

Athletic Trainers' Knowledge of Legal Practice within Information Technology and Social Media

Elizabeth R. Neil

Indiana State University, eneil@sycamores.indstate.edu


Zachary K. Winkelmann

Indiana State University, zwinkelmann@indstate.edu

Lindsey E. Eberman

Indiana State University, lindsey.eberman@indstate.edu

Follow this and additional works at: <https://scholarworks.bgsu.edu/jsmahs>

 Part of the [Biomechanics Commons](#), [Exercise Science Commons](#), [Motor Control Commons](#), [Other Kinesiology Commons](#), [Rehabilitation and Therapy Commons](#), [Sports Medicine Commons](#), and the [Sports Sciences Commons](#)

Recommended Citation

Neil, Elizabeth R.; Winkelmann, Zachary K.; and Eberman, Lindsey E. () "Athletic Trainers' Knowledge of Legal Practice within Information Technology and Social Media," *Journal of Sports Medicine and Allied Health Sciences: Official Journal of the Ohio Athletic Trainers Association*: Vol. 3 : Iss. 2 , Article 1.

DOI: 10.25035/jsmahs.03.02.01

Available at: <https://scholarworks.bgsu.edu/jsmahs/vol3/iss2/1>

This Article is brought to you for free and open access by the Human Movement, Sport and Leisure Studies at ScholarWorks@BGSU. It has been accepted for inclusion in Journal of Sports Medicine and Allied Health Sciences: Official Journal of the Ohio Athletic Trainers Association by an authorized editor of ScholarWorks@BGSU.

Athletic Trainers' Knowledge of Legal Practice within Information Technology and Social Media

Elizabeth R. Neil MS, LAT, ATC, Zachary K. Winkelmann MS, LAT, ATC, Lindsay E. Eberman PhD, LAT, ATC
Indiana State University

Purpose: As healthcare and technology continue to connect in daily practice, athletic trainers (ATs) must be knowledgeable of the governing acts for ethical and legal clinical practice. This is vital to ensure ethical and legal practice as a clinician and protection of confidential protected health information (PHI). The objective of this study was to assess certified athletic trainers' knowledge of regulations within technology and social media (SoMe). **Methods:** Certified ATs were recruited from the National Athletic Trainers' Association membership database. Respondents completed an instrument of 28 questions, including 16 participant demographics, clinical site demographics, SoMe usage and general questions, and a 12-item knowledge assessment tool on a web-based survey platform. Validity of the instrument was determined through a Delphi panel of experts in athletic training, healthcare lawyers and an information technologist. We analyzed data using descriptive statistics. **Results:** Respondents reported a Master's degree as their highest earned (n=106, 72.6%) with 33.6% of those degrees being at the professional level (n=49). Respondents predominately worked in the public secondary school setting (n=43, 29.5%) and worked 8-9 hours per day (n=78, 53.4%). Respondents self-reported an average of five active SoMe accounts with Facebook[®] (n=120, 81.6%), LinkedIn[®] (n=75, 51%), Instagram[®] (n=70, 47.6%), Twitter[®] (n=70, 47.6%), Pinterest[®] (n=64, 43.5%), and Snapchat[®] (n=64, 43.5%) being the most common sites. Within their athletic training clinic, respondents predominately reported (n=76, 51.7%) that all their computers had a virtual private network, and had a SoMe policy that was enforced to some extent (n=63, 42.9%). Respondents (n=136, 92.5%) stated that they have not reported someone for a breach of HIPAA, and have not been reported themselves (n=146, 99.3%); however, respondents (n=16, 10.8%) indicated they had one or more full faced photos of patients on their SoMe accounts, breaching HIPAA. The majority of respondents have had formal education on HIPAA regulations (n=115, 78.2%). On the knowledge assessment, Respondents correctly scored 7.7±1.9 out of 12 possible points (mean score=59.2±14.5%). **Conclusions:** Respondents lacked the appropriate knowledge regarding HIPAA and Health Information Technology for Economic and Clinical Health (HITECH) Act regulations, and application of this knowledge within SoMe. Future research should focus on educational interventions of technology advancements for safe and legal practice as an AT.

