UCIRVINE | INTERNAL AUDIT SERVICES

Social Media

Internal Audit Report No. I2019-209

July 1, 2019

Prepared By
Larry Wasan, Principal IT Auditor
Reviewed and Approved By
Mike Bathke, Director

UNIVERSITY OF CALIFORNIA, IRVINE

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO   SANTA BARBARA • SANTA CRUZ

INTERNAL AUDIT SERVICES
IRVINE, CALIFORNIA 92697-3625

July 1, 2019

BRIAN MICHAEL O'DEA
EXECUTIVE DIRECTOR
UCI HEALTH MARKETING & COMMUNICATIONS

MICHAEL J. STAMOS, MD
DEAN
UCI SCHOOL OF MEDICINE

Re: Social Media
No. I2019-209

Internal Audit Services has completed the review of the UC Irvine Medical Center and the School of Medicine's (SOM) management and administration of Social Media.

We extend our gratitude and appreciation to all personnel with whom we had contact while conducting our review. If you have any questions or require additional assistance, please do not hesitate to contact me.

Mike Bathke

Mike Bathke
Director
UC Irvine Internal Audit Services

Attachment

C: Audit Committee
Anne Warde, Manager, Communications and Public Relations, SOM

I. MANAGEMENT SUMMARY

In accordance with the fiscal year (FY) 2018-2019 audit plan, Internal Audit Services (IAS) reviewed the management and administration of social media for the UC Irvine Medical Center (the Medical Center) and the SOM. While basic internal control activities were noted by IAS, the review identified opportunities for improvement to minimize business risks and ensure compliance with the Medical Center and the SOM's policies and procedures, government regulations, and/or best business practices. The following observations were noted.

Social Media Strategy – The Medical Center and the SOM did not have a documented social media strategy, and therefore, IAS was unable to verify that social media strategies were in alignment with business objectives. This observation is discussed in section V.1.

Policies and Procedures – While various parts of the Medical Center's social media policies and procedures are still relevant, the document has not been reviewed and updated since June 2010. Additionally, social media accounts were started by other units/departments without prior approval from the Medical Center and the SOM's Marketing and Communications Departments, violating social media policy and guidelines. These observations are discussed in section V.2.

Social Media Monitoring – Monitoring of social media posts, comments, and reviews are performed manually as opposed to using the automated features of social media monitoring tools. This observation is discussed in section V.3.

Incident Response - A detailed and documented social media incident response protocol has not been created, and negative reviews about the Medical Center on a major review platform have not received appropriate responses from social media administrators. These observations are discussed in section V.4.

Regulatory Compliance – Positive reviews of the SOM by UCI staff were posted on the SOM's Facebook page without conspicuously stating their relationship to UCI, violating a federal regulation on endorsements. This observation is discussed in section V.5.

Information Security – IAS noted the following observations with regard to access management for various social media accounts: use of shared username and passwords; use of a generic username; two-factor authentication not enabled; and a vendor with access did not have a signed Business Associate Agreement (BAA). These observations are discussed in section V.6.

II. BACKGROUND

Social Media refers to the use of websites and mobile applications, both by individuals and organizations, as tools for communication and socialization through the posting of articles, photos/videos, comments, and reviews. Major social media platforms include Facebook, Twitter, YouTube, LinkedIn, and Instagram. Yelp is a review website that can also be considered as social media.

Due to the popularity of social media, with Facebook alone having 2.3 billion users globally and 169.5 million users within the United States, it is no longer a question of whether or not an organization should participate in social media, but rather, how they can best leverage this medium to improve communication, foster customer relationships, and increase their bottom line, while also managing risks. Currently, there are over 18,000 users who are following the Medical Center's Facebook account, and there are 3,400 users who are following the SOM's Facebook account.

Management of the various Medical Center and SOM social media accounts is decentralized. The Medical Center's social media accounts are managed by one full-time employee in the Marketing and Communications Department, which recently began reporting to the University's Strategic Communications Department. Management of the SOM's social media accounts are managed by the Marketing and Communications Coordinator as part of her overall duties. Many individual departmental social media accounts within the Medical Center and the SOM are independently managed by their corresponding departments.

