Top Mistakes Made When Releasing Medical Records

As a healthcare provider, you're responsible for releasing patient medical records upon request. The 21st Century Cures Act makes it easier for patients to access their information electronically, but not all health care providers know what this means for their team. When releasing medical records, mistakes can be caused by carelessness, weak security systems and inadequate training on accessing and releasing medical information.

Here are some of the top mistakes made when releasing medical records, and how you can avoid them.

INAPPROPRIATE ACCESS TO MEDICAL RECORDS

Inappropriately accessing or sharing information about a patient is a major issue, whether it's done intentionally or not. Something as simple as chatting with a friend about a patient's information falls under this category. Inappropriate access includes:

- Accessing a patient's chart when it's not directly related to patient care. This also pertains to past patients. For example, you cannot open a previous patient's chart to see how they're doing now. It also applies to friends and family. Unless you need to open the chart for reasons directly related to patient care, the chart is off-limits.
- Chatting among coworkers about a patient or their medical history.
- Accessing patient information from a personal, unsecured device.
- It's also important to make sure others around you don't obtain patient information. Make sure your close a patient's chart whenever you walk away to do something else.

FAILING TO PROVIDE EASY ACCESS TO PATIENTS

The 21st Century Cures Act was established to break down barriers between different medical records platforms and to make it easier for patients to access their own records electronically and more efficiently. The Cures Act mandates that patients have the right to obtain their records through an electronic link at any time, with no additional steps required. Patient access to information includes medical notes, test results, radiographic images, and reports to these images, with few exceptions. The law is rolling out over the next two years, with enforcement to follow. This includes penalties and incentives for providers and their EMR companies to comply with the law.

NOT OBTAINING CONSENT

All patient health information belongs to the patient. Patient information cannot be released to anyone else without the patient's consent. A signed consent form should always be obtained when sharing information with other healthcare providers and labs. This also applies to non-medical requests for information, such as for insurance claims or documentation of sick leave.

RELEASING INFORMATION TO FAMILY MEMBERS WITHOUT CONSENT

Since the establishment of HIPAA in 1996, and continuing with the Cures Act, a patient's information cannot be released to family members without the patient's consent. Physicians must always obtain information from the patient about who is authorized to receive their medical information.

The same rule applies to employers of the patient. If an employer is requesting information about the patient's health condition, you must get written consent from the patient before releasing any information.

Top Mistakes Made When Releasing Medical Records (continued)

Anytime you release information about a patient, for any reason, you are also required to keep records of who you gave the information to, which information you gave, and when you gave it.

RELEASING INFORMATION OVER THE PHONE

While most patients can access electronic medical records online, some patients may still request information by phone.

Patients may receive information, such as imaging or lab results, over the phone. However, this is only appropriate if there's a system in place to securely identify the patient. It's crucial to make sure that the person receiving this information is the patient. Each clinic needs to have a policy in place to confirm a patient's identity.

RESPONDING TO SUBPOENAS AND COURT ORDERS

Your clinical care team may receive subpoenas and court orders requesting medical records for a patient. Information about a patient may be shared to comply with a court order. However, only information directly related to the order, such as specific injury or illness, may be shared.

A subpoena isn't the same as a court order and you should not release medical information without the patient's written consent. To share medical information, you will need to have evidence that you notified the patient and gave them time to object, and that you obtained a qualified protective order from the court. It's important to note that information prepared for use in civil, criminal, or any court proceedings, does not fall under the category of electronic health information, and you aren't required to include this in a patient's electronic medical records.

INSUFFICIENT STAFF TRAINING

Mistakes can happen from lack of training. Employees need to be fully trained on HIPAA laws and the privacy rights of their patients, as well as the 21st Century Cures Act. They also need appropriate training on any software systems used at the clinic. Make sure that everyone on the clinical care team understands how to access and release confidential information properly and securely.

INADEQUATE COMPUTER SECURITY SYSTEMS

Each medical office must have a system in place to protect patients' information stored in electronic records. This can start with simply placing your computers in a way that clients in the waiting room cannot see what's on the screen. These computers should also be secure and out-of-reach, and no unauthorized person should be able to access the computers. Other steps include restricting access, using security passwords, and updating software to prevent unauthorized individuals from accessing electronic records.

IMPROPERLY STORING OLD RECORDS

Most clinics these days use electronic records, but old, written records are still around. It's important that these old records are also protected. Records need to be stored in a secure place. However, keep in mind that patients also have the right to request and access written records, so they need to be within reach.

If these records are not in a secure location, they need to be locked so that unauthorized people don't have access. You should also consider a process to track these records if they're used.

FINAL THOUGHTS

Physicians aren't the only ones that should be mindful of these mistakes. Medical assistants, office staff, nurses, therapists, and everyone on the clinical care team need to take the steps to ensure the ongoing confidentiality of all patients. Vivlio Health is here to help you and your clinical team avoid these common mistakes when releasing medical records. Visit our website to learn more about our information technology and services.