INTRODUCTION

Patient-centered care and protection is of the utmost importance for healthcare professionals. Athletic trainers, along with other healthcare professionals, must be conscientious in the way they choose to communicate with their patients. Modern communication expands from face-to-face methods to additional electronic methods. The expansion in the means of communication has the potential to allow for additional breaches of patient confidentiality. There are

several safeguards to ensure legal and ethical practice for these covered entities. The Health Insurance Portability and Accountability Act (HIPAA) was created in 1996 as a baseline of minimal standards that must be met to protect a patient's protected health information (PHI).¹ Athletic training clinics in secondary schools, and college and university settings have additional regulations regarding the protected health information of their patient student-athletes. The Federal Education Rights to Privacy Act (FERPA) is in place to

protect the educational records, which include all medical records, depending on where the athletic training clinic is housed.² These acts and regulations seek to minimize the risk to our patients while protecting the healthcare provider. The Health Information Technology for Economic and Clinical Health (HITECH) Act is an amendment to HIPAA and designed for protection of electronic protected health information of patients through digital and technological communication including that of medical records and photographs.

In order to provide the highest quality of care to our patients, all healthcare providers, without regard to discipline or expertise, should be competent in the delivery of five areas of interest according to the Institute of Medicine (IOM).³ These core competencies includes: (1) providing patient-centered care, (2) working in interdisciplinary teams, (3) employing evidence-based practice, (4) apply quality improvement, and to (5) utilize informatics.⁴ The realm of informatics and use of technology in healthcare has expanded to a scope that clinicians need to be able use technology to reduce errors, manage knowledge and information, make decisions, and communicate. Specifically, the use of technology to communicate has the potential to paradoxically increase the errors in legal and ethical actions regarding patient privacy.

As the adoption of the core competencies by all healthcare professionals occur, ATs will continue to see their practice with technology expand with electronic medical records, electronic health records, and their presence in social media (SoMe). Additionally, as advancements in technology have developed in conjunction with the current generation, there is a need for legislative efforts to protect the patient in these new mediums.⁴ The problem of ethics within SoMe is not isolated to only athletic training, but is an emerging concern for many other healthcare providers, including physicians.⁵ As a result of the advancements in healthcare technology and growth of SoMe, there is a need to investigate if ATs are aware of the regulations in place. The purpose of this study was to examine

certified ATs knowledge of legal practice within information technology and SoMe.

METHODS

Instrumentation

To design the instrument for this research, we surveyed a panel of experts in several disciplines by means of the Delphi technique. The Delphi technique is a method of structuring the collective judgments of a group of experts, conducted through a series of sequential questionnaires, each containing summarized information from earlier responses.⁶ A total of eight experts (3 certified athletic trainers, 2 healthcare compliance solution experts, and 3 lawyers with a specialty interest in risk management and healthcare) served on the panel. Three rounds of questionnaires were completed to gather the opinions of experts and ultimately reach consensus. Each questionnaire was generated from the results of the previous questionnaire. The initial questionnaire asked the expert panel to list items that they perceived as potential HIPAA breaches in SoMe. The second round was generated from the results of the first and asked the expert panel to comment on the entire survey for length, accuracy, and omissions. The third questionnaire allowed the expert panel to check accuracy of the content and answers choices. The Delphi technique concluded with a consensus confirmation report that asked the expert panel to agree with the final form of the instrument. Following content consensus from the Delphi panel, the research team utilized a pilot study. This method was used to increase success for the final research study.

For the pilot study, the professional athletic training students (n=51) at a Midwestern University were utilized as a convenience sample. The convenience sample respondents (age = 21±1 yr, 30 female, 21 male) took the survey and knowledge assessment. This data was not used for the final analysis, and all students at the university were excluded from participation in the final research study. The outcomes of the pilot study determined feasibility and content analysis for the variables of the knowledge assessment.

Tasks

Once IRB exemption was granted, a cross-sectional study design was used. Data were collected through a web-based survey (Qualtrics, Inc; Provo, UT). After electronically signing the informed consent, respondents entered the survey, which included demographic information about the respondent, their SoMe profiles and usage, and the setting in which they are employed. The respondents engaged in a 12-item knowledge assessment including six knowledge retrieval items on governing regulations (HIPAA and HITECH), two items focused on potential breaches when using technology, and four knowledge utilization items with specific examples of potential HIPAA violations in sample SoMe posts.