III. PURPOSE, SCOPE AND OBJECTIVES

The purpose of the audit was to determine whether policies, practices and procedures provide reasonable assurance to safeguard the University from social media risks, such as posting of Protected Health Information (PHI) and/or Personally Identifiable Information (PII), inappropriate comments, unmonitored negative public comments, and information security exposures resulting from hacking, phishing, and social engineering. The audit scope included a review of social media policies, procedures, and guidelines followed by the Medical Center as well as the SOM. It also included management interviews and a limited review of posts, comments, and reviews on the most popular social media accounts, including Facebook, Instagram, Twitter, Pinterest, and Yelp, during a one-year period ending February 28, 2019 (see page 9).

The following audit objectives were included in the review.

1. Verify the existence of a social media strategy and verify alignment with the Medical Center and the SOM's business goals and objectives.

2. Review social media policies, procedures, and guidelines, and verify that it includes key information to protect the Medical Center and the SOM from various social media risks. Verify compliance with such policies, procedures, and guidelines.

3. Verify that adequate monitoring of posts, comments, and reviews are performed to ensure regulatory compliance and to prevent negative publicity and reputational harm to UCI.

4. Verify the existence and adequacy of a social media incident response protocol.

5. Assess the effectiveness of social media access management and cybersecurity controls, and verify the existence of a spear phishing awareness campaign.

IV. CONCLUSION

Basic social media internal controls, including the monitoring of posts, comments, and reviews are being performed by the Medical Center and the SOM's social media administrators, and policies to protect confidential information are in place. However, opportunities for improvement and concerns were noted regarding social media strategy, policies and procedures, monitoring and response, access management, and regulatory compliance.

Observation details were discussed with management who formulated action plans to address the issues. These details are presented below.

V. OBSERVATIONS AND MANAGEMENT ACTION PLANS

1. Social Media Strategy

Observation

Interviews with the Medical Center and the SOM's management and staff, who are responsible for managing their respective social media accounts, confirmed that there is no formalized and documented social media strategy. Medical Center social media efforts are currently driven by service line marketing plans and the medical center's overall content marketing focus. SOM efforts are driven by academic and research needs. Without a clearly documented and well-planned social media strategy, there is a risk of performing activities that are inefficient, ineffective, and/or inconsistent with the Medical Center and the SOM's business goals and objectives. Due to a lack of documentation, IAS was unable to verify that strategies were indeed in alignment with business goals and objectives.

Management Action Plan

Medical Center

By September 30, 2019, management will produce a social media strategy that is aligned with the medical center's business goals and objectives.

School of Medicine

By September 30, 2019, management will produce a social media strategy that is aligned with SOM's business goals and objectives.

2. Social Media Policies and Procedures

Observation

- **Policies and Procedures Updates** – Although a UCI Health social networking policy for employees is available and covers important privacy issues, such as those related to the Health Insurance Portability and Accountability Act (HIPAA), it is dated June 2010. With a rapidly evolving world of social media and internet technology, it is important to review policies and procedures regularly and update it as necessary to keep pace with emerging risks.

- **Social Media Account Review and Approval** - Management responsible for the Medical Center and the SOM's social media are not aware of all the social media accounts that have been created by other units and departments. According to social media policy, social media accounts "must also be reviewed and approved for site content and appropriateness of material by the Public Relations and Media Relations Departments." The "Getting Started" social media guideline also states that, "When you create social media identities that are a part of UC Irvine Healthcare or UC Irvine SOM, please notify Marketing & Communications. This is required to ensure accountability as well as cross-promotion."

  However, according to management, a majority of the time, they are not contacted for approval prior to the creation of new social media accounts. IAS performed a limited Facebook search for UC Irvine Health and SOM social media accounts and found accounts which Marketing and Communications were not aware. IAS noted the following.

  - Fourteen Facebook accounts were found of which Marketing management were not aware. Six belong to Medical Center departments and eight belong to SOM departments.

- Four of the 14 accounts were inactive for more than six months but had not been deactivated per the social media "Maintain and Monitor" guidelines. One belongs to the Medical Center and three belong to SOM.

