COSMOS
Navigate the Compliance Universe

Compliance Today - October 2021
Partnering marketing and privacy to develop a proactive privacy program

By Lisa Taylor, JD, CCEP, and Daniel S. Elmlinger, MHSA, CHPC

Lisa Taylor (lisa.taylor@uchealth.com) is Vice President & Chief Compliance Officer, and **Daniel S. Elmlinger** (daniel.elmlinger@uchealth.com) is Compliance Operations Analyst at UC Health in Cincinnati, OH.

- linkedin.com/in/lisa-taylor-5b0b404/
- linkedin.com/in/danielelmlinger/

Privacy programs need to take the pulse on what is going on in their organizations, but some programs may struggle to keep up with their organizations' initiatives. Put simply, there is a limited number of people in privacy programs (sometimes only one person or a fraction of a full-time equivalent) but a multitude of information and ideas being exchanged across the organization. Sometimes privacy may get pulled into an idea or issue too late, or sometimes not until after a decision has been made, and then weeks, months, or maybe even years of work and procedures must be undone in order to safeguard patients' privacy. Every privacy professional dreads this moment, but every privacy professional can likely remember at least one incident like this. Short of approval to hire as many members onto your team as you would like, the next best solution is to proactively partner with teams in your organization. This partnership will help encourage a culture of compliance in your organization, one team at a time. One of the best teams to work with in your organization is the marketing & communications team.

This article will provide tips and suggestions to leverage your organization's marketing and communications (marketing) department to help develop a more proactive privacy program. This leverage comes from:

1. More efficient social media monitoring for possible HIPAA issues;
2. Risk-specific training and development with your workforce;
3. Better communication about your privacy program and what it does;
4. Compliance with the Breach Notification Rule in case the worst happens at your organization; and most importantly,
5. Stronger safeguards for some of your organization's high-profile patients.

First things first

Before implementing these tips and suggestions, privacy programs should examine the relationships they have with their marketing teams.

Privacy leaders:

- Do you know your organization's marketing leader(s)?

- Do you meet with your marketing leader(s) regularly?
- What is the context in which you meet with your marketing leader(s)?
- What do you discuss with your marketing leader(s)?

Privacy operations staff:

- Do you have contacts on the marketing team to help you with day-to-day issues?
- Does the social media team within marketing know what to do if they see a HIPAA issue online?
- Does the social media team know what they can say on social media when a person identifies themself as a patient on a public page?
- Do the copywriters, photographers, and videographers know when they need to ask you to review content before publication?

If the answer to any of the above questions is "No," or anything indicating a potential for a stronger relationship between your two teams, start working on the relationship.

Leader-to-leader relationship development

As the privacy leader for your organization, you should evaluate if you have an effective relationship with your marketing leader(s). If you do not have one, then establish one. Initiate the relationship by asking for some brief one-on-one time, and frame it as seeking to better understand what their team does, what your team does, and how the two of you can work together for the betterment of the organization. This can be a cup-of-coffee discussion, lunch, or a formal meeting—whatever you and marketing prefer. Once you have level-set with the leader, agree on recurring meetings between the two of you to check in and see if there is anything privacy can help marketing with, or vice versa.

Marketing often has a pulse on the rest of the organization and upcoming strategic initiatives, which, when appropriate, can be shared with privacy. Conversely, privacy can offer personalized training to marketing, such as when an activity is or is not considered marketing under HIPAA, when an authorization is needed, or whom to contact on the team for a specific issue. This relationship between leaders will facilitate the staff-to-staff relationship development discussed next.

Staff-to-staff relationship development

Once the privacy leader has established a relationship with the marketing leader(s), ask for a meeting between the two teams. This informal setting can be a 30-minute virtual or in-person meeting (as COVID-19 precautions allow) so that the operational staff on both teams can better understand what the other does. For example, a marketing team may have a group that only produces internal communications, only external communications, only media relations, or only social media content.

Once both teams understand what the other does, find out how privacy can help marketing and how marketing can help privacy. The privacy team could put together a quick reference document for the marketing team to use when creating new content. This document could include reminders such as "PHI includes anything reidentifiable, including tattoos or body modifications," or answer questions like "When do I need an authorization from a patient?" The key in a successful staff-to-staff relationship is both sides asking, "What can I do to help you?" Not only will this help your privacy program, but it will also contribute to your organization's overall culture of teamwork and culture of compliance.

