STATE OF NEW MEXICO
COUNTY OF BERNALILLO
IN THE DISTRICT COURT

STATE OF NEW MEXICO
-VS-
Seagate Backup Plus Portable Drive (1 terabyte)
External hard drive
Model: SRD00F1
S/N: NA9JQDPA
Color: Black and Blue

SW 2018 00019

SEARCH WARRANT

THE STATE OF NEW MEXICO, TO ANY OFFICER AUTHORIZED TO EXECUTE THIS WARRANT: Proof by Affidavit for Search Warrant having been submitted to me, I am satisfied that the person named/described and/or property described in the Affidavit are located where alleged in the Affidavit, and I find that grounds exist for the issuance of the Search Warrant. A copy of the Affidavit is attached and made a part of this Search Warrant.

YOU ARE HEREBY COMMANDED to search forthwith the person and/or place described in the Affidavit, commencing between the hours of 6:00 a.m. and 10:00 p.m. [unless I have specifically authorized a nighttime search as stated below], and continuing thereafter until completed, for the person and/or property described in the Affidavit, serving this Warrant together with a copy of the Affidavit, and making the search and if the person and/or property be found here, to seize the person and/or property and hold for safekeeping until further Order of the Court.

EXECUTING OFFICER (S) are directed to prepare a written inventory of any person or property seized. You are further directed to file the return and written inventory with the Court promptly after execution of this Search Warrant.

DATED THIS 4th **DAY OF** September , **2018 AT** 2:00 pm **HOURS.**

A Hart
JUDGE Alisa Hart

AUTHORIZATION FOR NIGHTTIME SEARCH

I further find that reasonable cause has been shown for nighttime execution of this Warrant. I authorize execution of this Search Warrant at any time of the day or night for the following reasons:

JUDGE

DATE

CASE # AGH
18-0[illegible]33

RETURN AND INVENTORY

STATE OF NEW MEXICO
-VS-
Seagate Backup Plus Portable Drive (1 terabyte)
External hard drive
Model: SRD00F1
S/N: NA9JQDPA
Color: Black and Blue

DEFENDANT'S COPY

I received the attached Search Warrant on 9/4/2018 And executed it on 9/4/2018
At 1432 Hours. I searched the person or premises described in the Warrant and left a copy of the Warrant with:

M.E Schmidt-Nowara @ Freedman, Boyd, Hollander
(Name of the person searched or owner at the place of search)

Together with a copy of the inventory for the items seizes. The following is an inventory of the property taken pursuant to the Warrant:

- ONE SEAGATE BACKUP PLUS PORTABLE DRIVE w/ USB CORD

This inventory was made in the presence of T. MARTINEZ
Applicant for Search Warrant

And M.E. Schmidt-Nowara
Owner or other witness

Signature of Special Agent

Signature of Owner or Witness

Return made this 5 day of September, 2018 at 11:03AM hours.

~~(Judge~~ Clerk)

STATE OF NEW MEXICO
COUNTY OF BERNALILLO
IN THE DISTRICT COURT

STATE OF NEW MEXICO
-VS-
Seagate Backup Plus Portable Drive (1 terabyte)
External hard drive
Model: SRD00F1
S/N: NA9JQDPA
Color: Black and Blue

SW 2018 00019

AFFIDAVIT FOR SEARCH WARRANT

Affiant, Ted Martinez, is a full-time, sworn Law Enforcement Officer with the New Mexico Office of the Attorney General. Affiant is currently assigned to the Medicaid Fraud Control Division. Affiant has been a full-time Law Enforcement Officer since 2011. Affiant's duties include follow-up investigations on all Medicaid related crimes and Abuse, Neglect, and Exploitation of Patients in Care Facilities. To include but not limited to Fraud, Forgery, Embezzlement, Exploitation, and Theft of Identity crimes. Affiant has received training and has experience in the writing and executing of Search and Arrest Warrants.

I, Special Agent Ted Martinez, being duly sworn, on my oath, state that I have reason to believe that on the following described external storage device:

The Seagate external portable hard drive, black and blue in color, model SRD00F1, serial number NA9JQDPA, one terabyte in size.

