Volume XXVIII, Number 7 Monday, May 24, 2021

Specialized Information Publishers Foundation
EDITORIAL EXCELLENCE AWARD WINNER

Ransomware Attacks:
Dangerous Threat to All Labs!
(See pages 8-11.)

From the Desk of R. Lewis Dark...

THE DARK REPORT

RELIABLE BUSINESS INTELLIGENCE, EXCLUSIVELY FOR MEDICAL LAB CEOs / COOs / CFOs / PATHOLOGISTs

INSIDE THIS ISSUE

Restricted information, see page 3

COMMENTARY & OPINION by...

R.Lewis Dark

Founder & Publisher

Goodbye Pandemic! Hello Ransomware!

Being first to predict an important trend's arrival or departure can bring accolades for perceptive foresight or rebukes for getting it wrong. This issue of The Dark Report puts us on the record for making early predictions on two trends, each with the potential to financially make or break your clinical laboratory or pathology group.

First, in our intelligence briefing on pages 3-7, we assess the COVID-19 data reported daily by the federal **Centers for Medicare and Medicaid Services** (CMS). As you will see, daily numbers of new COVID-19 cases, hospitalizations, and deaths have declined dramatically from their peaks early this year. For example, there were 18,692 new cases on May 17. That is a 94% reduction from the peak daily number of 312,824 new cases on January 8. This is strong evidence to support the prediction that the SARS-CoV-2 pandemic is waning.

Second, pages 8-11 present our intelligence briefing on the trend of ransomware attacks on healthcare providers, including clinical laboratories. The Dark Report is the first lab industry publication to provide an assessment of this threat, specifically as to why clinical laboratories can simultaneously be at risk for two highly-disruptive events. A single ransomware attack can shutdown access to all your lab's IT systems and databases, while at the same time breaching patients' protected health information (PHI). For this reason, defending against ransomware attacks should be a strategic priority for all clinical laboratory managers and pathologists.

But that's not all the bad news. Hackers and the parties behind these ransomware attacks are becoming increasingly sophisticated. No lab should consider today's defenses adequate to protect against tomorrow's ransomware attack.

This is why I titled today's opinion and commentary "Goodbye Pandemic! Hello Ransomware!" We believe the evidence strongly supports the prediction that the COVID-19 pandemic is waning. Whether it will resurface next influenza season or more virulent variants appear has yet to be determined.

Similarly, the increase in ransomware attacks against healthcare providers—most kept secret from the public—is powerful evidence that a new trend threatens all providers, including clinical laboratories and pathology groups. TDR

Predicting Future Demand for COVID-19 Testing

Clinical labs have important question to answer: What volume of SARS-CoV-2 tests will be needed?

CEO SUMMARY: After 15 months of the pandemic, the nation's clinical laboratories are at an interesting crossroads. Is the COVID-19 outbreak diminishing and close to disappearing? Or might it intensify again, particularly when the traditional influenza season arrives next fall? There has been an 82% drop in the daily number of molecular COVID-19 tests since January. To help clinical laboratories plan for the future, THE DARK REPORT surveys key trends in the current COVID-19 pandemic.

WILL THE COVID-19 PANDEMIC EMULATE THE CLASSIC ADAGE that "if March comes in like a lion, it will go out like a lamb?"

The pandemic certainly "came in like a lion" when it hit the United States, and the entire world, with full force in March 2020. Every aspect of clinical care and normal human activity was disrupted. Clinical laboratories played a key role in ramping up the SARS-CoV-2 testing required to respond to the pandemic.

Now, 15 months later, there is growing evidence that COVID-19 could possibly "go out like a lamb." If true, this has many clinical, operational, and financial implications for clinical laboratories and pathology groups.

In particular, labs have the pressing need to predict what volume of COVID-19 molecular tests will be needed in their communities for the balance of the year. An accurate prediction is essential to drive planning, staffing, spending, and revenue.

As clinical lab administrators and pathologists conduct planning and develop strategies associated with the COVID-19 pandemic, a prediction of higher levels of testing will require labs to perform more tests and incur more costs. But the increased testing also will generate more revenue from COVID-19 test claims.

The opposite is true if the prediction is for less demand for COVID-19 molecular tests. Labs will need to plan for a smaller volume of these tests, resulting in lower costs associated with SARS-CoV-2 testing and less revenue because of fewer COVID-19 test claims.

