Notifying Patients of Ransomware Incidents

“.....WITHOUT UNDUE DELAY”

November 8, 2020

Dissent Doe, PhD

Introduction

Some ransomware threat actors maintain dedicated leak sites where they post the names of victims who have not paid their ransom demands, and where they dump data from the victims to pressure them to pay. The data dumps involving personally identifiable information (PII) and protected health information (PHI) represent a significant shift from previous years when threat actors would hack and then either hang on to data to misuse it or list it for sale on the dark web. Now, we are seeing data dumps that make PII and PHI freely available in the public arena to the whole world. Some of these leak sites are on the dark web, but some of these threat actors also maintain mirror sites on clearnet.

HIPAA requires notification to HHS and to patients no later than 60 days from discovery and “without undue delay.” If data is dumped on Day 1 following an attack, is it reasonable for entities to take 60 days to alert patients that their data is in the wild and is being downloaded and shared by criminals and others? Should we require some quicker public alert system so that people can immediately become aware of potential risk and what steps they may want to take while the entity investigates further? How about a quick media notice or press release, and a statement on a web site -- something that doesn’t leave patients in the dark when you already know that at least some PHI is in the wild being circulated?

DataBreaches.net recently examined a number of dedicated leak sites for listings involving medical/health entities in the U.S. The bulk of this report provides descriptions of 30 incidents and whether or not they have notified patients or regulators. The sample of 30 is not complete. Not all ransomware victims are listed on dedicated leak sites (the threat actor may hold off adding them while they are trying to negotiate a ransom payment), and some entities that were listed were removed, possibly because they agreed to pay the ransom demand.

Incidents Posted by Conti Threat Actors

Ventura Orthopedics was added to Conti's site on August 26. An attack on Ventura had previously been added to Maze Team's site with a dump of dozens of files on August 2.

Ventura Orthopedics has six locations and is covered by HIPAA. DataBreaches.net reached out to Ventura Orthopedics several times and first reported on their incident on August 26. Ventura did not respond to subsequent inquiries, despite assurances that they were going to provide more details. The Ventura dumps contain sensitive medical information on patients -- there are hundreds of lab workups that list the presence or absence of psychotropic medications and pain-related medications like oxycodone. The reports give the patients' name, their date of birth, the referring physician, and other details. There are also files with employee information, although I did not spot any W-2 files (some W-9 files were found, however, as were a number of insurance-related files and other financial matters).

As of today, there is still no notice on Ventura Orthopedics' web site to alert patients that their data has been stolen and dumped by serious criminals. And there is no notice from Ventura on HHS's public breach tool, despite the fact that it is now more than two months since patient data and files were first dumped on the dark web. Have they notified patients or haven't they? Perhaps they notified patients but didn't file with the state and federal government? We do not know because they have not posted anything on their site, have issued no press release or media notice, and have not responded to inquiries.

Adams County Memorial Hospital was added to Conti's site on September 5. While the attackers dumped more than a dozen files, the files appeared to be more bank-related or financial in nature. I do not see patient files dumped, although that does not mean that the threat actors aren't in possession of any. The hospital, which is an acute care facility, is likely covered by HIPAA, but does not mention HIPAA at all on its web site.

Were hospital operations impacted by the attack at all? And did this breach have to be reported to HHS no later than November 5? That depends -- did the threat actors access or exfiltrate any ePHI? Does the hospital even know whether the attackers got ePHI? Many entities report that they believe there was no access or exfiltration, but then later found out that there was. Adams may not know for sure until Conti dumps more data -- if they do. In the meantime, there is nothing on the hospital's site to indicate any attack and nothing on HHS's public breach tool.

Higginbotham Family Dental has ten offices in Arkansas, Tennessee, and Missouri locations. The practice, which appears to be covered by HIPAA, was added to Conti's site on September 15. After getting no reply to an inquiry using their contact form, DataBreaches.net emailed Higginbotham on September 17 and specifically mentioned some of the ePHI that the threat actors had dumped. The dump, consisting of more than 700 files, was mostly image files, many with names in the filenames, and there were a number of QR codes with what appear to be first initial and last name in the filename. The codes appear to be employee-related codes for keeping track of their work time on buddypunch.com.