Procedures

The National Athletic Trainers' Association (NATA) e-mailed the informed consent and a link to the educational assessment to three random samples of NATA members (each sample contained 1000 members). These members consisted of those who are certified members. All 10 NATA districts were studied as well as all international members who met the previous criteria. Retired clinicians were excluded from the study. The NATA e-mailed reminders to each sample after two weeks. Respondents had access to the survey for a span of six weeks.

Respondents

A total of 3000 ATs were recruited for this study. 272 ATs began the study for a response rate of 9.1%. After filtering the responses who had not finished the survey in its entirety, 147 respondents were used for the analysis. A final response rate of 4.9% was used for the analysis.

Statistical Analysis

The data were collected and entered into custom spreadsheet software (Microsoft Excel

2013, Microsoft Corp., Redwood, WA, USA). These data were then analyzed using the Statistical Package for Social Sciences (IBM Corp. IBM SPSS Statistics for Windows, Version 23.0. Armonk, NY: IBM Corp.) We analyzed the data using descriptive statistics for the knowledge items including the mean and standard deviation. Data were analyzed for the knowledge assessment so correct answers accounted for a score of 1, while incorrect and omitted correct answers with multiple correct answers account for a -1, allowing negative scoring for this section. We utilized a negative scoring method to account for respondent guessing.

RESULTS

Respondents were predominately female (n=83, 57.1%) and were all BOC certified athletic trainers (n=147, 100%). Respondents reported a Master's degree as their highest degree earned (n=106, 72.6%). A total of 33.6% of the Master's degrees were at the professional level (n=49). Respondents predominately worked in the public secondary school setting (n=43, 29.5%) and worked on average 8-9 hours per day (n=78, 53.4%). Respondents self-reported an average of five active SoMe accounts with Facebook[®] (n=120, 81.6%), Google+[®] (n=113, 76.9%), LinkedIn[®] (n=75, 51%), Instagram[®] (n=70, 47.6%), Twitter[®] (n=70, 47.6%), Pinterest[®] (n=64, 43.5%), and Snapchat[®] (n=64, 43.5%) being the most common sites. The majority of respondents have had formal education on HIPAA regulations (n=115, 78.2%). Respondents (n=136, 92.5%) stated that they have not reported someone for a breach of HIPAA, and have not been reported themselves (n=146, 99.3%); however, respondents (n=16, 10.8%) indicated they had one or more full faced photos of patients on their SoMe accounts, breaching HIPAA. Table 1 provides a detailed explanation of the demographics for the respondents.

Table 1. Respondent Demographics

Characteristic (No. Reporting)	Frequency (%)
Sex (n=147)	
Male	63 (42.9)
Female	84 (57.1)
BOC Certification (n=147)	
NATA District (n=142)	
1: Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont	9 (6.32)
2: Delaware, New Jersey, New York, Pennsylvania	26 (18.3)
3: District of Columbia, Maryland, North Carolina, South Carolina, Virginia, West Virginia	16 (11.3)
4: Illinois, Indiana, Michigan, Minnesota, Ohio, Wisconsin	30 (21.1)
5: Iowa, Kansas, Missouri, Nebraska, North Dakota, Oklahoma, South Dakota	11 (7.7)
6: Arkansas, Texas	10 (7.0)
7: Arizona, Colorado, New Mexico, Utah, Wyoming	12 (8.5)
8: California, Hawaii, Nevada	9 (6.3)
9: Alabama, Florida, Georgia, Kentucky, Louisiana, Mississippi	14 (9.5)
10: Alaska, Idaho, Montana, Oregon, Washington	5 (3.5)
Clinical Sites of Employment (n=146)	
NCAA Division 1	17 (11.6)
NCAA Division 2	7 (4.8)
NCAA Division 3	13 (8.8)
NAIA	4 (2.7)
Public Secondary School	43 (29.5)
Private Secondary School	8 (5.5)
Hospital/ Emergency Room	5 (3.4)
Professional Sports	3 (2.1)
Physical Therapy Clinic	2 (1.4)
Student Health Center	1 (0.7)
Junior College (NJCAA)/Community College	5 (3.4)
Physician Office	7 (4.8)
Industrial	2 (1.4)
Other	10 (6.8)
2 or more job settings	19 (13.0)
Average Hours Worked per Day (n=146)	
0-1 Hours	2 (1.4)
2-3 Hours	0 (0)
4-5 Hours	7 (4.8)
6-7 Hours	24 (16.4)
8-9 Hours	78 (53.8)
10 or More Hours	35 (23.8)
Highest Degree earned (n=146)	
Professional Bachelors	31 (21.2)
Professional Masters	49 (33.6)
Post-Professional Masters	18 (12.3)
Non-AT Masters	39 (26.7)
PhD	5 (3.4)

