act

*Edited by G Eysenbach; submitted 27.06.10; peer-reviewed by T Lagu, F Grajales III; comments to author 05.08.10; revised version received 22.09.10; accepted 21.10.10; published 19.01.11*

*Please cite as:*

*Thompson LA, Black E, Duff WP, Paradise Black N, Saliba H, Dawson K  
Protected Health Information on Social Networking Sites: Ethical and Legal Considerations*

*J Med Internet Res 2011;13(1):e8*

*URL: <http://www.jmir.org/2011/1/e8/>*

*doi: [10.2196/jmir.1590](https://doi.org/10.2196/jmir.1590)*

*PMID: [21247862](https://pubmed.ncbi.nlm.nih.gov/21247862/)*

©Lindsay A Thompson, Erik Black, W Patrick Duff, Nicole Paradise Black, Heidi Saliba, Kara Dawson. Originally published in the Journal of Medical Internet Research (<http://www.jmir.org>), 19.01.2011. This is an open-access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/2.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work, first published in the Journal of Medical Internet Research, is properly cited. The complete bibliographic information, a link to the original publication on <http://www.jmir.org/>, as well as this copyright and license information must be included.