Property for which authorization to be seized, viewed and analyzed

Any and all medical records, treatment records, prescription records, for any individuals treated by Dr. Edwin B. Hall or any other provider in his medical practice, and any and all records for individuals employed by Dr. Edwin B. Hall, to include the following:

1. Any and all records, charts, and notes;
2. Patient intake forms, referrals, applications, authorizations from insurance;
3. Full initial and updated assessments, evaluation forms, agreements, consents of treatment, diagnosis;
4. Any and all treatment plans while under the care of the above provider;
5. Any and all records from prior and current physicians regarding patients' care;
6. Documents within your possession that are required to be fully disclosed detailing the extent and nature of all services furnished to the patient;
7. Any and all medication prescriptions and refills, including but not limited to those required to be reported to the Prescription Monitoring Program;
8. Any and all orders for laboratory testing and corresponding test results, including urinalysis/blood tests made in your office and/or independent laboratories;
9. Any and all signed appointment logs, complete log of cancelled or missed appointments;
10. Any and all communications with the patient and/or patient's representatives regarding

appointment cancellations;

11. Any and all communications with the patient and/or patient's representatives regarding patients' care;
12. Any and all electronic files associated with the treatment and/or care of the listed patients.
13. Complete personnel files for each employee that provided direct services to the listed patients, as indicated in item #6 above, including but not limited to all employment forms required by your Policy and Procedure Manual, background verifications, trainings, and licensures, scope of work, responsibilities, and resumes.
14. Any and all records, information, and documentation which appear to be related to the services furnished for Medicaid recipients, including all medical records, employee records, business records, financial records, billing records, notes, and communications made by staff and administration. Records, information, and documentation consists of written, recorded, printed, or electronically stored materials.
15. Any and all computer hardware. Computer hardware consists of all equipment that can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Computer hardware includes but is not limited to any data processing units, memory typewriters, and self-contained "laptop" or "notebook" computers; internal and peripheral storage devices such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, flash or "thumb" drives, and other memory storage devices; peripheral input/output devices such as keyboards, printers, scanners, plotters, video display monitors, and optical readers, and related communication devices such as modems, cables, and connections, recording equipment, RAM or ROM units, acoustic couplets, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices; as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware such as physical keys and locks.
16. Any and all computer software that may contain data relevant to financial and clinical records. Computer software is digital information that is interpreted by a computer and any of its related components to direct the way the components work. Software is stored in electronic, magnetic, optical, or other digital form. It may include programs to run operating system applications like basic demographic and insurance information, patients' personal health information, practice management system, creation and submission of claims, accounting applications, patient statements, word processing, graphics, or spreadsheet programs, and utilities, and communications programs.
17. Passwords and Data Security Devices. Computer passwords and other data security devices may restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates as a sort of digital key to "unlock" particular data security devices.
18. Any and all "cloud" or web based data relevant to the services rendered to the Medicaid consumers. Data may be found in "cloud" or "cloud-like" applications, which include data on a web server(s), application server(s) and database server(s). Data may also consist of backup data.
19. Any and all forms of information relevant to the services provided to Medicaid consumers. The term "information" includes all of the foregoing items of evidence in whatever form and by whatever means such records, documents, or materials, their drafts, or their modifications that may have been created or stored, including, but not limited to, any handmade form (such as writing, drawing, with any implement on any surface, directly or indirectly); photocopies; any mechanical form (such as printing or typing); any electrical, electronic or magnetic form (such as video, cassettes, compact disks); any information on an electronic or magnetic storage device (such as floppy diskettes, hard disks, backup tapes, CD-ROMs, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, electronic notebooks, as well as printouts or readouts from any magnetic storage device); and any photographic form (such as microfilm,

microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies).

Based on your affiant's knowledge, training, and experience, and the experience of other law enforcement personnel, your affiant knows that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, all computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer, must be seized and subsequently processed by a qualified computer specialist in an appropriate setting such as an office or laboratory. The analysis of computer and/or digital media is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover digital information, to include hidden, erased, compressed, password-protected or encrypted files. The high volume of the contents and the potential intentional concealment of criminal activity through random ordering and deceptive file names may require the examination of all stored data. This process may take weeks or months depending on the volume of the data involved and the caseload of the computer expert.