TABLE 1. CONT

Other	4 (2.7)
Does your athletic training clinic have a social media policy (n=147)	
Yes, and I is strictly enforced	36 (24.5)
Yes, and it is somewhat enforced	27 (18.4)
Yes, and it is not enforced	3 (2.0)
No, and I do not believe we need a policy	25 (17.0)
No, but I believe we need a policy	24 (16.3)
Not sure	32 (21.8)

Within their athletic training clinic, respondents predominately reported (n=76, 51.7%) that all their computers had a virtual private network, and had a SoMe policy that was enforced to some extent (n=63, 42.9%). Additionally, 17% of respondents (n=25) did not have nor believe their athletic training clinic needed a SoMe policy.

On the knowledge assessment, respondents correctly scored 7.7 ± 1.9 out of 13 possible points (mean score = $59.2 \pm 14.5\%$ out of 100%). The most missed questions included identifying a potential breach of HIPAA in a sample Twitter[®] post (correct: n=27/146,

18.5%), appropriate communication via text message (correct: n=21/99, 21.2%) and governance of the HITECH Act (correct: n=45/137, 32.8%).

Contrastingly, respondents correctly answered questions regarding open-area conversations (correct: n=129/146, 88.4%), a patient requesting a copy of their medical records (correct: n=131/147, 89.1%), and identifying a potential breach of HIPAA in a sample Instagram[®] post (correct: n=132/142, 96.6%). Table 2 includes the full knowledge assessment and frequencies of correct answers for the respondents.

Table 2. Knowledge Assessment

Questions (only complete knowledge assessment were included)	Correct Frequencies (%)
1. I am not allowed to respond to a text message as an athletic trainer from a student-athlete in regards to medical information, even if it is life threatening.	21/99 (21.2)
2. Which of the following law(s) primarily govern health record as a student health clinic as a college/university?	102/147 (69.4)
3. Are conversations in open areas among two medical professional that are overheard by a third party considered to be a HIPAA violation?	129/146 (88.4)
4. Does HIPAA apply to media and journalists who do not work for a covered entity?	75/147 (51.0)
5. Your place of employment utilizes a paper sign-in sheet and treatment log on the front counter of the Athletic Training Room for athletes that you work with to easily access their rehabilitation plan, as well as document who visited the clinic that day. Could be a potential HIPAA violation occur?	75/147 (51.0)
6. According to HIPAA, patients have the right to request a copy of their medical records on demand.	131/147 (89.1)
7. You are working on a medical documentation (including personal health information) on your personal laptop. Your supervisor has asked you to use a Google Drive to upload this information once completed. Unfortunately, you run out of time at clinical and tell your supervisor you will finish that evening. During your night class, your laptop was stolen from your dorm room. Your laptop lacked encryption but was password protected. Has a potential HIPAA violation occurred?	119/146 (81.5)
8. In addition to HIPAA, what law/act governs the electronic transmission of health information?	45/137 (32.8)

- | | |
|--|----------------|
| 9. Which of the following could lead to a potential HIPAA violation from the Facebook® post and comments below? Profile information for each of the accounts list school that they attend or place of employment. | 84/147 (57.1) |
| 10. Please read the sample Twitter® post below and indicate which of the following tweets could be a potential HIPAA violation. Select all that apply. | 95/147 (64.6) |
| 11. You are at your place of employment and decide to post a 10 second Snapchat® to your “story” for only your friends to see. Please indicate which of the following post(s) could be a potential HIPAA violation. Select all that apply. | 72/145 (49.7) |
| 12. You are at your place of employment and decide to post a photograph for your Instagram® account which is public. Please indicate which of the following post(s) could be a potential HIPAA violation. Select all that apply. Profile information for each of these accounts list the school that they attend in their bio. | 132/142 (96.6) |

7.7±1.9/13

Overall Knowledge Assessment Score (points and percentage)

(59.2±14.6%)