- Sixteen Facebook accounts did not have UCI Health's Social Media Participation Guidelines or a link to the document posted on the pages, as required by the social media "Best Practices" guidelines. The Participation Guideline informs visitors to the Medical Center and the SOM social media accounts of UCI Health's policy on posts/comments that are inappropriate, including the posting of PHI, language that is obscene or defamatory, libelous material, and others. Although all social media participants are bound by the terms and conditions of each social media platform, not making visitors aware of UCI Health's specific policies increases the risk of inappropriate content, potentially resulting in non-compliance with regulations, legal exposure, and/or reputational damage to UCI.

Note: The above statistics are a result of a limited search, and it was conducted only on Facebook, which is the most popular social media platform.

Management Action Plan

Medical Center

- The Public Relations Team has been working with Compliance to update our social media policy. We will also work with Compliance to determine an appropriate timeframe for regularly reviewing the policy to ensure that it is up to date.

- Additionally, management found multiple Social Media Policies available on different sites (a compliance owned policy available via the intranet site, a second policy available on the Health Sciences Website, etc.). The most recent had expired in January 2018. We will work with Compliance to create a single policy that applies to all. We will also explore the feasibility of a centralized database to avoid confusion and reduce duplicated work.

- Marketing can commit to conducting periodic searches for rogue accounts, likely on a quarterly basis, as current staffing does not allow for greater frequency. We will also work with Compliance to establish and document a process for decommissioning accounts that do not positively reflect on UCI Health and determining management awareness of such behavior.

- Marketing will work with Compliance to ensure that staff members are made aware of the social media policies, procedures, and guidelines.

- All of the above will be completed by September 30, 2019.

School of Medicine

- SOM is in the process of developing a new intranet site specifically designed to meet the needs of SOM faculty and staff, primarily located on the Irvine campus. Included in the plan is a communications resource page which will include guidelines for establishing social media accounts. We anticipate the new intranet will be launched by summer 2020. Currently the SOM communications staff conducts periodic searches and has collected links to accounts once we have been made aware. We can implement a more formal quarterly review and decommissioning plan, in line with UCI Health, by September 30, 2019.

- We will work with UCI Health Marketing and Communications as well as Compliance to update the social media guidelines so that they apply to both UCI Health and SOM as well as direct individuals, who are looking to create a new social media account, to the appropriate department for notification. We will also work together to ensure that staff members are made aware of the social media policies, procedures, and guidelines.

3. Social Media Monitoring

Observation

Automated Keyword Monitoring - Management responsible for the Medical Center and the SOM's social media are performing basic monitoring of posts, comments, and reviews. However, automated tools for more advanced monitoring are not being utilized. Although the Medical Center and the SOM each have an account to a popular social media monitoring application called Hootsuite, IAS found that social media administrators were not using this application's automated keyword monitoring capabilities. Due to the large potential reach of social media and the speed in which negative information can spread, it is important for management to have a method for effectively and efficiently monitoring discussions about the Medical Center and the SOM in order to prevent negative and/or inappropriate posts from becoming a major issue and causing serious reputational, regulatory, and legal harm to the University.

Management Action Plan

Medical Center

We are exploring the monitoring capabilities Hootsuite offers, and by September 30, 2019, we will decide on whether or not to use Hootsuite or another solution.

School of Medicine

We are currently monitoring daily and will explore utilizing Hootsuite or other free applications to enhance monitoring effectiveness. We will determine which tool is most suitable by September 30, 2019.

4. Incident Response Protocol

Observation

- Management who are responsible for the Medical Center and the SOM's social media accounts confirmed that there are no documented social media response protocols. In addition to active monitoring of social media posts and comments, it is a best business practice to have a well-documented and coordinated social media response protocol in order to quickly respond to negative comments before they spread and become a major news story, resulting in reputational damage to UCI. A social media response protocol should include, among others, policies and procedures for responding to a social media incident, a flowchart of actions to be taken based on the topic and scenario, and a list of subject matter experts who can quickly be contacted for consultation or to provide appropriate responses to given incidents.

