COSMOS
Navigate the Compliance Universe

Compliance Today - June 2023

Jonathan A. Porter (jonathan.porter@huschblackwell.com, linkedin.com/in/jonathanaporter/) is Partner at Husch Blackwell LLP, Savannah, GA.

Jeff Jensen (jeff.jensen@huschblackwell.com, linkedin.com/in/jeff-jensenesq/) is Partner at Husch Blackwell LLP, St. Louis, MO.

Gregg N. Sofer (gregg.sofer@huschblackwell.com, linkedin.com/in/gregg-sofer/) is Partner at Husch Blackwell LLP, Austin, TX.

What healthcare entities need to know about search warrants

by Jonathan A. Porter, Jeff Jensen, and Gregg N. Sofer

A few years back, following a sad occurrence in which a nurse administered incorrect medication that killed a patient, state investigators descended upon a prominent academic medical center armed with a search warrant. Law enforcement showing up with a search warrant and taking health records was not something this medical center saw coming, as surely law enforcement raids were reserved for shady medical practices and not prestigious health systems tied to top-ranked universities. Right?

In recent years, federal agents have executed search warrants at many healthcare facilities, including hospitals,[1] physician groups,[2] dental groups,[3] pharmacies,[4] laboratories,[5] medical equipment companies,[6] hospices,[7] nursing homes,[8] and even the offices of a managed care plan.[9] State and local investigators have done the same.[10] Search warrants are not just for shady pill- mill-doctors and fly-by-night kickback schemers; they are increasingly for legitimate, compliant providers of all types. Warrants that allow the search of healthcare facilities are being granted for the acts of rogue employees[11] and the acts of patients.[12] So if your healthcare entity has employees or patients, you need a plan because even a basic plan—on how to communicate with the agents, what privileges to assert over medical records, whether to speak to employees and how to address any media fallout—is going to help in a crisis. And a company's response to a search warrant could alter the outcome of the government's investigation.

This article provides the basics of what healthcare entities need to know about search warrants.

Understand the basics

Why is law enforcement allowed to take your documents? Because a law enforcement officer previously went before a judge and presented sufficient information to allow the judge to conclude that certain documents *probably* contain evidence of a crime. Upon such a finding, the judge will issue a search warrant, which describes exactly what law enforcement is allowed to search and seize. This process occurs in secret. The target isn't entitled to advance notice of the search and cannot halt the search to present a defense to the judge. Impeding or obstructing a lawful search carries the risk of a criminal conviction and other headaches.

In cases where the healthcare entity or its senior leaders are the targets of the investigation, the search warrant is likely a culmination of significant covert investigative activity, a signal that the covert investigation has reached critical mass and is ready to proceed to the next steps. In other cases—like if an employee is committing crimes on employer property or a patient commits crimes using the healthcare entity's server—then a search may be a less-critical event. The key to distinguishing between the two is reviewing the warrant for clues. (See Step three.)

Federal search warrants almost always come in four parts, but you will only have immediate access to three of them. Unless a judge orders otherwise, you will be provided by the law enforcement officer executing the search: (1) the warrant itself, usually on Form AO 93; (2) an identification of the person or property to be searched, usually on Attachment A to the warrant; and (3) an identification of the person or property to be seized from the location being searched, usually on Attachment B to the warrant. These three things are required by law to ensure that the search has lawful bounds.

The fourth part of a federal search warrant is something you are not likely to have access to immediately (or potentially ever). That is the agent's search warrant application and accompanying affidavit. Federal agents commonly provide requisite allegations to support probable cause in signed affidavits given to a judge. This signed document is often kept under seal during the search. Do not be surprised if you do not receive a copy of the affidavit during the search; the affidavit exists to convince a judge that probable cause exists to conduct the search, not to convince you that probable cause exists.

A fifth part of the search warrant will be created after the search. That is a receipt describing the seized property as part of the search.

What to do

The following are some suggested steps to take when you find yourself in the unfortunate scenario of undergoing a search. The best practice is to adapt these into a formal plan (as discussed below in the "How to prepare" section) based on your individual situation and applicable state-level privileges that may apply.

Step one: Contact designated individuals, including outside counsel

Depending on the size and structure of your entity, pick a few individuals to be contacted in case of a search and coordinate the process. This should include (1) counsel, (2) a corporate officer, and (3) the individual in charge of records. Having at least one person on-site to coordinate is critical. It is vital for this step to include outside counsel, which you should hopefully have lined up in advance. This is because, in every state, there is a rule against contact with represented parties. Outside counsel should act quickly to alert the lead agent and prosecutor of the representation, which shields your organization and its current employees from interviews that agents often attempt while executing the search warrant. Outside counsel does not need to be on-site to communicate the representation. The best setup is to have a designated on-site employee ready to lead efforts in-person, and outside counsel coordinating with that person and U.S. Department of Justice (DOJ) attorneys from afar.