In the United States, the third wave of the pandemic crested on Jan. 8, 2021,

THE DARK REPORT Intelligence Briefings for Laboratory CEOs, COOs, CFOs, and Pathologists are sent 17 times per year by The Dark Group, Inc., 21806 Briarcliff Drive, Spicewood, Texas, 78669, Voice 1.800.560.6363, Fax 512.264.0969. (ISSN 1097-2919.)

R. Lewis Dark, Founder & Publisher. Robert L. Michel, Editor.

SUBSCRIPTION TO THE DARK REPORT INTELLIGENCE SERVICE, which includes THE DARK REPORT plus timely briefings and private teleconferences, is $15.27 per week in the US, $15.27 per week in Canada, $16.05 per week elsewhere (billed semi-annually).

when the CDC reported a record number of 312,824 new COVID-19 cases. The number of deaths per day peaked on Jan. 7 at 4,131. Since then, the number of new cases and deaths per day in this country have continuously declined.

94% Fewer Cases Per Day

This slowdown in new cases of SARS-CoV-2 infections is reflected in recent statistics. As of May 17, the CDC reported daily new COVID-19 cases and deaths as 18,692 and 679, respectively. That is a decline of 94% and 86% in the number of daily new cases and deaths since the January peak for both statistics.

Not surprisingly, the demand for molecular COVID-19 tests collapsed in parallel with the decline in new cases. It was on Jan. 6, 2021, when the CDC reported a record daily total of 2,315,502 COVID-19 tests. As of May 18, that number had fallen to 385,860 tests for the day. This is a decline of 82% in the daily volume of COVID-19 tests over the past five months.

The timing of this decline coincides with the first release of the COVID-19 vaccines in late December and early January. Priority was given to essential workers—including healthcare workers and medical laboratory professionals—and then expanded to include elderly and those with specific chronic conditions.

Vaccination Factor

As of May 20, CDC data show that 127.8 million Americans are fully vaccinated. That is 38.5% of the population. Another 10% of the population have received at least one vaccination shot. COVID-19 cases in this country now total 32.8 million, or about 10% of the population.

Epidemiologists arguing in favor of a diminishing pandemic point out that more than half the population of the United States now has some level of immunity to SARS-CoV-2.

Clinical lab executives and pathologists will want to interpret the significance of these statistics that document a decline in incidences of COVID-19 in the United States since the start of 2021.

Labs also should consider another important factor in their strategic planning—falling consumer demand for both COVID-19 tests and vaccinations. One major reason for the substantial decline in the number of daily COVID-19 tests performed by the nation's clinical labs is simply that many Americans no longer want to be tested.

This phenomenon differs from COVID-19 testing required by an employer, university, or school for regular testing of employees, faculty, and students. These organizations may require rapid COVID-19 tests for months into the future simply to reduce their liability. They are concerned about being named as a defendant in potential lawsuits, for example, if an employee, customer, or student becomes infected and files a lawsuit claiming to have been exposed to SARS-CoV-2 while working, studying, or shopping at the organization.

Serology Testing for COVID

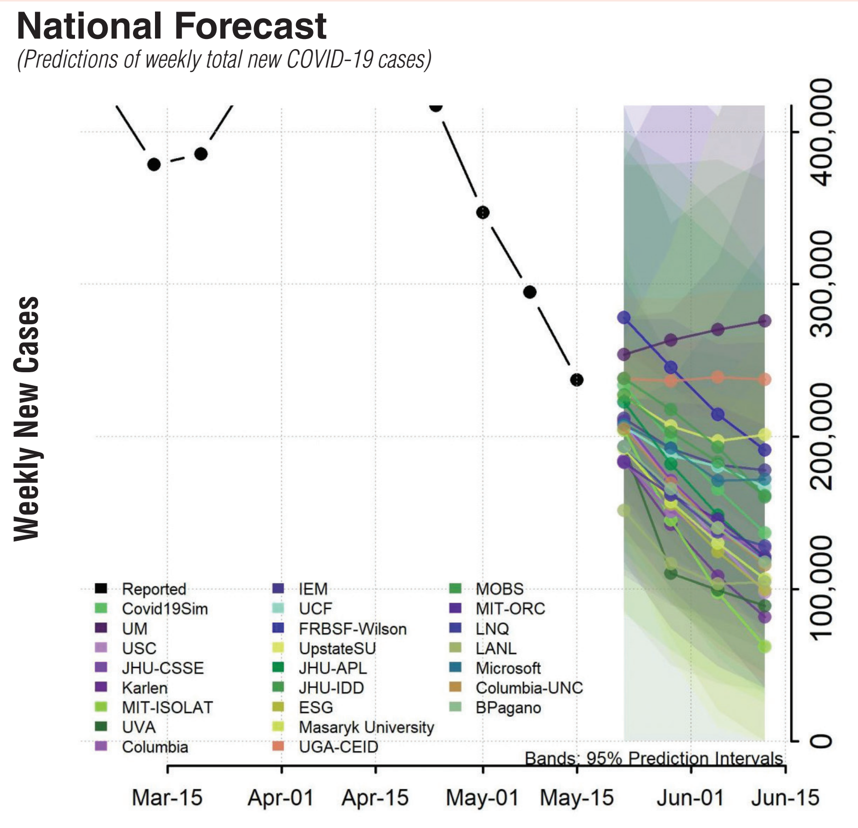
The facts presented here deal with molecular COVID-19 testing. Separately, clinical labs will need to watch the development of accurate serology tests for SARS-CoV-2. In the early months of the pandemic, many experts believed serology testing would play a greater role in helping physicians and public health officials track outbreaks and identify individuals with existing antibodies to COVID-19. As of this date, that has not happened.

