Patient Portals: Open Doors or Trap Doors?

5.18.2016

The desire by physicians and others to leverage their services and those of their staff as well as the consumer demand for greater access to have information about their health is leading the **push** for patient portals. This push is coming from many sources: patients, health care providers, insurers and regulators. Patient portals include any type of secure online website that provides access to health information or health care professionals from anywhere using an Internet connection. Patient portals can provide any number of benefits including by example, better patient-provider communication, improved workflow, benefits and coverage, making payments, a customized patient engagement and experience, self-service care, remote management of care, behavior changing preventative care and chronic care management, improved quality, meeting various "meaningful use" incentive requirements, research, coordination of care across providers and many other benefits.

The implementation and dissemination of patient portals must overcome the **push back** from various sources. The push back occurs because of the need to achieve security and privacy and the need to comply with HIPAA and state privacy and security regulations and address privacy breaches. Also, providers need to be mindful of inadvertently establishing a physician/patient relationship online, committing malpractice by omission or action in online communications, committing fraud or abuse by promising things of value to induce referrals, or violating state licensing laws by providing medical advice across state lines in which they are not licensed and for which a protocol has not been established.

Patient portals are becoming essential component of a modern, successful, flexible healthcare industry business model. Whether implementing new website, or fine tuning or enhancing the features of a portal already in existence, providers and others

Related Services

Cybersecurity and Privacy Specialty Team

E-Discovery Specialty Team

Health Care

Health Care Industry Team

Health Information Technology

Media, Entertainment, and Digital Content Law Specialty Team

Privacy, Data Breach & Data Security

Telecommunications and Technology

Telemedicine & E-Health

must undertake, a serious risk assessment as a necessary part of the plan. The risk assessment must encompass “meaningful use” and HIPAA privacy and security requirements along with best practice industry standards for comprehensive security programs.

Prevention of the unauthorized access to confidential protected health information (PHI) must be a key component to any portal. HIPAA compels any organization or individual using, storing or transmitting PHI to undertake a risk assessment of its actions, systems and processes to ensure that they comply with current HIPAA requirements as measured against current regulations and the Office of Civil Rights OCR audit protocols. Gaps in privacy and security requirements identified in the risk assessment must be plugged or organizations sponsoring patient portals in which there is a breach and release of PHI may be subject to costly and damaging loss of reputation and trust, as well as fines, penalties, enforcement actions and class action litigation.

For HIPAA, there is one key lesson: not just for patient portals but for all situations in which PHI is used or held or transmitted electronically: Encryption. HIPAA provides a “safe harbor” for all electronic devices that are encrypted according to the guidelines of the National Institute for Standards and Technology (“NIST”). NIST encrypted devices are not considered to be “unsecured” and, thus, are exempt from their improper disclosure being deemed a “breach” requiring notification and/or fines. Other HIPAA compliant portal issues include strong identity and access controls to verify each portal use, such as through secure username and password logons and other device intelligence and systems to prevent unauthorized use, access, malware and hacking.

Business Associates and individuals and organizations in a “chain of trust” are the focus of this month’s HIPAA Cyber Awareness Update. Sponsors of patient portals have multiple relationships with patients, their family members and care takers, as well as numerous vendors, suppliers, payors, health care providers, billing companies, consultants and IT vendors, etc., each with whom they share PHI. Each one of these relationships creates a point of risk and vulnerability for a data breach, making due diligence of business partners and business associate agreements a mandatory part of each relationship. HIPAA also imposes limits on how PHI may be used in relationship building initiatives such as marketing and fundraising.

Relatively new to the regulatory panoply is the Telephone Consumer Protection Act (TCPA). Patients using patient portals may expect to receive information when they want it, where they want it. But health care providers and their business associates are restrained by state and federal regulations that govern when and how they interact with their customers.The TCPA limits automatically dialed and prerecorded telemarketing calls to wireless and residential phones. In the past, healthcare providers and other "advertisers" could rely on an established business relationship (such as a previous physician/patient relationship) to circumvent the need to obtain a consumer's written consent to receive certain telemarketing or advertising calls. The “established business relationship” exception no longer applies, although other exceptions may apply. Portal sponsors must be especially careful as this strict liability statute carries with it fines of $500 per call, which can easily run up given the number of potential contacts a provider may make.

The Federal Trade Commission (FTC) and the Federal Drug Administration (FDA) are also interested in patient portals and interconnected devices including those intended for health monitoring. At present, the FTC is making recommendation about cyber protections built into such devices but additional regulation is certain to come.

Finally, Medicare, Blue Cross and the Affordable Care Act (ACA) now allows for reimbursement for limited telehealth services. Given the rapid growth of telehealth applications and devices, the ACA may be expected to be a source of future requirements for patient portal sponsors. Currently, however, the ACA does not impose technical requirements on portals, other than coverage criteria.

Conclusion

With the need for greater communications between providers and consumers and others the use of portals is certain to increase and likely to be the standard. Although useful, be informed of the rights and obligations that come from the use of portals. Implementing a portal in the right way will prove to be a valuable addition to the relationship between patients and providers establishing or using portals incorrectly could write fines, damages and embarrassment.

If you have questions regarding patient portals or other health care law matters, please contact your regular Butzel Long attorney, the authors of this alert, or any member of Butzel Long's Health Care Industry Group

Mark R. Lezotte
313.225.7058
lezotte@butzel.com

Robert H. Schwartz
248.258.2611
schwartzrh@butzel.com