Step two: Manage employees

Few things evoke excitement at the workplace like federal agents showing up with a warrant. Rumors will quickly spread about why federal agents are there, which becomes problematic when agents begin attempting to speak to employees present during the search. When the search comes out of a covert investigation, and no representation exists for that matter, such employee interviews are fair game. But the healthcare entity can still have a plan to limit the damage of these interviews by (1) obtaining counsel to represent it for the purposes of the investigation, (2) attaining pool counsel to represent former employees, and (3) ensuring employees know that they (a) are not

required to speak with the agents, (b) could have their text messages and emails from the day of the search warrant handed over to the government, and (c) could face consequences if they make false statements to the agents. It could be proper to ask the agents to allow the company to line up attorneys for employees wishing to talk with the agents to make sure the employees' rights are protected.

Step three: Review the warrant

If counsel is on-site, counsel should ask for an opportunity to review the warrant. If counsel is off-site, ask to take a picture of the warrant and email it to counsel. If law enforcement officials executing the warrant are unaccustomed to healthcare, politely explain that patient health law requires ensuring the validity of the legal process before turning over documents. Once counsel starts reviewing the warrant, take note of a few things:

- The warrant itself is signed in the space left for the judge's signature.
- The warrant gives a time window for execution. Make sure the search is occurring within the authorized time frame. If the time frame has expired, politely point that out to the law enforcement officer spearheading the search. If law enforcement proceeds with the search anyway, document the problem and that you gave notice of the problem.
- On Attachment A, note the property to be searched. The property description could be broad (e.g., an entire property) or narrow (e.g., a specific physician's office or a specific filing cabinet). If the search exceeds the contours of Attachment A, politely point that out to law enforcement and document what is being taken from locations beyond what is described in Attachment A.
- On Attachment B, note the property to be seized. This guides what things law enforcement can seize. It is usually drafted broadly, but this is your best indicator of what the agents are investigating. Attachment B typically lists specific things, like servers, patient records, or personnel files, to meet specificity requirements. Again, if the search exceeds the scope, bring your concern to law enforcement's attention, and then note your concern.
- Note any statutes listed in the warrant or attachments. Sometimes statutes believed to be violated appear on the warrant itself. Other times, statutes are on Attachment B. Some courts may not require statutes to be listed on the warrant or attachments. But these statutes will give you an idea of the conduct being investigated. For example, a warrant listing 18 U.S.C. § 1347 means the investigation is healthcare fraud, and a warrant listing 42 U.S.C. § 1320a-7b means the investigation is into kickbacks. A warrant listing a Title 21 offense could mean the investigation centers on drug diversion or improper opioid prescriptions. But a warrant listing a statute unrelated to healthcare could mean that an employee or patient is the target.

Step four: Identify privileged documents

This is why preparing for a search must be done in advance: if you're Googling applicable privileges as agents carry out boxes, you may be too late. There are several potential privileges that may apply to healthcare providers, but a key privilege to be on top of is attorney–client privilege. This is because DOJ policy requires agents to adopt special protocols when they know their search involves potential attorney–client privileged materials.[13] At that point, the investigators should establish a "taint team" separate from the investigation team to review potentially privileged materials. But these protocols do not go in place until the agents learn of potentially privileged materials, so alerting agents as to privilege is critical. Otherwise, agents will have full run of privileged materials until they learn of privilege one way or another, and a court could even find that any privilege was waived.[14]

Other privileges besides the attorney–client privilege may apply to a healthcare entity's records. Some privileges turn on their recognized existence under state law, so it is vital to flesh out these potential privileges beforehand. Potential privileges in the healthcare setting, depending on the nature of the privilege, the state in which the privilege-holder is based, and whether the matter is in federal or state court, include:

- An academic research privilege,[15]
- A medical peer review privilege,[16] and
- The work–product doctrine.[17]

Neither the physician–patient privilege[18] nor HIPAA[19] are grounds for refusing to turn over documents in federal investigations, despite some belief in the medical community to the contrary.

It is critical to know where potentially privileged documents are housed so that if agents are carrying off a particular set of patient files or a particular server, you can alert agents as to potential privilege and preserve privilege.[20]

Step five: Monitor all agents and memorialize concerns

As discussed in Step three, there are important limits to what federal agents are allowed to search and what they are allowed to seize. If agents start searching something they are not authorized to search, start taking documents they are not authorized to take, or start taking documents regardless of being told about privilege despite no presence of taint agents, then it could be crucial later that those acts are memorialized by those tasked with monitoring the search. You will also want to compare your own list of seized property against the list the agents will leave with you at the end of the search. Also, note which employees the agents sought to interview and what, if anything, was said by those employees. These notes will ensure that agents accurately record what employees say and will also help a compliance officer or outside counsel with an independent investigation if one becomes necessary.