Leveraging the relationship

Developing and maintaining a relationship is just one of many steps your privacy program can take to move from a reactive program to a proactive program. While a strong relationship with other departments in your organization will always bring your program benefits, the following are five ways that you can leverage your relationship with marketing specifically to improve your privacy program.

More efficient social media monitoring for HIPAA violations

Social media can be a low-hanging fruit in a privacy program's move to proactive work. Note, this discussion about social media is limited only to HIPAA-questionable content. It is not the privacy program's responsibility to monitor and determine professionalism of an employee's social media presence.

COVID-19 has changed healthcare in many ways, one of which has been an increased use of social media by healthcare professionals to show what it is like to be on the frontlines of a pandemic.[1] These users likely make these posts with the best of intentions, whether it is advocacy or education, but what the users sometimes forget is that HIPAA protects more than just the "obvious" information. Marketing can help monitor social media for these questionable posts when employees tag the organization or check in to work, because if done correctly, the individual(s) running the organization's account receive a notification. At that point, marketing knows right away if someone has posted a picture that may contain a patient in the background, made a comment about a procedure they did that day, or anything else that could border the fine line between breach and nonbreach. By having a strong interdepartmental relationship, marketing will know to immediately notify privacy of the issue so that privacy can make a determination of whether there is a breach.

Another way that marketing can help with proactive social media monitoring is by watching the comments of the posts under the organization's pages. Oftentimes, patients may want to share how grateful they are to have received care from the organization, sometimes going so far as to share the name of their aide, nurse, pharmacist, or physician in a comment on a post the organization makes. The patient is free to share this as much as they want, but the issue will come from the organization's response confirming the treatment relationship, or from the previously named employee responding and thanking the commenter for their gratitude. Why? Because protected health information includes any information that relates to an individual's past, present, or future mental/physical health, provision of healthcare, or payment for the individual's care. Many employees of covered entities find this shocking, but it is true. And confirming a patient's treatment relationship exposes your organization to fines from the Department of Health & Human Services Office for Civil Rights.[2] If your marketing team knows to watch for comments that confirm a treatment relationship, they can quickly hide or delete the comment and notify your privacy team so that appropriate coaching and training can occur with the employee who made the comment.

Risk-specific training and development with your workforce

One of the elements of an effective compliance program is conducting training and education. If your training and education program is computer-based, your marketing team can also help you with this. Marketing can provide you with branded presentation templates, help you communicate to the organization your training window, and even help you put together some of the content.

At UC Health, we used our marketing team to help us film short videos that we incorporated into our training. These videos included scenarios such as a patient asking for his after-visit summary and the employee retrieving it from the printer and another employee answering a phone, searching for the patient on the phone, and asking for multiple identifiers to confirm she had the correct patient's record open before disclosing information or

changing anything in the record. We chose these scenarios because we determined these two issues to be our biggest risk areas based on the previous year's reported incidents. These scenarios could be described with text and presentation slides, but marketing helped us develop our training to replicate real scenarios that our clinical employees find themselves in every day and show what the right thing is to do each time.

An added bonus will also come to your general compliance (not privacy) team. The relationship between privacy and marketing will allow compliance to develop a similar relationship. Compliance can provide ongoing trainings to marketing about the Anti-Kickback Statute, Civil Monetary Penalties Law, Stark Law, and other fraud and abuse laws to assist in identification of any issues when someone approaches marketing about an idea and wants to offer something that may be an issue according to one of these laws or regulations. Once the department knows how to identify an issue, they will contact the compliance department when they see any possible problems prior to encountering them.

Better communication about your privacy program and what it does

Many privacy programs are known as the "HIPAA police," or some variation of the phrase, in their organizations. For better or for worse, many individuals in your organization may assume that you and your team only exist to respond to incidents. Your marketing team can help you change that perception so that your organization knows that you are also available to help proactively.

If your organization has an internal communication tool or process, ask your marketing team if they would be willing to include your privacy team in a communication that goes out to the organization. This could be an opportunity to publish to your whole organization what exactly you do and how you can help everyone do their job without worrying whether something is a HIPAA violation. Alternatively, this communication can address a large risk in your organization. For example, if your organization has a policy that forbids an employee from accessing their own electronic medical record (or other record system), and your privacy program notices an uptick in individuals still accessing their own records, marketing can help you push out a reminder to everyone about the institutional policy. As your privacy program becomes more visible in your organization, it will become easier to move from a reactive program to a proactive program.

