bodman

A Health Care Law Update

Bodman PLC **February 4, 2025**

Resolutions for Healthcare Providers:
Part 1 of 2 – Cybersecurity, Privacy and HIPAA Compliance

By: Grace A. Connolly (Associate) and Brandon M. Dalziel (Member and Chair), Health Care Practice Group

As the new year begins, it is useful to review your practice's processes and policies to ensure that the practice operates with efficiency and remains compliant with ever-changing healthcare regulations. In this first installment of a two-part series, we propose resolutions for health care providers involving Cybersecurity, Privacy, and HIPAA compliance that will help promote the success of your practice in 2025 and beyond. Look for more resolutions in part two of our series.

1. **Review and update cybersecurity protections**.

Data breaches and cybersecurity continue to be a paramount issue for all healthcare providers. Taking time to review the protections you have and provide updated training to staff on cybersecurity attacks can minimize the risk of a cyber-attack while helping you to stay on top of the ever-changing landscape of cybersecurity.

Best practices for a robust cybersecurity policy include, but are not limited to,

- Frequent education and training opportunities for staff members;
- Conducting risk assessments, using technologies including firewalls and anti-virus software;
- Limiting the number of individuals who have access to protected information;
- Implementing strong password protections; and
- Reviewing and updating policies regularly.

Ensuring that your existing policies and procedures follow these best practices will protect you and your patients from potential breaches. During your review, it is also important to keep up to date with changing cybersecurity regulations. Recently, the HHS Office for Civil Rights proposed measures aimed to strengthen cybersecurity in health care under HIPAA. Proposed changes include, but are not limited to,

- An increased scope to the annual risk analyses that covered entities are required to complete;
- The development and revision of a technology asset inventory and a network map that illustrates the movement of ePHI through electronic information systems;
- Required vulnerability scanning at least every 6 months;
- Network segmentation; and
- Inclusion of additional cybersecurity provisions in business associate agreements.

These proposed changes would increase the burden on providers and limit their flexibility in choosing cybersecurity providers and software. Connecting with your health care attorney and other professionals can help guarantee you don't fall behind.

2. **Update Notice of Privacy Policy (NPP) and other policy documents to stay up to date on new regulations**.

Refreshing your patient-facing documents in accordance with updated rules and regulations is crucial to a successful practice. In certain instances, providers are now required to receive signed attestation from certain requestors before providing disclosures involving reproductive health information. Providers ***are not*** prohibited from using or disclosing patient information when it is being requested to investigate or impose liability on patients, health care providers, or others who seek, obtain, provide, or facilitate lawful reproductive health care, or to identify persons for such activities.

Also, effective February 16, 2026, HIPAA will require additional protections and provisions related to the disclosure of reproductive health information to be included in Covered Entity's Notice of Privacy Practices. Keeping your policies up to date with HIPAA and other healthcare law regulations helps not only protect you against liability, but it makes certain that you are providing the safest and highest quality of care.

3. **Stay on top of HIPAA compliance training for staff**.

Schedule training with your staff on HIPAA-related processes to review proper procedures to decrease the potential for wrongful disclosures and breaches. Continued and yearly training not only helps to ensure that all staff are utilizing proper practices but provides evidence that your practice's policies are compliant in the event of an actual or alleged breach. Online resources or third-party trainers can provide materials and presentations that can help create a more immersive and hands-on experience for staff members.

Bodman PLC can provide guidance on this matter and others provide practical advice to meet your needs. To discuss these or any other legal issues affecting your organization, please contact Brandon Dalziel at (313) 393-7507 or bdalziel@bodmanlaw.com, Annalise Lekas Surnow at (313) 392-1059 or alekas@bodmanlaw.com or Grace Connolly (313)-393-7563 or gconnolly@bodmanlaw.com. Bodman cannot respond to your questions or receive information from you without first clearing potential conflicts with other clients. Thank you for your patience and understanding.