Recognizing that specialized and highly technical equipment and software will be needed to conduct the analysis of the previously seized digital media, the media may be transferred to the RCFL or other qualified laboratory with a request that a forensic examination be conducted in this matter. Additionally, under limited situations, assistance may be required by the receiving laboratory from other qualified laboratories. I know that a specialized examiner is required because of the following:

1. Computer storage devices (like hard disks, diskettes, tapes, laser disks, Bernoulli drives, CDs, DVDs, PDAs, MMCs, memory sticks and optical disks) can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence, and he or she might store criminal evidence in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site;

2. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification of destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis; and

3. The size of electronic storage media continues to grow, creating a large amount of data that must be searched to locate specific items. To place this in perspective, 250 GB hard drive can contain:

    a. up to 93,750 digital images;
    b. up to 221 days of around-the-clock MP3;
    c. up to 375 hours of VHS quality video; or
    d. 106 two-hour DVD-quality videos.

Based on your affiant's consultation with experts in computer searches, data retrieval from computers and related media and from his consultations with other law enforcement officers who have been involved in the

search of computers and retrieval of data from computer systems, your affiant knows that searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize all of the computers system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:
The peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system (known as dongles). It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices. If the analyst determines that the input/output devices, software, documentation, data security devices are not necessary to retrieve and preserve the data after inspection, the government will return them in a reasonable period of time.

Based on my training and experience, I know that computer hardware, software, documentation, passwords, and data security devices may be important to a criminal investigation in two distinct and important respects: (1) the objects themselves may be instrumentalities, fruits, or evidence of crime; and/or (2) the objects may have been used to collect and store information about crimes in the form of electronic data. Based upon my training and experience, I know that the elements of information described above in items 1 thru 6, may include evidence that declares the identity or source of authorship of any persons involved in the criminal conduct, and all of the above records, together with any evidence or items which would be used to conceal the forgoing or prevent its discovery.

The aforementioned information, items or data may have been obtained or is being possessed in a manner which constitutes a criminal offense, is designed or intended for use or which has been used as a means of committing a criminal offense, and would be material evidence in a criminal prosecution. The facts tending to establish the foregoing grounds for issuance of a Search Warrant are as follows:

Affiant, Special Agent Ted Martinez, is a commissioned police officer for the New Mexico Office of the Attorney General and has been assigned to assist in the investigation into Medicaid fraud alleged to have been committed by Dr. Edwin B. Hall.

Background:

On April 12, 2017 a referral was made to the New Mexico Office of the Attorney General Medicaid Fraud Control Division regarding a provider by the name of Dr. Edwin B. Hall. The referral was filed by the Children Youth and Families Division (CYFD) in regards to Dr. Hall's practice. CYFD received a complaint from a community-based Child Psychiatrist, submitted to CYFD's then Child Psychiatrist Dr. George Davis. The complaint was in reference to three former patients of Dr. Edwin B. Hall.

The complaint involved the prescribing practices demonstrated by Dr. Edwin B. Hall's management of these three siblings' medications throughout their course of approximate twenty six months in Treatment Foster Care (TFC) services. The community-based Child Psychiatrist described Dr. Hall's prescribing practices for the first three children in the following terms: "the three boys were each on a bewildering variety of meds."

Dr. Davis conducted a review of the treatment provided to children in the TFC program, Red Mountain Treatment Foster Care. Dr. Davis reviewed a selection of fifteen children Dr. Edwin B. Hall provided treatment

to, some of which were siblings. Dr. Davis stated in his review that seven of the fifteen children he reviewed all displayed the same prescribing issues of excessive medications and probable conflicting actions of these medications. Dr. Davis stated in his review that this is the most egregious example of unprofessional and illogical prescribing he has ever witnessed. Dr. Davis also expressed concerns for the types of medications being prescribed to young children (ten years and younger). Dr. Davis submitted a detailed report to the Medical Board on his findings. This investigation led to obtaining records via subpoena from the Medical Board for any complaints that had been submitted in regards to Dr. Edwin B. Hall and his practice.

Medicaid claims data was analyzed and a query of all children eighteen and under was completed. The children that displayed an elevated prescribing pattern outside normal prescribing habits were pulled from this data. Approximately seven hundred fifty four children were identified in this analysis.

Within these records was a complaint initiated on March 3, 2016 stating Dr. Edwin Hall was listed on the Pharmacy Boards quarterly report as a "high risk prescriber". It was noted in this report that Dr. Edwin B. Hall prescribes concerning amounts and combinations of controlled substances to his patients. An additional complaint was initiated on October 1, 2017 when the Medical Board received an Office of the Medical Investigator (OMI) data report from the Department of Health. The report listed patient overdose deaths from certain providers from the time period of 2015 through 2017. Dr. Edwin B. Hall was listed as a provider who had six patient overdose deaths during this time period. The report states Dr. Edwin B. Hall had written controlled substance prescriptions to these patients within thirty days or less of their death. This complaint also notates that Dr. Edwin B. Hall has consistently been listed as a high risk prescriber who is not accessing the required patient Prescription Monitoring Program (PMP) prior to prescribing controlled substances to patients.