Compliance with the Breach Notification Rule in case the worst happens at your organization

As the HIPAA Breach Notification Rule requires, "covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are…required to provide notice to prominent media outlets serving the State or jurisdiction."[3] For many covered entities, if it has not already happened, it is only a matter of time until a breach happens that requires media notice. Privacy programs should plan now, not when trying to create their response and notification to the Office for Civil Rights, how to handle media notice.

Your marketing team may have contacts at your local media outlets or may know how to get in touch with the outlets. Marketing can also help you draft the news release that will go to the media outlets. Marketing can help you draft a brief but clear news release that complies with the requirements in the Breach Notification Rule. Additionally, your marketing team may be able to help you field any media calls your organization gets about the breach, although your organization may have a policy about speaking to media.

Stronger safeguards for some of your organization's high-profile patients

While this may seem like an issue that only applies to large hospitals, trauma centers, or academic medical centers, it can also apply to community hospitals and smaller providers. When a significant event happens, such

as a mass casualty, sporting event injury, car accident that shuts down the interstate, or other event that can create an attention-grabbing headline, marketing can quickly become privacy's right hand. Or, for less tragic situations, if a VIP is in your facility for routine care, this same process can apply, and marketing can help privacy ensure that the patient's privacy is always being protected.

The news will likely report where the patient has gone for treatment. Your marketing team may have contacts with most or all the local news organizations and will field questions or requests for comments from the outlets. For large events that have everyone's attention, such as a major league athlete being injured during a match, it will be obvious to privacy that they need to actively monitor that athlete's electronic medical record for snooping or other inappropriate uses/disclosures.

But for incidents that may not seem as obvious, if marketing receives multiple calls or requests for comments from news organizations about a patient reportedly at your facility, your marketing team can tip off your privacy team that the patient may need to be considered high-profile/VIP, activating your internal policy on safeguarding their records.

At UC Health, we have established a standard operating procedure for what we call "media events." A media event is any situation in the local or national news media that involves patients at any of our facilities. Because of our relationship with our marketing team, our media relations director will notify the chief privacy officer whenever there are multiple requests for a statement about a patient in our care. The chief privacy officer will then work with the registration team to ensure that the patient is marked as confidential, add our electronic medical record system's added security feature ("Break the Glass") to the patient's record, and if the patient has not arrived yet, ensure that they will arrive under an alias. At that time, privacy and information security conduct regular auditing and monitoring of access to the patient's electronic medical record to ensure that no snooping occurs, or if it seems that snooping has occurred, then activate the standard investigation process. In practice, this has helped privacy ensure that individuals' HIPAA rights are protected despite the news media sharing information it obtains from other sources.

Making it happen

Before your organization can recognize the benefits of a privacy/marketing collaboration, the two teams have to learn how to work well together. Privacy programs that want to grow from reactive to proactive should start doing so by reaching out to their organization's marketing team and developing the relationship. Once these programs have established the relationship with marketing, they should maintain the relationship. This collaborative relationship will benefit the organization and, at the end of the day, the patients and clients that the organization serves.

Takeaways

- Marketing can be a valuable partner to your privacy program.
- Marketing can play a key role in protecting patients' privacy.
- Collaborating with your marketing team can help your program grow to be more proactive.
- Your organization can develop a standard operating procedure for high-profile patients with marketing as a stakeholder.
- A relationship with marketing will allow privacy and compliance to provide more specific and thorough training on relevant rules and regulations.

1 Nina Youngstrom, "Magnified by COVID-19, Social Media Posts Risk HIPAA Violations, Allegations of Abuse," *Report on Medicare Compliance* 30, no. 6 (February 15, 2021), https://bit.ly/3iRZvI4.
2 U.S. Department of Health & Human Services, "Dental Practice Pays $10,000 to Settle Social Media Disclosures of Patients' Protected Health Information," news release, October 2, 2019, https://bit.ly/3ARmYiA.
3 "Breach Notification Rule," Office for Civil Rights, U.S. Department of Health & Human Services, last reviewed July 26, 2013, http://bit.ly/2LaoCnh.