DISCUSSION

SoMe continues to be an outlet for Baby Boomers, Millennials, and Generation Z users to connect with each other, and to share and promote organizations.^{7,8} Medical facilities, including athletic training clinics, are not exempt from the same growth in SoMe usage. Clinicians have utilized the SoMe platform to announce treatment availability, market athletic programs at the institution, and promote the profession of athletic training. We are able to see that ATs in this study had an average of five active SoMe sites, thus engaging with the digital connectivity trends within the literature. The concerns about the professional presence of healthcare providers, specifically ATs, in SoMe comes in the form of inappropriate posting, commenting, and sharing of protected health information of their patients. Several respondents indicated they had one or more full-faced photographs of a patient on their SoMe accounts. While this percentage is low, the potential for HIPAA violations to occur from these posts can cause patient privacy concerns and/or extensive fines to the responsible covered entity.¹ There is a need to educate all healthcare providers in order to help minimize the amount of potential breaches to a patient’s privacy as technological advancements occur.

Respondents scored poorly on the knowledge assessment (7.7±1.9 out of 13, 59.2%) indicating a lack of adequate understanding of the rules and regulations the various laws enacted to protect PHI. Healthcare providers, including ATs, must be knowledgeable about governing acts such as HIPAA, FERPA, and HITECH. Risk mitigation techniques should be implemented to ensure not only the legal protection of the healthcare provider but ultimately for that of the patient. Respondents (n=136, 92.5%) stated that they have not reported someone for a breach of HIPAA, and have not been reported themselves (n=146, 99.3%). While we are unable to determine if the respondents in this study had witnessed or been involved with previous HIPAA or FERPA breaches, we believe it is necessary that ATs understand the role of reporting known violations. According to the NATA Code of Ethics⁹ and BOC Standards of Professional Practice¹⁰, ATs have a duty to report any provider that fails to uphold their professional obligation to these documents. In addition, a failure to report known violations from other clinicians is a failure to protect the protected health information of the patient and uphold the standards of the profession.

In aligning with the IOM core competencies, informatics and technology should be used to promote patient communication. It is critical that healthcare providers are ensuring safeguards are in place for the patient’s PHI.

Only 21.2% (n=21/99) of the respondents correctly answered the question concerning the ability to text message a patient indicating they believed that text message is an appropriate form of communication to patients. A majority of the respondents (n=75/147, 51%) believed that a paper sign-in sheet with PHI was an acceptable form of documentation, however, this medium allows potential HIPAA violations as there is no way to determine who is seeing the information. Athletic trainers and other healthcare providers should consider alternative routes such as having the patient sign into their electronic medical record profile to keep an accurate log of the patients seen each day.

Patients and healthcare providers have vastly different reasons for using electronic healthcare.¹¹ Patients overall prefer the anonymity that accompanies online health searches to provide additional advice and express their emotions.¹¹ An issue arises that although patients prefer online healthcare and SoMe, the potential of ethical standard violations, patient privacy breaches, and the misrepresentation of information on SoMe has created a fear of use from providers.¹¹ Healthcare providers valued being able to share the information they had learned and network with other healthcare professionals on SoMe.¹² Out of all of their health-related SoMe use, sharing of medical information accounted for 54% (out of 100%).¹¹ An alarming statistic was that the concern for privacy was at the very end of all of the precautions of medical SoMe use with only a 2.65/5 rating by healthcare professionals for overall concern.¹¹ All healthcare providers are discouraged from posting anything to common online platforms including SoMe.¹³ Previous research on medical students and residents identified that they experience a lapse of judgment when partaking in medical mission trips through posting pictures of their service on SoMe.¹⁴ The same concern may arise for ATs when they provide services to special events such as triathlons, tournaments, and Olympic qualifying meets. The recommendations to medical students,

residents, and physicians is that when opportunities arise to provide healthcare in unique and exciting locations, the utmost importance for ethical and legal practice including patient privacy must be respected.

In an effort to reduce the legal and ethical implications from a lack of knowledge identified in this study, we suggest that ATs establish policies to protect themselves and the clinic. While policies and procedures can help to mitigate risk, oftentimes healthcare facilities fail to address SoMe. Previous research has indicated that although ethics is covered in great detail, ethics concerning electronic means of communication is lacking in all healthcare professions.⁵ In the athletic training clinical setting, 42.9% ATs (n=63) reported that they had a SoMe policy for their work place and it was enforced to some extent. The presence and enforcement of a policy and procedure on SoMe for athletic training practice is vital to mitigate risk. The respondents in this study were predominately from a secondary school setting which comes with it the legal obligation of consent from the parent and assent from the minor to have their picture taken and posted to SoMe sites. Additionally, 17% of respondents (n=25) did not have nor believe they needed a SoMe policy. It is crucial ATs reduce the risk of violating one of the privacy acts by ensuring safe practices outside of non-injury situations through the creation of a SoMe policy to protect themselves and protect their patients from errors in judgement in terms of technology and SoMe.