Step six: Think about how to maintain business operations

Agents walking out with all servers and devices could be a problem for a physician group, health system, or other medical providers that rely on electronic medical records to treat patients. Work with the lead agents on the practical implications of their actions with patient safety in mind. To the extent possible, make copies of operational critical systems, files, and documents. You will want to think about if and when to make an internal statement to employees as well as another statement to the media. You will also want to start thinking about potential collateral consequences like whether any provisions of a debt covenant have been triggered.

How to prepare for all of this

Make a plan. These processes can be implemented now: responding individuals for each site can be identified and trained; employees can be educated about how their text messages can be obtained by federal agents and educated about the risks of speaking with federal agents; privileges can be identified; privileged documents can be located; identifying who needs to be alerted and when they need to be alerted; planning for media responses; and distinguishing provisions that may apply in debt covenants. Lastly, you can select the attorney to help with this plan and deal with the investigation to follow now.

Very few healthcare providers think they will see the day when federal agents come through their doors. However, it occurs more frequently than you might imagine, and now more often than ever. A proactive plan will

be worth the time and money you invest in it.

Takeaways

- Search warrants executed on the premises of healthcare entities are no longer just for shady medical practices. There is a definite uptick in search warrants happening at all types of healthcare locations.
- Getting searched without a plan could have major ramifications. Unknowing employees could create more problems, and the agents could take documents they are not entitled to.
- Healthcare entities can plan for search warrants by taking a few critical steps, like identifying and training an on-site point person to interface with the agents.
- Healthcare entities can also start identifying potential privileges that apply to sets of documents and noting the location of those documents for use in the event of a search warrant.
- Healthcare entities can also plan now by retaining an experienced attorney who can handle search warrant preparations and planning and who can carry out the plan if a search warrant ever happens.

1 Ayla Ellison, "FBI raids Pennsylvania hospital," *Becker's Hospital Review*, January 31, 2020, https://www.beckershospitalreview.com/legal-regulatory-issues/fbi-raids-pennsylvania-hospital.html; Daniel Karell, "FBI agents execute search warrant on Southwest Regional Medical Center in Georgetown," *The News Democrat*, October 6, 2015, https://www.newsdemocrat.com/2015/10/06/fbi-agents-execute-search-warrant-on-southwest-regional-medical-center-in-georgetown/; Associated Press, "FBI Raids 3 LA Hospitals in Fraud Case," *CBS News*, August 6, 2008, https://www.cbsnews.com/news/fbi-raids-3-la-hospitals-in-fraud-case/.
2 Memphis News Staff, "FBI and TBI agents conduct joint raid of Memphis doctor's office," Fox 13 News, August 17, 2022, https://www.fox13memphis.com/news/local/fbi-tbi-agents-conduct-joint-raid-memphis-doctors-office/C3H4RFTXBJC5NCC7E63MPAOKQM/; Mike Holden, "Urgent care in Green Tree closed until further notice after FBI conducted 'law enforcement activity,'" WPXI-TV News, March 3, 2022, https://www.wpxi.com/news/top-stories/fbi-agents-seen-carrying-boxes-out-urgent-care-green-tree/VUDAPWE7VRCTFEB3QHG3AAFMCM/.
3 Amber Stegall, "FBI, police, Homeland Security raids office of popular Lubbock dentist," KCBD News, January 14, 2021, https://www.kcbd.com/2021/01/14/fbi-police-homeland-security-raids-office-popular-lubbock-dentist/.
4 U.S. Department of Justice, U.S. Attorney's Office for the Southern District of Iowa, "Search Warrant Execution at Rashid Pharmacy," news release, March 31, 2021, https://www.justice.gov/usao-sdia/pr/search-warrant-execution-rashid-pharmacy; Marco Bello, Maria Alejandra Cardona, and Sarah N. Lynch, "Federal agents raid Miami-area pharmacy as part of opioid prescription crackdown," Reuters, August 16, 2022, https://www.reuters.com/business/healthcare-pharmaceuticals/federal-agents-raid-miami-area-pharmacy-part-opioid-prescription-crackdown-2022-08-16/.
5 Tom Jones and Lisa Parker, "FBI Serves Search Warrant at Rolling Meadows COVID Testing Company and Lab," NBC 5 News Chicago, January 24, 2022, https://www.nbcchicago.com/news/local/fbi-serves-search-warrant-at-rolling-meadows-covid-testing-company-and-lab/2736994/.
6 Kate Jacobson, "FBI raids medical-supply company in Boca Raton," *South Florida Sun Sentinel*, January 14, 2015, https://www.sun-sentinel.com/local/palm-beach/fl-boca-raton-medical-supply-fbi-20150114-story.html.
7 KHOU.com Staff, "FBI raids hospice on Houston's south side," KHOU 11, May 18, 2017, https://www.khou.com/article/news/local/fbi-raids-hospice-on-houstons-south-side/285-440975688; WMCActionNews5.com Staff, "Federal search warrant executed on hospice co-owned by county attorney,"