There were also a number of deposit reconciliation files and other files. DataBreaches.net does not know whether the threat actors acquired much ePHI or not. DataBreaches.net reached out to the practice again recently, but has received no response again. As of today's date, there is no notice on their web site, and no notification on HHS's public breach tool. DataBreaches.net does not know if they have mailed notifications to patients or submitted notifications to any state attorneys general.

New York Foundation for Senior Citizens was added to Conti's site on September 17. NYFSC is not a HIPAA-covered entity as far as this site can determine, but would have other notification obligations. The threat actors dumped dozens of files with personnel and personal information, including many files with guardianship-related financial accounting to courts and bank account information. We also saw a psychiatric evaluation on a senior citizen that contained sensitive information. NYFSC has no notice on their site, and did not respond to an email inquiry sent September 17. A second inquiry was sent this week, but no response was received.

Family Health Centers Of Georgia Inc was added to Conti's site October 19, 2020. FHCGA is covered by HIPAA. The attackers posted some old personnel files relating to an administrator and also some old log files. They also posted a copy of the _r3adm3.txt file they uploaded on FHCGA's server.

FHCGA has not posted any notice about any attack on their site as of today's date.

Riverside Community Care Inc was added to Conti's site October 21, 2020. Riverside provides behavioral healthcare and human services to children, their families, and adults. They also provide community programs and services. RCC is covered by HIPAA.

Conti posted a few files as proof -- one contained the names, home addresses, and cellphone numbers of staff. Another contained a discharge summary with medications on a patient. Another contained home health care plan for a named patient that has all his details including a diagnosis of schizophrenia.

DataBreaches.net sent Riverside an email inquiry with specific details on October 21. They did not respond at all and there is nothing on their web site as of today to warn people that their personal and possibly sensitive information is in the hands of criminals.

Out of the 6 Conti incidents described above, none appear to be listed on HHS's public breach tool, none appear to have notices on their web sites, none have issued any press release, and we have not seen any notice on any state attorney general's site.

Incidents Posted by Maze Team

The following incidents were listed on Maze Team's dedicated leak site. As background: Maze initiated the model that includes publicly naming victims and dumping data on a dedicated leak site to increase pressure on victims to pay. Eventually, ransomware threat actors also added a second ransom or extortion demand to their model: pay us for the decryption key to unlock your systems that we encrypted, and then pay us extra to delete all the data we dumped on the internet and that we have stored. In January, 2020, this site began to track their listings from the U.S. medical sector. Not all of Maze's attacks that involve medical or health-related entities can still be found on what remains of their dedicated leak sites. This past week, Maze announced that they are closing their "project." Others have suggested that they are now "Egregor," although they have denied it. In some cases incidents were removed from Maze's site because the victim presumably paid ransom.

Crossroads Technologies is no longer listed on Maze's site, but in January and February, this site reported on that attack. By the end of January, there had been one report to a state attorney general's office. Eventually 17 Personal Touch Home Care units reported the Crossroads breach to HHS and state regulators. The Personal Touch reports accounted for more than 157,000 affected patients reported to HHS.

Stockdale Radiology in California was one of Maze's victims in January, and this site reported the attack on January 21. When their name was removed from Maze's leak site, the threat actors told me that they had reached an agreement with the practice. Even though their files with ePHI were removed from the leak site, this was a reportable HIPAA breach and on March 27, Stockdale reported the incident to HHS as impacting 10,700 patients.

Sunset Cardiology was also attacked in January. This site reported it on January 31. Maze did not dump a lot of data from this group -- only a handful of files with PHI. There was nothing ever posted on HHS's public breach tool, and of four email inquiries sent to the practice, two bounced back, and two to the email address listed on their site came back "Access denied." So were patients or regulators ever notified? We have no evidence that they were.

Affordacare Urgent Care Clinic in Texas was attacked in early February. DataBreaches.net reported on the attack in March, here. The attackers dumped a tremendous amount of ePHI, including insurance information. On March 31, this site reported that patients had been notified -- but had been misinformed about SSN not being involved. On April 3, Affordacare revised their notification to include patients' SSNs. On March 31, Affordacare notified HHS that 57,411 patients had been affected by the attack.