There are two other factors to consider. One: that new variants may emerge which are more infectious and/or cause a more severe form of the disease. Two: it has yet to be determined how long current vaccines will protect the individual from infection. If protection is not long-lasting, there may be the need for serology testing of vaccinated individuals to determine when and if they need a booster shot. The charts on pages five, six, and seven will help clinical labs and pathology groups with their strategic planning. TDR

CDC's Current Predictions of COVID-19 Cases Show Steady Decline in Weekly Numbers

CLINICAL LAB ADMINISTRATORS AND PATHOLOGISTS TASKED WITH PREDICTING the uncertain future of the COVID-19 outbreak in the United States will find a useful tool on the website of the Centers for Disease Control and Prevention (CDC).

The CDC tracks the predictive models of 28 different entities. It publishes updates that show the number of weekly new COVID-19 cases in past weeks and what the 28 models predict will be the number of new cases in the coming four weeks.



- This chart was posted on the CDC website as of May 21, 2021. It shows "ensemble forecasts of new reported COVID-19 cases over the next four weeks, included are forecasts from 28 modeling groups, each of which contributed a forecast for at least one jurisdiction."
- This week's national ensemble predicts that the number of newly reported COVID-19 cases will likely decrease over the next four weeks, with 60,000 to 268,000 new cases likely reported in the week ending June 12, 2021.
- It is significant that only three of the 28 different models predict an increase in the number of weekly new COVID-19 cases in the coming four weeks.

CDC Statistics Demonstrate the Steady Decline of the SARS-CoV-2 Outbreak in the United States

Chart A: Trends in Number of Daily New COVID-19 Cases in the US

(Reported to CDC, by State/Territory)

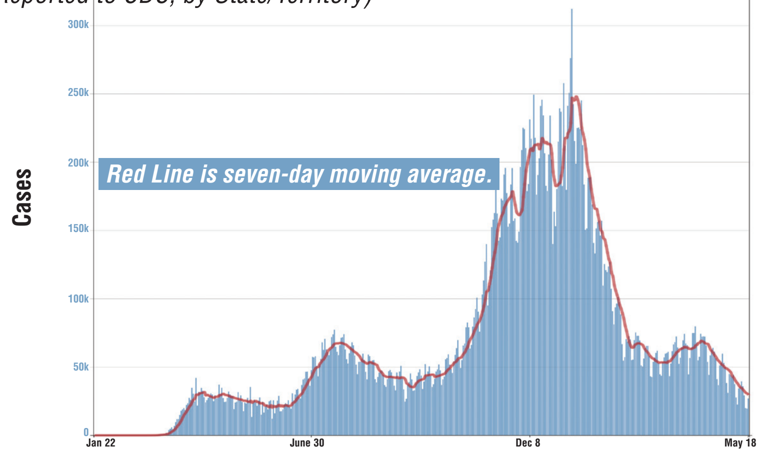


CHART A SHOWS HOW THE THIRD WAVE OF SARS-COV-2 CASES peaked in early January, 2021, then declined steadily in recent months. Highest number of COVID-19 cases per day was on Jan. 8, 2021, with 312,824 cases per day. COVID-19 cases per day on May 17 was 18,692. This is a 94% reduction in new cases per day from the peak day in January 2021.

