HIPAA Compliance: Do you understand the rules?

Recently, the University of Mississippi Medical Center agreed to pay $2.75 million to settle multiple alleged Health Insurance Portability and Accountability Act violations from an incident in which an employee’s laptop, containing access to electronic protected health information, was stolen.

Make sure you are in compliance to avoid fines. These penalties can be assessed per violation per day.

<table>
<thead>
<tr>
<th>VIOLATION CATEGORY</th>
<th>PENALTY</th>
<th>MAX PER YEAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A) UNAWARE</td>
<td>UP TO $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(B) REASONABLE CAUSE</td>
<td>$1,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(C) WILLFUL NEGLECT*</td>
<td>$10,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(C) II) WILLFUL NEGLECT NOT CORRECTED**</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

The HIPAA security rule covers electronic protected health information (ePHI), but what is considered ePHI?

ePHI includes:
- Electronic health information that can identify an individual
- Information about a health condition (like a health history)
- Information about provision of health care (like a treatment plan)
- Information about payment for health care (like a bill)

Policies and safeguards must be implemented by all covered health care providers in order to be compliant. The covered dental office is required to ensure confidentiality, integrity and availability of ePHI, identify and protect ePHI against threats to security, and ensure everyone in the practice complies with practice security policies and procedures.

PBHS, endorsed by the North Carolina Dental Society to provide members with Secure Email, recommends that dental offices follow these five steps to help you avoid HIPAA penalties.

1. Determine your specific security requirements - Cover all electronic patient information, including email, in your risk assessment, identify threats and vulnerabilities that could lead to a data breach, and remember to specifically address encryption.
2. Identify types of data sent and set protocols - Determine who needs to have access to send email messages that contain ePHI and set policies to be enforced regarding proper use of technologies to encrypt, transmit and archive messages.

3. Think about how data could be leaked or lost - Do patient files or referrals ever get left on the copier? Do staff always lock their computer screens when they step away? Are attachments containing patient charts or treatment plans being sent through regular email?

4. Implement secure communication practices by making technology upgrades if necessary - Secure your email system and secure any digital space where collaboration on patient ePHI occurs.

5. Educate staff on security policies - Educate all doctors and staff and implement proper security procedures.

PBHS is the endorsed provider for secure email by the North Carolina Dental Society. Contact them today at 855-932-4232 or pbhs.com to help you stay HIPAA compliant.