Action News 5, February 28, 2014, https://www.actionnews5.com/story/24845881/federal-search-warrant-executed-on-hospice-co-owned-by-county-attorney/.
8 Daveen Rae Kurutz, "FBI serves federal search warrant at Brighton Rehab," *Beaver County Times*, September 3, 2020, https://www.timesonline.com/story/news/2020/09/03/fbi-serves-federal-search-warrants-brighton-rehab/5702747002/.
9 Catherine Larkin and Bloomberg News, "WellCare stock falls $72.50 day after FBI raid," *Orlando Sentinel*, October 25, 2007, https://www.orlandosentinel.com/news/os-xpm-2007-10-26-wellcare26-story.html.
10 Dustin Lattimer, "Police raid hospital room of terminally ill patient," KTSM.com, December 26, 2022, https://www.ktsm.com/news/police-raid-hospital-room-of-terminally-ill-patient/; 9and10news Site Staff, "Troopers Raid Wayne Co. Medical Clinic For Overprescribing Opioid Drugs," 9 and 10 News, August 17, 2017, https://www.9and10news.com/2017/08/17/troopers-raid-wayne-co-medical-clinic-for-overprescribing-opioid-drugs/.
11 Michelle Homer and Melissa Correa, "FBI raids Houston Health Department headquarters during investigation," KHOU 11, February 16, 2022, https://www.khou.com/article/news/crime/fbi-raid-houston-health-department/285-e1443b16-a2ef-4d69-bab0-1049d3287f1e.
12 Lattimer, "Police raid hospital room of terminally ill patient."
13 U.S Department of Justice, *Justice Manual* § 9-13.420.
14 United States v. Pelullo, 917 F.Supp. 1065, 1077–78 (D.N.J. 1995) (noting that records "were in a disorganized state" and therefore "there was no way the agents searching the warehouse could possibly have known that Pelullo claimed privilege with respect to the contents," and commenting upon how "the carelessness with which Pelullo treated supposedly privileged documents [could have] constituted a waiver of his privilege").
15 This is rarely recognized but could be recognized for certain types of research-related records in academic medical centers. Eric Robinson, "No Confidence: Confidentiality, Ethics and the Law of Academic Privilege," *Communication Law and Policy* 21, no. 3 (2016): 323-381, https://doi.org/10.1080/10811680.2016.1184917 (noting few courts recognize the privilege). Compare in re Request from United Kingdom Pursuant to Treaty Between Government of U.S. and Government of United Kingdom on Mutual Assistance in Criminal Matters in the Matter of Delours Price, 685 F.3d 1 (1st Cir. 2012), *cert. denied*, 133 S.Ct. 1796 (2013) (declining to recognize academic research privilege) *with* Cusamano v. Microsoft Corp., 162 F.3d 708, 714 (1st Cir. 1998) ("Academicians engaged in pre-publication research should be accorded protection commensurate to that which the law provides for journalists.").
16 Agster v. Maricopa County, 422 F.3d 836 (9th Cir. 2005) (Federal courts rarely recognize a medical peer review privilege, rejecting a medical peer review privilege with respect to federal law), but state courts largely do; federal courts will occasionally extend state-granted medical peer review privilege in considering law intending to supplement state law, such as a federal Emergency Medical Treatment and Active Labor (EMTALA) case, Grenier v. Stamford Hosp. et al., 2016 WL 3951045 (D. Conn. 2016) (recognizing medical peer review privilege in EMTALA case because EMTALA supplements state law).
17 Fed. R. Civ. P. 26(b)(3). To the extent searches involve servers or other locations that house attorney work–product, those should be noted for law enforcement.
18 Stephen A. Silver, "Beyond Jaffee v. Redmond: Should the federal courts recognize a right to physician–patient confidentiality?" *Ohio State Law Journal* 58, no. 5 (1998): 1809-1866, https://pubmed.ncbi.nlm.nih.gov/16211748/; United States v. Bek, 493 F.3d 790 (7th Cir. 2007) (holding that medical records of physician defendant not subject to any physician-patient privilege under federal law).
19 45 C.F.R. § 164.512(f).
20 Pelullo, 917 F.Supp at 1078 (noting that careless treatment of privileged documents could result in waiver).