A preliminary examination of Medicaid claims submitted by Dr. Edwin B. Hall for the time period of 2013 through 2018 revealed thirty additional patients that had died while under Dr. Edwin B. Hall's care. Further investigation as to the cause of death of these patients is ongoing.

Four patients of the six overdose deaths that OMI reported were found to be Medicaid recipients. The two other patients, James Burke and Andrew Mason, were covered by other insurance plans. It was confirmed through the reports provided from the Medical Board, as well as PMP reports tracking Dr. Edwin B. Hall's prescribing habits, that James Burke and Andrew Mason were patients of Dr. Edwin B. Hall.

Through communication with Dr. Edwin B. Hall's attorney, the physical location of these records were confirmed to be in possession of Dr. Edwin B. Hall's former assistant, who resides at 11520 Del Rey Avenue Northeast, Albuquerque, NM 87122. Additionally, his attorney advised that the medical practice records, including all patient files, prescriptions and employee records were scanned and stored on a computer. This computer has been made available to the Medicaid Fraud Control Division by Dr. Edwin B. Hall's attorney. A regulatory request was made to his attorney for all of the records regarding the treatment and care to the thirty-six patients who died while under the care of Dr. Edwin B. Hall. It is believed, however, that additional information of evidentiary value is contained and could support the investigation.

Based on the referral to the MFCD, the investigation and analysis completed by CYFD and the investigation completed by the Medical Board, probable cause exists to obtain and search medical records held and kept by Dr. Edwin B. Hall, or his record custodian, for the treatment, evaluation and prescription practices of Dr. Edwin B. Hall. Such treatment, evaluation and prescription practices may indicate actions which could result in patient harm or death.

Affiant is aware through training and experience that medical records document information regarding treatment provided, nature of treatment provided, and identifies who provided treatment. These medical records also contain and document types, quantities, and combinations of prescriptions that were prescribed and the

reason for the prescriptions. Without these records we are unable to determine who provided treatment and why the treatment was medically necessary.

The Medicaid Fraud Control Division has the power and authority to investigate violations of the Medicaid Fraud Control Act [30-44-1 NMSA 1978]. The Medicaid Fraud Control Division does not have the authority to obtain patient records with regulatory authority when the records being requested are not associated with the Medicaid program. Affiant believes the medical records being requested contain information of evidentiary value that is essential to determine what treatment was provided and who the provider was. Affiant is requesting a search warrant to obtain the above listed records that Dr. Edwin B. Hall is responsible for maintaining as a provider.

SUBSCRIBED AND SWORN TO BEFORE ME IN THE ABOVE NAMED COUNTY OF THE STATE OF NEW MEXICO,

THIS 4th **DAY OF** September **, 2018.**
@ 2:00p.m.

A Hart
JUDGE Alisa Hart

T. Martinez
AFFIANT

District Judge
TITLE

Special Agent
TITLE

APPROVED BY ASSISTANT ATTORNEY GENERAL _____ **ON** 9-4-18

CASE #
18-033

RETURN AND INVENTORY

STATE OF NEW MEXICO

-VS-

STATE'S COPY

Seagate Backup Plus Portable Drive (1 terabyte)
External hard drive
Model: SRD00F1
S/N: NA9JQDPA
Color: Black and Blue

I received the attached Search Warrant on 09/04/2018 And executed it on 09/04/2018
At 1432 Hours. I searched the person or premises described in the Warrant and left a copy of the Warrant with:

M.E. Schmidt-Nowara @Freedman. Boyd. Hollander
(Name of the person searched or owner at the place of search)

Together with a copy of the inventory for the items seizes. The following is an inventory of the property taken pursuant to the Warrant:

- One Seagate backup plus portable drive w/ usb cord

This inventory was made in the presence of T. Martinez
Applicant for Search Warrant

And M.E. Schmidt-Nowara
Owner or other witness

_____
Signature of Special Agent

_____
Signature of Owner or Witness

Return made this _____day of _____, 2018 at _____hours.

_____
(Judge Clerk)