227268 How to use media and social networking effectively in public health settings

Jill Herzog, Senior Associate, Booz Allen Hamilton

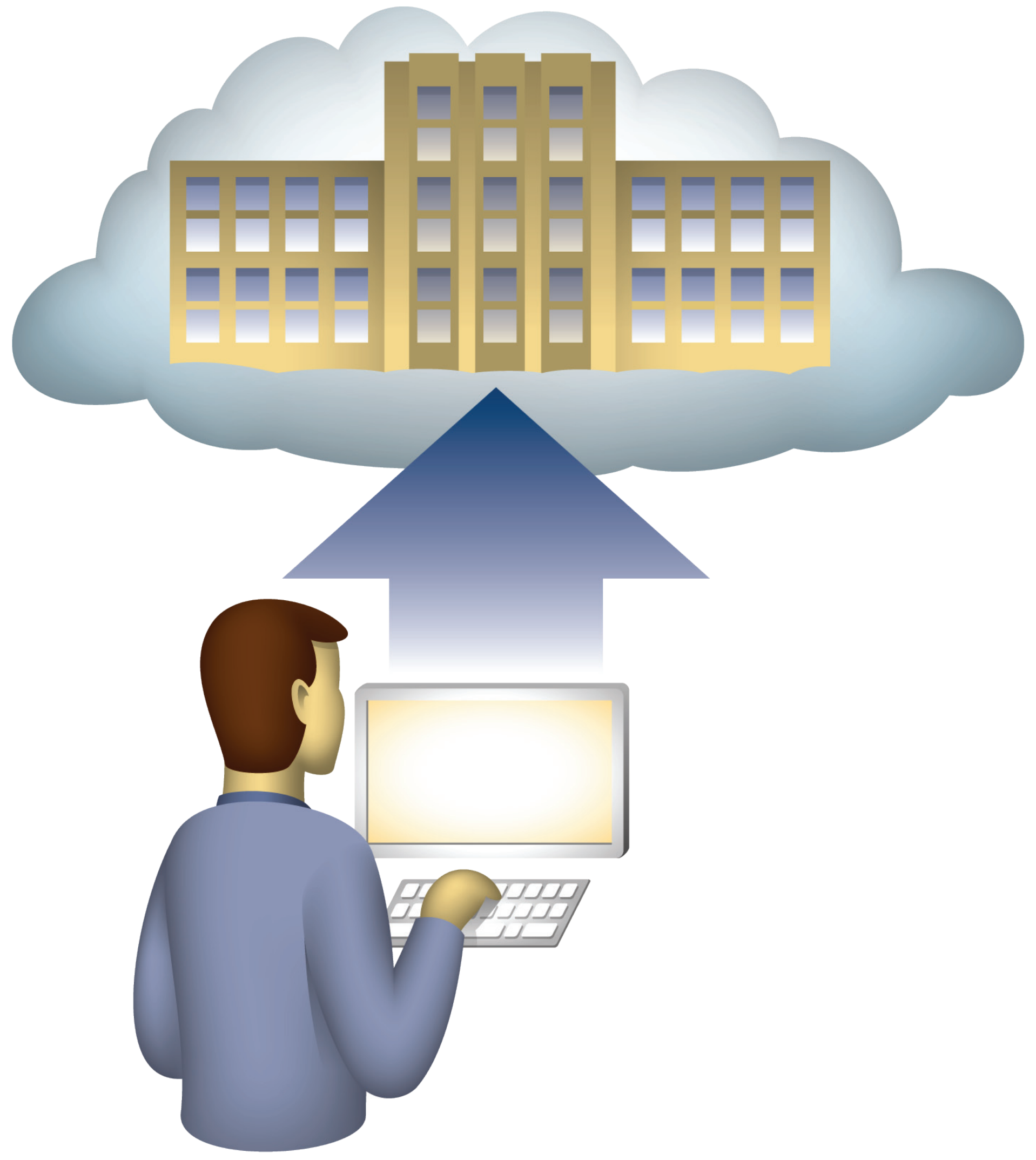
Purpose

Increasingly, social media is playing a critical role in health programs, including those related to outreach, education and intervention. Implementing these new, public technologies is not always easy. Policies related to acceptable sharing and handling of information must be carefully crafted and conveyed to users, both internal and external, as such data may contain Protected Health Information (PHI).

