Data Security Questions Healthcare Practices Should Ask

This is an extra resource to go along with the original article:
[This is how much it costs to keep patient data safe]

Data security is paramount to any healthcare practice. If you can answer these data security questions, you should be in a good place to protect sensitive patient information.

1. What kinds of sensitive data are our staff members handling?

Another question you might ask would be: "Do employees and staff have access to only the information they really need?"
Human error and internal theft are the second highest threat to patient privacy. Make sure that only staff members that should have access to patient data do and that everyone else is limited.

2. Do our emails follow HIPAA's data security rules?

HIPAA and email rules around patient privacy and security technology are broad.
Anything that identifies someone — be it name, address, or phone number — falls under HIPAA if it's used in a medical context.
This includes an HR professional informing a manager that a worker is out for surgery, or emailing an employee for an update on medical history.
It also includes a lot of communications to other HR department members. Whether these emails are sent internally to other team members, or externally to insurers/providers, to be compliant — they must be encrypted.

3. Are our patient portals secure?

Patient portal systems are a great way for patients to take control of their own healthcare information, but they also leave private data vulnerable.
Make sure that patients are aware of the need to protect their private information (don't give out your password, etc.) and you have best practices for using the patient portal posted on your website.

4. How and where are our patient files/patient data stored?

It's imperative that healthcare providers understand exactly where and how patient data will be stored. This means information going into an EMR system or stored on a cloud server or internal server.
Access to these storage locations should also be secured. If you're using a third party vendor for data security, make sure the proper individuals within your practice have access to this information.

5. Do we have training programs and policies for employees and staff?

Policies and procedures are only as good as the employees who implement them. Your staff should be trained to recognize sensitive information and to carry out proper handling techniques.

The HHS Notice of Proposed Rulemaking stipulates that fines and penalties will be applied to any staff member or employee that breaches healthcare information, even accidentally.

6. Do we have a breach or data incident response plan? Do our vendors?

Anyone is susceptible to breach or fraud, even security vendors. That's why it's important to have contingencies accounted for.

It's also essential that your practice understand the scope and depth of your vendor's incident response plan. This includes notification policies, too.