Kristin Tarbet, M.D. has a plastic surgery practice in Washington state. Maze attacked the practice on May 1, as this site reported on May 5. There was a large amount of personally identifiable information (PII) and protected health information (PHI) dumped freely and publicly on Maze's onion site and clearnet site. I have not found any public disclosures from Dr. Tarbet about the breach and it is not on HHS's public breach tool even 6 months later. Dr. Tarbet has not responded to any inquiries from this site. ***Update****: This may have been disclosed in a press release on Oct.26 as Amara Medical Aesthetics, but is not on HHS's breach tool.*

The day after Maze posted Kristin J. Tarbet, M.D., they added a second plastic surgery group to their leak site: Nashville Plastic Surgery Institute, LLC, dba **Maxwell Aesthetics**. As they did to Dr. Tarbet, the threat actors dumped a lot of patient information, as DataBreaches reported here. The owner called

DataBreaches.net when he saw this site's reporting to ask where the data had been dumped so he could take action. On June 30, the practice notified HHS that 656 patients had been impacted.

At some point (date unknown to DataBreaches.net), Maze added **Medical Management, Inc**. to their site. On inspection, the files involved electronics claims processing with ePHI that includes health insurance information. DataBreaches.net cannot find any media coverage of this attack, nor any notification to HHS. On November 3, more than four months after the exfiltration likely occurred, DataBreaches.net reached out to MedMan to inquire about their incident response and any notifications, but received no response.

As noted in the Conti listings, Maze also listed **Ventura Orthopedics Inc.** as one of their victims. As also noted previously, we could find no notification to HHS or California and no notice on Ventura Orthopedics' web site. It is now three months since Maze first listed them.

At the end of August, Maze added **United Memorial Medical Center** in Texas to their leak site. DataBreaches.net reported on it on August 30. UMMC never answered this site's inquiries at the time, and there is no statement on their site or any press release or posting on HHS's site. DataBreaches.net sent a follow-up inquiry to UMMC to find out what, if anything, they have ever done in response to the attack, but received no reply. UMMC had been heavily impacted by the COVID-19 situation prior to the ransomware attack, which may account for them not responding to this site's earlier inquiries, but have they done anything to alert patients and help protect them from the claimed ransomware attack?

Abington Reproductive Medicine was also added to Maze's leak site. The medical practice did not respond to inquiries from this site, but of note, the "proof" that Maze provided had nothing to do with any medical practice at all. Did Maze really attack Abington and just upload the wrong proof, or didn't they attack them? DataBreaches.net sent Abington (now Sincera) two inquiries but received no reply.

Of the 10 Maze listings, we have only seen notifications or statements from four of the entities.

Incidents Posted on Other Leak Sites

The following incidents were seen on other dedicated leak sites by other ransomware threat actors in 2020:

In May, **AKO** threat actors added **North Shore Pain Management** to their dedicated leak site, as DataBreaches.net reported on May 13. They dumped more than 4 GB of data that included patient names, addresses, Social Security numbers, health insurance info, and more. On June 18, the medical group notified HHS of the incident, reporting that 12,472 patients were impacted. They also dutifully reported the incident to the Massachusetts AG Office.

AKO recently rebranded itself as **Ranzy.**

REvil (Sodinokibi) threat actors added **Valley Health System** in Virginia to their leak site in August, as reported by DataBreaches.net. Data dumped included PII and PHI. Valley Health's name was subsequently removed from the leak site. A spokesperson for Valley Health later informed DataBreaches.net that less than 15 patients had their data stolen and those patients have all been notified by letter. HHS will be notified following the requirements for "less than 500" incidents.

REvil also recently added **Beacon Health Solutions, LLC.** The entity was added on or about October 21, although from time stamps, the data may have been exfiltrated in mid-September. Consistent with their handling of other victims, the attackers began by posting screenshots of directories of the victim's systems, with a few files. On November 6, REvil started dumping the Clients data.

Beacon provides integrated health benefits and claims administration solutions for covered entities. It would be covered by HIPAA as a business associate. As of publication time, there is nothing on Beacon's site to indicate any breach or compromise, and there has been no response to emailed inquiries and requests for statements, even though the attackers have started dumping actual files.

Nefilim threat actors added **Luxottica** to their dedicated leak site on October 18. The Luxottica attack had received media coverage at the time of the attack in September. Luxottica is the parent company of Ray-Ban, Sunglass Hut, Pearle Vision, LensCrafters, and EyeMed. While Luxottica publicly acknowledged a breach, their disclosure initially claimed that no personal information was compromised-- a claim that the attackers refuted on their dedicated leak site.