Chart B: Trends in Number of COVID-19 Deaths in the US

(Reported to CDC, by State/Territory)

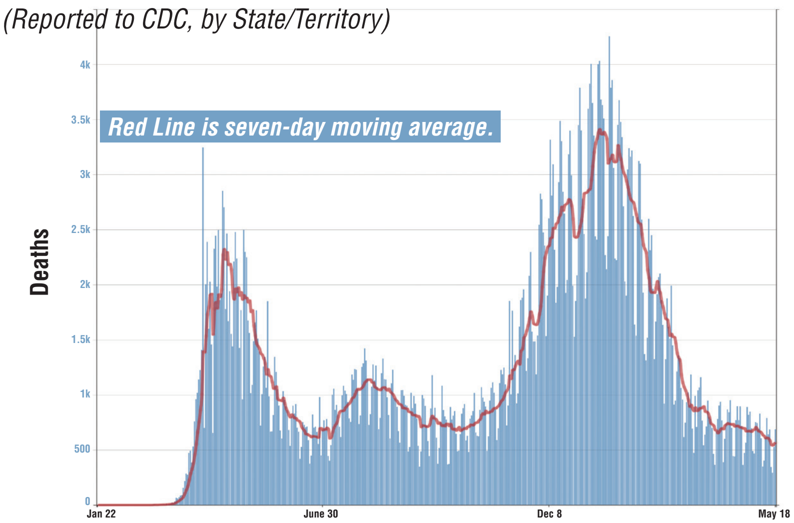


CHART B TRACKS THE NUMBER OF DEATHS PER DAY SINCE THE ONSET OF THE PANDEMIC in early 2020. Highest number of COVID-19 deaths per day was Jan. 7, 2021, with 4,131 deaths on that day. Daily deaths from COVID-19 declined steadily since that date. On May 18, there were 679 deaths from COVID-19 reported to the CDC and that represents an 86% reduction from the peak of 4,131 deaths on Jan. 7.

Chart C: Daily COVID-19 Viral (RT-PCR) Laboratory Tests Performed and COVID-19 Viral (RT-PCR) Laboratory Test 7-day Percent Positivity

(Reported to CDC, by State/Territory)

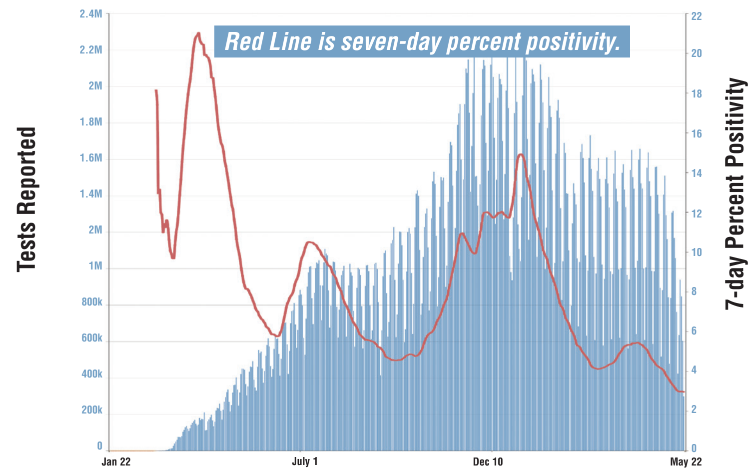


CHART C PRESENTS THE DAILY NUMBER OF MOLECULAR COVID-19 TESTS. The highest number of COVID-19 tests per day was on Jan. 6, 2021, with 2,135,502 tests reported that day. By comparison, the number of COVID-19 tests per day on May 18 was 385,860, an 82% reduction from the peak day of Jan. 6. This chart also shows the decline in the percent of positive tests, which has fallen to under 2%.

Chart D: Prevalent Hospitalizations of Patients with Confirmed COVID-19

(Reported to CDC, United States, August 1, 2020–May 19, 2021)

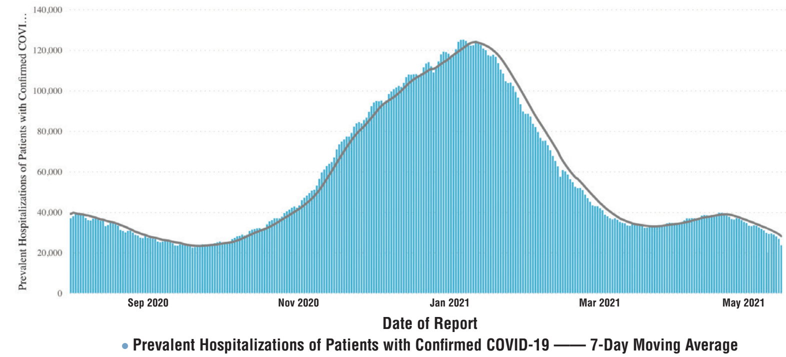


CHART D CONTAINS THE DATA ON THE NUMBER OF PREVALENT HOSPITALIZATIONS FOR PATIENTS CONFIRMED POSITIVE FOR SARS-COV-2. Peak seven-day average was 123,845 between Jan. 5-Jan. 11, 2021. For the seven days of May 13-May 19, 2021, the average was 25,313. That is 80% less than the peak seven-day average of prevalent hospitalizations.