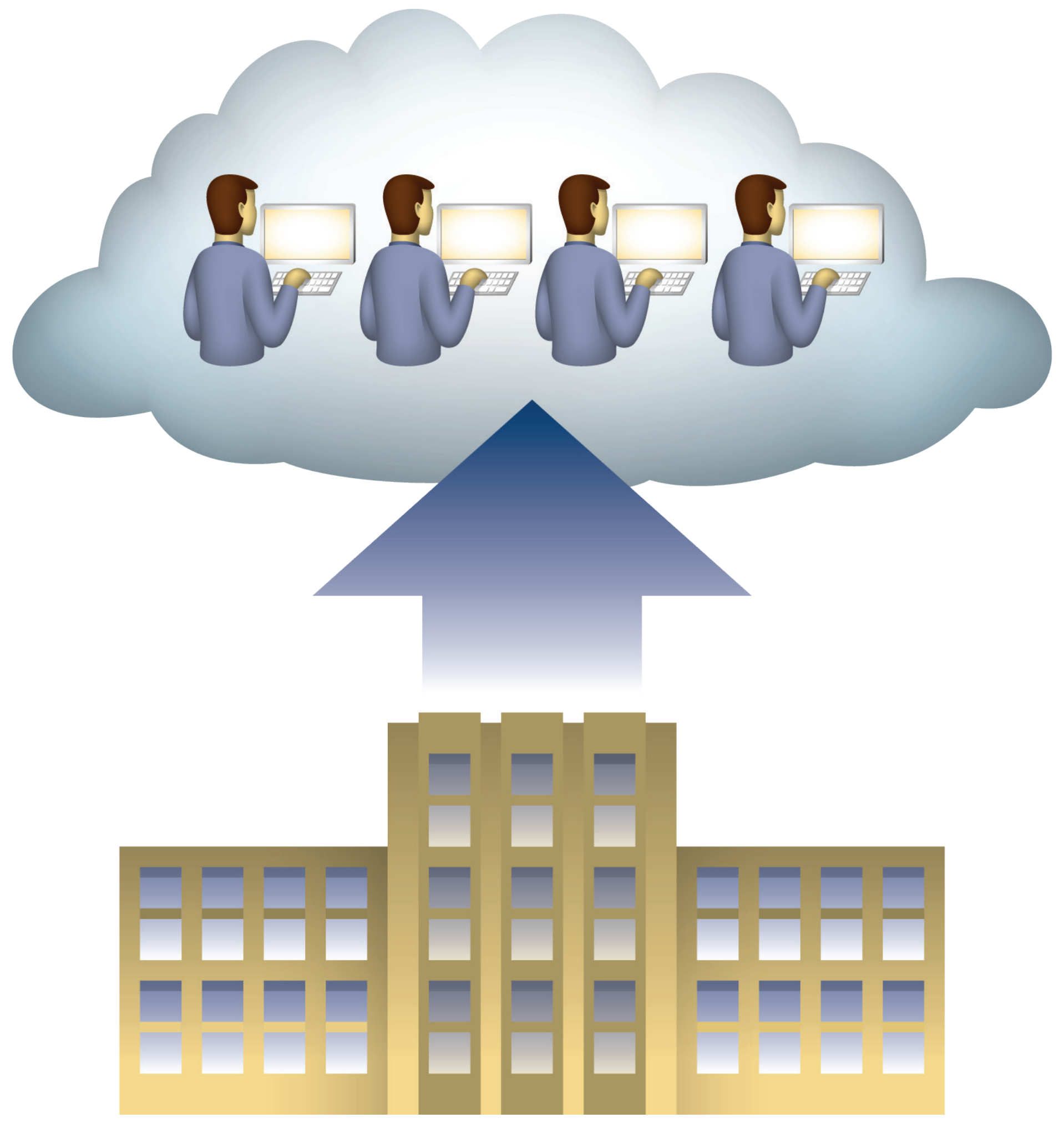
Background

Social media and networking sites are integrating themselves into many aspects of modern life, including health care. Social media has great connecting power; it can draw people together and allow for broader collaboration. Within the healthcare arena, social media and networking sites will help promote collaboration between patients and the rest of the medical industry. This collaboration is embodied by a key social media tenant: information sharing. When an organization engages the public, inviting it's feedback, two types of information sharing exist.