Also in October, Luxottica announced what appeared to be the discovery of an earlier breach -- one that had occurred on August 5 and was discovered on August 9. Bleeping Computer has more details on that one, which Luxottica admits did involve patient and customer information. But was this attack also by Nefilim? Was it connected to the ransomware attack in September? Luxottica has not responded to inquiries this site sent it last month and then again days ago -- including an inquiry about a tip this site received that 800,000 were impacted by the compromise of their appointment scheduling system in August.

In the interim, the threat actors continue to dump more data from the ransomware attack. None of the above has shown up on HHS's public breach tool. There is an EyeMed attack that occurred at the end of June that has been reported by both EyeMed and a health plan, but that is not the ransomware incident.

Elsewhere, **SunCrypt** ransomware operators attacked **University Hospital New Jersey (UHNJ).** DataBreaches.net reported on the breach on September 15. At the time , the attackers dumped 48,000 files from what they claimed was a 240 GB dump. Following media coverage, the hospital's name disappeared from the leak site. We subsequently learned that the hospital paid $672,744 ransom to get the attackers to remove the data dump and to allegedly destroy it.

Almost two months later, there still does not appear to be any statement on the hospital's website or on HHS's public breach tool. Using the 60-day window as the outer limit, UHNJ should notify HHS and patients no later than November 15.

In the aftermath of the UHNJ attack, SunCrypt pledged that they would not attack any more medical entities.

On September 13, **Pysa** threat actors added **Assured Imaging** to their leak site. The provider of diagnostic and mobile mammography services had already disclosed the breach on their own site by then, however, having become aware of the attack on May 19. On August 26, Assured Imaging also notified HHS that the attack impacted 244,813 patients. The data dump contains a lot of PHI that is mostly mammography pre-screening histories or forms. The scans DataBreaches.net skimmed did not contain SSN, but did contain medical record number, names, addresses, date of birth, referring physician, health insurance carrier information, and reason for scan with relevant personal and family history.

Pysa also added **Piedmont Orthopedics | OrthoAtlanta** to their leak site. The dumped files included a lot of financial files, but there was patient information accessed and exfiltrated that may have included patient names and addresses, birthdates, phone numbers, medical or health insurance information and social security numbers. On September 18, the practice published a notification on their web site. OrthoAtlanta also notified HHS that the breach impacted 5,600 patients.

NetWalker threat actors also attacked some medically related facilities, including **Lorien Health Services** in Maryland. Maryland Health Enterprises d/b/a Lorien Health Services was attacked on June 6 and by mid-June, they had been listed on NetWalker's leak site. The screenshots offered as proof included directories of folders from the Lorien's system, but also one admission record with personal information. They subsequently dumped some of Lorien's data. In response, Lorien promptly reported the incident to Maryland's Attorney General and by mid-June had notified patients and issued a press release that revealed that 47,754 patients had been impacted.

Olympia House in Petaluma, California was also attacked by **NetWalker**, as first noted on this site on August 10. Olympia House provides residential and outpatient services to those with addiction problems. The screenshots NetWalker posted as proof included one with patients' first and last names and their dates of admission. Other screenshots revealed others' names as part of file names or in redacted screenshots showing driver's licenses or health insurance information. The actual data dump, however, was not working -- it is not clear whether this is intentional on NetWalker's part, as many of their data dumps either expire before they go live or have passwords that do not work. That may be a blessing for patients whose data are in the dump, but does not negate any obligation to notify them or regulators on the part of HIPAA covered entities. Olympia House does appear to be a HIPAA covered entity, but there is no notice on their web site and nothing on HHS's public breach tool or the California AG's site. DataBreaches. net contacted them in August and again on November 4 after finding no notice on their site, no notice on HHS's public breach tool, and nothing on the California AG's site. They have not responded at all.

The Center for Fertility and Gynecology in Los Angeles was also added to **NetWalker'**s leak site at the beginning of August. The screenshots and data dump included routing business files for the practice, but also included employee data and patient information. DataBreaches.net contacted them on August 30 and again on November 4, but received no replies. There is nothing on their web site or HHS's public breach tool or the California AG's site.

Most recently NetWalker added **Wilmington Surgical** in North Carolina to their leak site. The threat actors posted screenshots showing directories of files on the surgical group's system. DataBreaches.net reached out to Wilmington Surgical on October 21 and again on November 4, seeking information on their incident response. So far, there is nothing on their site, on HHS, or on any state attorney general site that publishes their reports online.