Ransomware Attackers Target Health Providers

Currently, Scripps Health is in the news as it battles a ransomware attack that struck on May 1

CEO SUMMARY: Both malware and ransomware have been around for a number of years. But the attacks launched today against healthcare providers are more sophisticated and better at achieving the total shutdown of targeted hospitals, doctor groups, and clinical laboratories. For this reason, clinical labs and pathology groups should put ransomware high on their list of threats. They should also regularly assess and upgrade their defenses against both malware and ransomware.

If you are not familiar with the term "ransomware," you soon will be. Ransomware is poised to become the single biggest threat to your clinical laboratory, parent hospital, or anatomic pathology group.

Ransomware is defined by **Oxford Languages** as "a type of malicious software designed to block access to a computer system until a sum of money is paid."

Ransomware and Malware

As a concept, ransomware is simple: hackers find a way into your organization's digital systems. They insert malware (another term you will want to understand better) which encrypts your lab's data files and computer systems. From that moment forward, there is a shutdown of all or most digital systems and it becomes impossible to access the company's data files.

This happens suddenly and without warning. Once the malware is implanted, the files cannot be decrypted without a mathematical key known only by the attacker. The hackers will send a message to your lab's IT team announcing the attack and that your lab's data systems and files are locked and inaccessible. The only way your lab can decrypt the files and gain access to the systems is for you to transmit an untraceable Bitcoin payment to the attacker.

The latest major health system to be attacked by malware is **Scripps Health** in San Diego. On May 1, the attackers successfully encrypted the files and locked Scripps out of certain essential information systems. The situation became news in the following days, primarily because patients complained that they could not access their digital health records, make appointments, or send emails to their physicians.

Administrators at Scripps said little about the situation. On May 10—days later—it issued a public statement. That document acknowledged the attack, stating, in part, "As you know, on May 1st Scripps was hit with a cybersecurity incident with malware placed on our information system. Our team prepares for this type of situation and immediately took steps to contain the malware by taking a significant portion of our network offline."

Scripps scrambled to establish procedures to keep emergency departments and other clinical services operating. In some cases, this included use of paper forms.

Within the San Diego medical community, this malware attack has disrupted normal care. Scripps Health operates five hospitals and 19 outpatient facilities. It has 2,600 affiliated physicians and treats about 500,000 patients annually.

Restoring Digital Systems

As of May 20, Scripps Health announced that its *scripps.org* website was again up and running. However, local news sources said the system's "My Scripps" digital portal, which patients use to make appointments and communicate with their doctors, "was still returning an error message as of the early afternoon."

On May 21, reporter Lisa Morgan of *Cyber Security Hub* wrote, "high-risk patients such as heart attack, stroke, and trauma patients have been funneled from **Scripps Memorial Hospital La Jolla** to other hospitals nearby. Some patients are complaining that they are having trouble making appointments with other doctors and that Scripps is not referring patients to other doctors."

Similar to the Scripps Health attack, another ransomware attack with national ramifications happened on May 7.

Colonial Pipeline Hacked

As reported by the national news media, the 5,500-mile petroleum pipeline operated by **Colonial Pipeline** was shut down after hackers encrypted the company's data systems and sent a ransom demand to the company.

This pipeline delivers 45% of all the gasoline, aviation fuel, and other products—about 100 million gallons per day—from refineries in Houston to states on the East Coast. As of last Wednesday, 9,500 gas stations were out of fuel in the 13 states and Washington, D.C., served by the pipeline.

After days of refusing comment on whether it was paying a ransom to obtain the decryption keys needed to access its data systems, Colonial Pipeline CEO Joseph Blount confirmed that his company did pay ransom.

The Guardian wrote, "Blount said Colonial paid the ransom in consultation with experts who previously dealt with the group behind the attacks, DarkSide, which rents out its ransomware to partners to carry out the actual attacks.

"Multiple sources had confirmed to the *Associated Press* that Colonial Pipeline had paid the criminals who committed the cyberattack a ransom of nearly $5M in cryptocurrency for the software decryption key required to unscramble their data network," *The Guardian* continued.