- Major Medical Center and SOM social media accounts, including Facebook and Yelp, a popular consumer review website, were analyzed during a one year period ending February 28, 2019, to determine if negative comments or reviews were provided with appropriate responses by social media administrators. IAS found 45 negative reviews of the Medical Center on Yelp, and none of the 45 received a response from social media administrators.

  With an appropriate response, the effect of some negative reviews can be minimized. By contrast, not providing an appropriate response can allow negative feelings to fester and give the impression that the Medical Center does not care about its patients and their concerns, which goes against one of the main reasons for social media, which is to build relationships with patients, their families, and the community at large.

Management Action Plan

Medical Center

We are collaborating with our Patient Experience department to formulate a response protocol involving staff from the area/department about which the comment was made. We can produce a flowchart of the current process, including the names and contact information of subject matter experts that can assist in providing a response to incidents, by September 30, 2019.

School of Medicine

We review comments daily and forward concerns to the appropriate department for review. We follow UCI social media guidelines regarding actions taken related to inappropriate posts and negative comments. We will include documentation of this process in our strategy report which is scheduled to be completed by September 30, 2019.

5. Regulatory Compliance

Observation

Four positive reviews on the SOM Facebook account were posted by UCI employees, but the employees did not conspicuously disclose their relationship to UCI, as required by federal regulations. According to the Code of Federal Regulations (16 CFR Part 255), when employees endorse a product or service, regardless of the medium (including social media), they must conspicuously disclose their relationship to the organization.

Management Action Plan

School of Medicine

We have made individuals aware that their relationship to UCI must be disclosed and this guideline is included in the social media policy posted on SOM's Facebook page. Although it can be difficult to identify all individuals who leave comments, we will do our best to continue to monitor for employee posts.

6. Information Security

Observation

During management interviews and a walkthrough of both Medical Center and SOM social media account access, IAS noted the following observations:

- **Shared Login** – Some social media accounts have one username and password that are shared by all who have access. With shared login, it is difficult to determine who made changes or posted a comment or photo, and therefore difficult to hold anyone accountable if or when inappropriate content is posted or unauthorized changes are made.

- **Generic Username –** The Medical Center's YouTube account has a generic account with a username that is not attributable to any one individual. Consequently, similar to a shared login, this login information can be used to log into the account to upload inappropriate content, and it might be difficult to hold a specific individual accountable for such uploads.

- **Two-Factor Authentication** - Although the major social media platforms are capable of Two-factor Authentication during login, this functionality was not enabled on the various Medical Center and SOM accounts. Two-Factor Authentication requires anyone who is logging in with an unrecognized device to provide additional authentication using a code number sent to a known cell phone number, in addition to using a username and password. This prevents unauthorized individuals from hijacking an account, posing as an official UCI staff, and posting inappropriate comments, posts, or photos, potentially causing serious reputational damage to the organization.

- **Business Associate Agreement -** A marketing consultant called MedTouch had access to the Medical Center's Facebook account and management stated that it was a trusted vendor with a signed Business Associate Agreement (BAA). However, when IAS requested a copy of the BAA, management discovered that there was no signed Master Service Agreement and no signed BAA. Although UCI has a policy which prohibits the posting of PHI or any confidential information to social media sites, it is good business practice to have vendors with access to restricted accounts to sign a BAA. Not having a BAA agreement with a vendor who has access to restricted accounts does not ensure that the vendor has a documented understanding of their responsibilities under the law (e.g. HIPAA) in terms of protecting sensitive data, and it does not hold such vendor accountable for any breaches that may occur due to their access. IAS notes that management had MedTouch sign a BAA agreement immediately after they discovered that they did not have one.

Management Action Plan

Medical Center

We will transition to individual login credentials, and although several platforms do not support multiple users/passwords, we have found a way to use Hootsuite to access the platforms, and it will support unique users/passwords. Two-factor authentication has been enabled where possible (Instagram, Twitter, YouTube, etc.).

Although MedTouch does not post to our social media platforms, we are in the process of renewing their BAA. Additionally, we are sunsetting our social media relationship with MedTouch.

School of Medicine

We are using individual login credentials and will immediately implement two-factor authentication where possible. We will note in our strategy document the necessity of a master service agreement and BAA in the event that we collaborate with an outside vendor in the future. We have no BAAs in place at this time.