HIPAA, Legal Holds, and PHI: Rachel Rose, J.D., M.B.A. With Sean McKenna, J.D., B.A.



achel Rose (RR): Please tell us a bit about your background. Sean McKenna (SM): I spent almost 16 years with the federal government handling healthcare fraud matters, first with CMS, then OIG-HHS, and my last ten

years were with DOJ in Dallas as a federal prosecutor. For the last three-plus years, I have represented healthcare providers and executives in enforcement actions varying from administrative, civil, and criminal matters, including advising clients on fraud and abuse and HIPAA issues.

RR: Can you explain what a legal hold is and what types of information healthcare providers and business associates may be required to maintain?

SM: Generally, a legal hold is the process used by companies and executives to preserve all forms of relevant information within the custody of certain persons or "custodians." This usually includes all relevant information, including electronic material or "ESI" and protected health information (PHI), but limited only to when litigation is "reasonably" anticipated. A legal hold also is used for government investigations or other matters that require a party to avoid spoliation of information. Cases where a legal hold should be issued could be a medical malpractice action or simply notice of an audit. Increasingly, notice is required when there is a HIPAA breach or cyber-attack. The information typically requested is specific to a claim or action, but in government investigations, the evidence to be preserved by the relevant custodians is very broad. Such as medical records, billing claim forms, and other documents that contain PHI. If that occurs, federal and state HIPAA and privacy laws are applicable. But it also often includes other documents, such as contracts, emails, etc. that do not include PHI and don't implicate HIPAA.

RR: How long is the length of a legal hold in relation to

items containing protected health information?

SM: A hold will be required and should be in effect if there is current or anticipated litigation, an audit, or government investigation. This includes documents that contain PHI. The scope of the hold should be tailored to the nature of the issue. However, time limits will depend on the length of the action or litigation of any potential claim.

Be mindful that under HIPAA, there is an automatic obligation to retain records for 6 years. It doesn't require any legal process since it involves PHI and a patient's medical care. This obligation may be longer if a State privacy law is more expansive.

The other thing to remember is the concept of preservation under a litigation hold. Information should be preserved under a hold and not altered or deleted. Contrast that concept with a covered entity's obligation under HIPAA to amend a medical record at the individual's request. That request can be denied, but there are specific requirements under HIPAA when a provider denies an individual's request that could run afoul of a litigation hold.

RR: From your perspective, how important is it that entities that create, receive, maintain or transmit PHI have policies and procedures, as well as the technology, to preserve the PHI for the legal period of time? SM: It is very important that entities adhere to the HIPAA requirement of six years and the state law requirement, which may be longer. A legal hold may extend the length of time that the information needs to be preserved. In general, the recent fines from HHS have hit inadequate policies and procedures hard. So, make sure that both the policies and procedures and adequate technology are in place.

RR: Even if a medical condition is at issue, the documents are public and no one's insurance number, full DOB, or SS number should be included.

SM: That's correct. During litigation, all parties have to balance the individuals' right to protect their PHI with resolution of the conflict. That usually means painstaking efforts to thoroughly

review and redact the records, or the use of other legal processes to protect the individuals. Under no circumstances in civil litigation should identifiable information be available to the general public. Normally, a confidentiality or protective order is sought and granted by the Court. But remember, the government can rely on exceptions to HIPAA to obtain and use PHI in litigation.

RR: For sensitive information (e.g., substance abuse, mental health, minors, rape, etc.), what should be redacted and when is it appropriate for in camera review?

SM: Good question since HIPAA addresses these issues differently than normal PHI. Identifying information should be redacted always, unless it's a governmental entity. If PHI or identifying information is crucial to the conflict, and no exception to a State or HIPAA law applies, in camera review by the Court is appropriate.

RR: Are there any other recommendations that you have for persons who create, receive, maintain, or transmit PHI?

SM: In this era, err on the side of caution. As enforcement efforts in privacy increase, it is better to overprotect information. Subsequently scale back the transmittal of PHI if prudence dictates or you are compelled. Be thoughtful about how documents

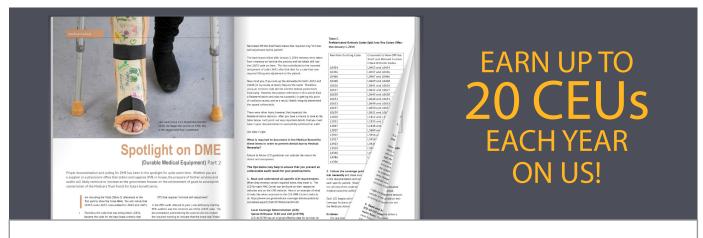
are transmitted and kept, both between parties and from clients and vendors, including attorneys. Vendors and law firms also should know their obligations under HIPAA, and in some cases, stricter state privacy laws.

Rachel Rose

J.D., M.B.A., is the principal at her company of the same name, based in Houston, TX. She is extensively published and presents on a variety of healthcare, False Claims Act, and securities law topics including: cybersecurity, qui tam, physician reimbursement, ICD-10, access to care, anti-kickback and Stark laws, U.S. Supreme Court cases impacting the medical device industry, international comparative healthcare laws, and the HIPAA/the HITECH Act. www.rvrose.com

Sean McKenna

J.D., B.A. is a Shareholder with the law firm of Greenberg Traurig and focuses his practice on healthcare enforcement and regulatory issues, representing individuals and providers under civil or administrative investigation by the Department of Justice, Offices of Inspector General, and Attorneys' General Medicaid Fraud Control Units, as well as in criminal investigations and matters involving the United States and State Attorneys General. www. gtlaw.com



Subscribe to the leading practice management magazine and educational resource available today!

Approving associations: AAPC , AHIMA , ARHCP , PAHCS , PHIA , POMAA , MAB , MED-C , PMRNC , PAHCOM , AHCAE , HBMA , APMBA , PMI , NHCLA

Visit www.billing-coding.com/subscribe for more information and to start your subscription today!