Cryptocurrency Payment

"A ransom payment of 75 Bitcoin was paid the day after the criminals locked up Colonial's corporate network, according to Tom Robinson, co-founder of the cryptocurrency-tracking firm **Elliptic**," *The Guardian* said.

THE DARK REPORT is providing details on the Scripps Health and Colonial Pipeline ransomware attacks because each contains elements common to most ransomware attacks. Understanding how these ransomware attacks are conducted is essential if clinical laboratory administrators and pathologists are to work with their chief information officers, attorneys, and outside experts to harden their labs' defenses against attackers using ransomware or malware.

During interviews, executives at companies who were victims of ransomware attacks, and several lab industry attorneys who have worked with client labs similarly attacked with ransomware, described the common processes used by the hackers.

Once the target company's files and software systems have been encrypted, the hackers send an email describing their attack and demanding some amount of ransom. The email also states that if the target company refuses to pay the ransom, the hackers will use the stolen data—particularly data involving patients and customers—in ways that will harm the company and its reputation.

Third-Party Negotiators

Upon discovery of the shutdown of their data systems, most organizations will bring in their attorneys and retain consultants in cybersecurity and negotiations. The third-party negotiators handle communications with the hackers and understand the unspoken rules of negotiation.

For example, the organization's negotiators know how frequently the hackers will email or telephone. They understand the consequences should the organization not communicate with the hackers at expected points in time.

It is important for lab executives and pathologists to understand that negotiations do happen and are part of the ransomware attack. One example was shared with THE DARK REPORT by a business owner who was dealing with such an attack.

He explained that—not only did the attack encrypt every data function and software app used by his company—but the malware attack successfully encrypted all the company's back-up systems as well, including off-site and cloud-based backups. He said every data system in this $30 million company was encrypted, manufacturing stopped, and staff had no access to information when customers called seeking information.

Routine of Daily Calls

The company retained a negotiating consultancy firm. Each morning, the hackers called at a specific time. The owners were told that if they did not respond in a timely way, the hackers would simply walk away, leaving the company to solve the problem on its own.

The original ransom demand was for $500,000. Over 10 days, the third-party negotiators were able to reduce that down to about $240,000. The owners agreed to pay that amount in Bitcoin.

After the payment was made, a de-encryption key was received. However, according to this source, that key only unlocked certain software systems and databases. A substantial amount of the company's software products and databases remained encrypted.

Further negotiations to obtain a more complete de-encryption key were not successful. According to our source, the company will spend several million dollars over many months to restore the full performance of the company's information technologies back to how they functioned prior to the attack.

Protected Health Information

Clinical laboratory administrators and pathologists should recognize that a ransomware attack directed at their laboratory creates another problem. Yes, the encryption of software and databases denies the lab access to those functions. But the ransomware attack may also cause a breach of patients' protected health information.

This means that the victimized laboratory must also comply with federal HIPAA requirements as it responds to the ransomware attack. Along with notifying those patients whose protected health information (PHI) was breached, the provider must notify the federal government and may need to issue a press release to the news media, depending on the number of patients affected by the breach.

The value of PHI on the Dark Web is a major reason why hackers increasingly target hospitals, physician groups, clinical laboratories, anatomic pathology groups, and other healthcare providers. Not only can the hackers get paid a ransom from the victim, but they also can make money by selling the patient medical records they access.

Experian, the credit reporting agency, says patient health records can be sold for up to $1,000 each. This depends on how

Ransomware Attacks Generally Go Unreported and Healthcare Providers Are Ripe Targets

IT IS IMPOSSIBLE TO KNOW THE TRUE TOTAL OF RANSOMWARE ATTACKS against healthcare organizations in the United States for a simple reason: hospitals, physicians' offices, clinical labs, pathology groups, and other providers don't want the news to become public. One obvious reason is because of harm to the provider's reputation. But the other equally-significant reason is that when other hackers learn a healthcare organization paid a ransom, they want to attack that same provider because they know this provider will pay a ransom to regain access to its data and software systems.

One source of public information about malware attacks is the federal database of reported HIPAA breaches of protected health information (PHI). *Comparitech* writer Paul Bischoff studied the federal database for 2020 breaches. (To be reported to the public, a PHI breach must involve the data of 500 or more patients.) Bischoff published his findings on March 21, 2021, under the headline "Ransomware Attacks on US Healthcare Organizations Cost $20.8 Billion in 2020."