INBOUND SHARING: Allows organizations to obtain input from patients. This includes gauging public sentiment, obtaining input on current issues, providing an alternate customer service communications method and more.



OUTBOUND SHARING: Allows organizations to communicate with and/or empower their patients. This could include disseminating critical health information quickly, conducting awareness campaigns, and delivering other messages to patients/customers.



Outbound sharing is easy to control through policies, access restrictions, management oversight, and technical controls. Inbound sharing, however, is difficult to control. Despite numerous warnings about identity theft, medical identity theft, or general physical safety, people still share intimate and sensitive details about their life. This is especially true when people are looking for medical assistance they have not been able to find or that has been denied.

Handling this information in an appropriate manner is critical to the security and privacy of an organization's customers and patients.

Security Safeguards

The recommendations below provide a starting point for your organization to implement a secure social media experience.

- Conduct a security assessment on any social media platform that the organization intends to use. Is this service a potential vector for malware and viruses? Hint: all social media and networking sites are malware threat vectors.
- Perform proper due diligence. When you use these services, you agree to a Terms of Service. Can you legally sign that ToS for your organization? Does the ToS apply to your organization? Does it break and legal protection? Who owns the data that is shared and discussed on the social media platform? Where does the data reside? Involve legal counsel immediately.
- Update IT security policies. Ensure that your organization's IT security policies define clear requirements, roles and responsibilities for those using social media. For example, if your organization's IT assets require a 15+ digit pass phrase, create a policy that requires that on social media sites as well.
- Physical or logical separation of networks. As mentioned above, social media and networking platforms are large vectors for malware. Would the computer being used to update a Facebook, Twitter or other social media/networking site be on the same network as your patient data? Physically or logically separate networks to ensure a malware infection would not spread to your critical systems and data.
- Create information handling policies. Employees must know how to handle the inbound information shared from the public. For example, if someone shares PHI on your organization's Facebook page, should it be deleted? Would a record need to be kept of that deletion? Would it fall under an accounting of PHI disclosure? These questions must be answered by organizational leadership to ensure proper policies are in place to protect the organization and patient.

Privacy Protections

The recommendations below provide a starting point for your organization to implement a social media experience that bolsters patient privacy.

- Plain language privacy notices. Notices should appear on all third-party social media and networking sites. These notices should state a clear purpose, how information will be used, and whom to contact if a problem arises. Provide notice to users about acceptable use of the social media platform, including what information should not be shared (PHI or sensitive PII such as SSN, DOB, etc). If space is limited, link back to the official organization privacy policy.
- Updated privacy policies. Ensure that each third-party service is evaluated and added to the organization's privacy policy. Be honest with your customers/patients about your use of their information. Do not bury them in legalese. Inform patients/customers on uses of data obtained through third-party social media and networking services. Privacy policies should be posted on your organizations website and be accessible on every page.
- Ensure commenting policies are fair, legal and documented. If your organization wishes to moderate comments on a particular social networking site, ensure your commenting policies are available for review. For those moderating the comments, ensure there is a documented "test" that would be met for a comment to be deleted or published. For comments that are deleted, document how it failed the test.
- Make information available. Do not only publish information via social networking sites. A customer/patient should be able to find the same information on both a social networking site and the company's official website.

Conclusions

Social media and networking sites are an excellent outreach tool. However, organizations must be mindful of the security and privacy risks that are inadvertently created by using these sites. A site that encourages individuals to share will always draw individuals who wish to share too much. Each organization that uses these services has a responsibility to provide a secure, privacy-protected environment to the best of its ability. Due diligence, clear and actionable policies, and proper management oversight will ensure a safe and successful experience.