On September 24, HHS Cybersecurity Program issued an alert about NetWalker ransomware. Their report included some of the incidents mentioned here as well as NetWalker's attack on ***Champaign-Urbana Public Health District*** *in March, their attack on* ***Crozer-Keystone Health System*** *in Pennsylvania, and the* ***UCSF School of Medicine*** *attack where the university paid $1.4 million.*

Egregor threat actors added **Dyras Dental** in Michigan to their leak site in September. The data dumped by the attackers as initial proof contained more than 100 files, almost all of which dealt with financial aspects such as insurance billings with patient protected health information, employees' W-2 statements, and voice mail recordings containing patient-related information. Dyras did not respond to two inquiries sent to it in September and October. There is no statement to be found on their web site, and I can find no press release or mention of them on HHS's public breach tool.

Mount Locker is reportedly claiming responsibility for an October attack on **Sonoma Valley Hospital** in California, and reportedly dumped 75 GB of data, but DataBreaches.net was unable to find any actual data dump, although the hospital's name does appear on the threat actor's leak site. The dump, reported by a well-known site, may have been removed as part of some renewed negotiations or something.

DoppelPaymer threat actors added **Med-Care Infusion Services, Inc**. to their dedicated leak site on October 16. Med-Care is a specialty pharmacy in Florida. The threat actors posted two documents as proof of access. Neither contained any personally identifiable information or protected health information, leaving us in the dark as to exactly what data the attackers may have accessed and exfiltrated. Med-Care has ignored two email inquiries from this site on October 16 and October 21. There is no notification or anything on their site to suggest that anything is amiss.

Of the 14 incidents mentioned in this subsection, we have found notifications to patients or regulators for 7 incidents.

Conclusion

In this report, we described 30 incidents where patient data is already in the wild and being shared and/or misused, and yet only 11 entities have notified regulators or patients, or even posted or published some kind of preliminary warning/alert to patients to take precautions. In many cases, the only way a patient might have early warning is if they happen to read a site that is reporting on the breach or data dump.

The 30 incidents included in this report are just those that this site is aware of. We know that there are many other ransomware attacks hitting healthcare entities. Some of those threat actors have hit major entities, such as the UHS attack that was never posted on any leak site, or the Blackbaud attack that involved information on what this site projects to be more than 12 million patients.

HIPAA's notification requirements were written at a different time and with different understanding of criminal attacks and breaches. While we need to remain realistic and supportive of victim entities, we need to remember that people are at greater risk nowadays when data is stolen and then dumped publicly for the world to freely access and take.

If the legislature thinks I'm just dead wrong (which wouldn't surprise me), then perhaps HHS would at least consider issuing more recommendations of revised best practices for incident response. Those recommendations might usefully include:

1. Having a monitored email account or phone number for receiving alerts or notifications if someone finds your data leaking online due to a misconfiguration or dumped on line by criminals. Feel free to call this requirement, "Dissent's Law."

2. Requiring entities to issue a public notice or statement on their web site within 48 hours of discovery, where "discovery" is defined as being notified of a data dump or leak that involves PII or PHI, or receiving a ransom demand accompanied by proof of data access or exfiltration.
3. Preliminary or "early warning" public notifications should not be permitted to include any claims that criminals have promised to delete and not misuse data -- unless such statements are accompanied by a statement that criminals lie and no one should believe their assurances. Nor should entities be permitted to include any assurance that the entity doesn't believe any personal information was acquired, as entities have been all-too-frequently wrong about that. The purpose of the early notification is to encourage protective action, not to make people feel that they are not at imminent risk. Finally:
4. HHS should immediately begin to take enforcement action against entities that have not disclosed reportable data leaks or breaches within the currently required timeframes. Failure to disclose or report is too common. It's time for HHS to send a strong message that "without undue delay" means entities cannot take 60 days when patients' data has been dumped.

I realize that my recommendations may be discounted or dismissed by others. That's fine -- as long as you come up with some way to better protect patients than what we are currently doing, because if only 11 out of 30 are warning patients that their data has been stolen and some data has been dumped already, we are not protecting patients well.

Any corrections or updates to this report can be e-mailed to breaches[at]databreaches.net.