Included in the *Comparitech* report were these key findings:

- There were 92 individual ransomware attacks on healthcare organizations in 2020—a 60% increase from 2019.
- Over 600 separate hospitals, clinics, and other healthcare organizations were potentially affected (plus a further 100 providers in the Blackbaud attack).
- 18,069,012 individual patients/records were affected—470% increase from 2019.
- Almost 50% of Maine's population was impacted by ransomware attacks in 2020.
- Ransomware amounts varied from $300,000 to $1.14 million.
- Downtime varied from minimal impact due to frequent data backups, to weeks or months of paper-only systems. One healthcare organization even lost all of its patient records in an attack.
- Based on the average ransom demand in 2020 ($169,446 according to the average across all of the quarterly reports from **Coveware** data), hackers demanded an estimated $15.6M in ransoms.
- In 2020, hackers received at least $2,112,744 in ransom payments (plus the undisclosed amount paid by Blackbaud and several other attacks).
- The overall cost of these attacks is estimated at around $20.8 billion (which includes downtime, cost of providing security services to patients whose PHI was breached, cost of bringing systems back into operation, and other related expenses).

complete the data file is and whether it is a single record or an entire database.

Thus, after Farmingdale, N.Y.-based **Apex Laboratory** was hit by DoppelPaymer ransomware in mid-2020, the hackers posted the medical records of 10,000 patients it stole from Apex.

Assuming a value of $500 per record (half of Experian's estimate of $1,000), potentially these hackers could have harvested a $5 million payday from that part of the ransomware attack.

Unfortunately, ransomware attacks are now a fact of life in the healthcare and clinical lab industry. For that reason, lab administrators would be well-advised to regularly assess and strengthen their labs' defenses against this threat. TDR

$400,000 Settlement in VA Wrongful-Death Case

Citing malpractice, daughters of deceased veteran sued a former VA pathologist, the VA, and the USA

CEO SUMMARY: Did "the system" fail patients and physicians at one Veterans Health Administration center? The public disciplinary records of pathologist Robert Morris Levy over several decades show that any laboratory employing Levy had reason to monitor closely the accuracy of his diagnoses and his sobriety on the job. In March, the federal government agreed to settle a case filed by family members of a veteran who died as a result of Levy's inaccurate cancer diagnosis. Might greater oversight of Levy by VA officials have prevented his diagnostic errors?

NOW THAT A DISGRACED PATHOLOGIST IS SERVING TIME in federal prison on criminal charges related to misdiagnoses of cancer cases and other issues, his former employer has settled at least one lawsuit filed by family members of a now-deceased patient whose cancer was misdiagnosed.

In a wrongful-death case, the federal government agreed to pay $400,000 in March to the estate of a U.S. veteran who died after the now-jailed pathologist at the **Veterans Health Care System of the Ozarks** failed to spot a malignant tumor, a misdiagnosis that led to the veteran's death in 2014, court documents show.

Settlement Agreement

Attorneys from the federal **Department of Justice** (DOJ), and for the executors of the estate of the deceased veteran, reached the agreement on April 15 to settle the case rather than go forward with a trial in the **U.S. District Court for the Western District of Arkansas**, in Fayetteville.

The case offers lessons for any clinical laboratory or anatomic pathology group that employs or contracts with anatomic pathologists or clinical laboratory scientists who may be under the influence of drugs or alcohol, or otherwise impaired, while at work, as THE DARK REPORT previously noted. *(See sidebar "Attorney Identifies Useful Lessons to be Learned from Levy Case for Clinical, Pathology Labs," on page 15, and "Pathologist's Prison Term Is a Warning for AP Groups," TDR, March 1, 2021.)*

In January, the pathologist, Robert Morris Levy, MD, was sentenced to 20 years in federal prison and ordered to pay a fine of almost $500,000 following his conviction on charges of involuntary manslaughter and mail fraud.

The DOJ alleged that Levy was under the influence of alcohol and drugs over multiple years, and that factor led to diagnostic errors which resulted in the deaths of at least three—and possibly as many as 15—VA patients because they did not receive correct or timely treatment for their conditions.

One of those patients was John D. Quick, a former resident of Greenwood, Ark., and a former infantry soldier who served in the U.S. military for 20 years, and who fought in the Korean and the Vietnam wars. As a veteran, Quick was treated at the Veterans Health Care System of the Ozarks in Fayetteville from September 2014 through September 2015.

Worked 'Under the Influence'

During this time, Levy was the chief of pathology at the Fayetteville, Ark., VA and often was under the influence of drugs and alcohol while at work, according to a complaint that Quick's daughters filed against Levy and the United States in August 2020. Quick died in September 2015 of squamous cell carcinoma.