LIMITATIONS

The limitation of this study was in reference to external validity. The sample from this study was limited to the responses that completed the entire tool. In survey research, partial data responses are typically included as respondents have the opportunity to not answer questions they do not wish. In order to assess the knowledge of the respondents, we decided to use completed surveys, as we were not able to determine if respondents chose not to answer because they did not wish to or were unsure of the answer. This is a threat to

external validity as the results from this study may not be generalizable to ATs as a whole. Secondly, the response rate and sample size are low in this study. We believe this could have been due to the fact that ATs may have been apprehensive to take part in a knowledge assessment focused on ethical and legal practice. Additionally, some ATs may not have a prior experience with SoMe and did not engage in the study as they were disinterested in the context and aims of the project.

CONCLUSIONS

Healthcare providers work directly with patients PHI daily. ATs on average scored poorly on the knowledge assessment of potential patient confidentiality breaches and governances of technology in healthcare. Similar to the core competencies, healthcare providers are not knowledgeable of how to implement best practice techniques for PHI to meet the needs of the American public.⁴ Since a knowledge gap has been identified, future research should focus on educational interventions to inform clinicians of best practice within technology and SoMe to protect the patient and protect themselves.

REFERENCES

- Centers for Disease Control and Prevention. HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services. *MMWR Morb Mortal Wkly Rep*. Vol 522003:1-17, 19.
- Kiel JM, Knoblauch LM, HIPAA and FERPA: competing or collaborating? *J Allied Health*. 2010;39(4):161E-165E.
- Knebel E, Greiner AC. *Health professional education: A bridge to quality*. National Academies Press; 2003. doi:<https://doi.org/10.1111/j.19451474.2004.tb00473.x>
- Bilimoria_NM. HIPAA Privacy/Security Rules: where we've been and where we are going. Updates from the HITECH Act to dramatically impact HIPAA privacy/security. *J Med Pract Manage*. 2009;25(3):149.
- Dyer KA. Ethical challenges of medicine and health on the Internet: a review. *J Med Internet Res*. 2001;3(2):e23.doi:<https://doi.org/10.2196/jmir.3.2.e23>
- Erickson MA, Martin M. Contributors to initial success on the national athletic trainers board of certification examination as perceived by candidate sponsors: a Delphi study. *J Athl Train*. 2000;35(2):134-138.
- Treem JW, Leonardi PM. Social media use in organization: Exploring the affordances of visibility, editability, persistence, and association. *Annals Intl Comm*.2013;36(1):143-189.doi:<https://doi.org/10.2139/ssrn.2129853>
- Chou W-YA, Hunt YM, Beckjord EB, Moser RP, Hesse BW. Social media use in United State: Implications for health communication. *J Med Internet Res*. 2009;11(4):e48.doi:<https://doi.org/10.1037/e521582014-115>
- NATA code of ethics. *National Athletic Trainers' Association*. 1995
- BOC standards of professional practice. Board of Certification, Inc. 2016:1-3.
- Antheunis ML, Tates K, Nieboer TE. Patients' and health professionals' use of social media in health care: Motives, barriers and expectations. *Patient Educ Couns*. 2013;92(3):426-431.doi:<https://doi.org/10.1016/j.pec.2013.06.020>
- Grajales Iii FJ, Sheps S, Ho K, Novak-Lauscher H, Eysenbacj G. Social media: A review and tutorial of applications in medicine and health care. *J Med Internet Res*.2014;16(2):e13.doi:<https://doi.org/10.2196/jmir.2912>
- Harder AL, Brown ED. Legal Briefs: Patient privacy and social media. *AANA J*. 2010;78(4).
- Thompson LA, Black E, Duff WP, Black NP, Saliba H, Dawson K. Protected health information on social networking sites: Ethical and legal considerations. *J Med Internet Res*. 2011;13(1):e8.298. doi:<https://doi.org/10.2196/jmir.1590>