As the co-executors of Quick's estate, his daughters, Catherine A. Hill and Melody K. Jones filed the lawsuit, seeking $3 million in damages on two counts: medical malpractice and wrongful death under the Federal Tort Claims Act.

In the lawsuit, Hill and Jones alleged that Levy was the pathologist who examined a sample of Quick's tissue and rendered Quick's diagnosis after examining that tissue.

"During Levy's employment at the Fayetteville VA, Levy severely abused drugs and alcohol and was regularly intoxicated therefrom while providing medical services to Fayetteville VA patients in the course of his employment," the complaint alleged.

Obivious Signs of Inebriation

"Often times, while under the influence of drugs and alcohol in the course of his employment with the Fayetteville VA, Levy exhibited obvious symptoms of inebriation that should have been readily apparent to those around him and his co-employees at the Fayetteville VA," the complaint added.

In addition, Levy concealed being under the influence of alcohol by routinely ingesting 2-methyl-2-butanol [2M2B] to mask the alcohol in his blood during routine drug and alcohol tests that the Fayetteville VA administered to Levy and other employees, the complaint noted. *(See "Arkansas Pathologist Faces Manslaughter Charges," TDR, Sept. 3, 2019.)*

Here are what may be the most relevant facts in the complaint against Levy:

- "In providing care to Mr. Quick, Levy negligently entered a materially false and misleading diagnosis in Mr. Quick's medical records, diagnosing him with small cell carcinoma, when in fact, Mr. Quick suffered from squamous cell carcinoma," the complaint noted.
- "It is required for first-time malignancy cases to be subject to peer review, which did not happen here. In fact, Levy intentionally falsified records and claimed a second pathologist agreed with this diagnosis of small cell carcinoma, when in fact, a second pathologist did not agree with the diagnosis," according to the complaint.
- "Levy's incorrect diagnosis, which he entered into Mr. Quick's medical records, influenced decisions by Levy and other Fayetteville VA healthcare providers regarding Mr. Quick's course of treatment," the complaint added.

Settlement Terms

The facts in the case led to the settlement last month in which the federal DOJ agreed to pay Hill and Jones $400,000. Of that amount, 25% will be paid to the attorneys for the plaintiffs, **Taylor Law Partners** of Fayetteville, Ark.

In reaching the settlement agreement, the DOJ asserted no admission of liability. "This agreement is not, is in no way intended to be, and should not be construed as, an admission of liability or fault on the part of the United States, the Department of Veterans Affairs, or any of its agents, servants, or employees," the agreement said.

It should be noted that a search for complaints against Levy by the legal staff at **O'Connell and Aronowitz** of Albany, N.Y., showed that the malpractice and wrongful-death case filed against Levy last year was not the only time he was cited for misconduct.

A search of records showed that in 1987 Levy was practicing in North Miami Beach, Fla. At that time, the **Florida Department of Health** cited Levy for providing substandard care, incompetence or negligence, and ordered him to pay a fine of $250 for failing to keep written records justifying treatment. He was given a 12-month probation in this case, disciplinary records show.

Ten years later, in December 1997, the **Nevada Board of Medical Examiners** revoked Levy's license and charged him with a violation of a Nevada law related to criminal offenses committed by healthcare professionals. This violation was related to action taken against his license in California, for attempting to renew his license by fraud or misrepresentation, and for engaging in conduct intended to deceive the state **Board of Medical Examiners**, disciplinary records show.

Despite these offenses, he was later hired as the Chief of Pathology at the Fayetteville, Ark., VA in 2005, where he worked until his termination in 2018.

Alcohol Rehab Program

Court documents in Levy's criminal case describe how, in July 2016, Levy voluntarily entered an in-patient alcohol treatment program which he completed in October of the same year. That fall, as Levy prepared to return to work, he entered an impaired physician monitoring program and agreed with the **Mississippi Physician Health Program** and the **Mississippi State Board of Medical Licensure** "to maintain sobriety to ensure his ability to practice medicine with reasonable skill and safety to patients," according to the indictment.

These facts illustrate how, even while employed at the Veterans Health Care System of the Ozarks, his behaviors and actions were noticed and he was subject to disciplinary action. But even at this stage, did "the system" fail to protect the patients and physicians using the diagnostic reports Levy signed?

Involuntary Manslaughter

In the original indictment, federal prosecutors charged Levy with three counts of involuntary manslaughter and 24 other criminal counts. At that time, *The Washington Post* reported that VA officials said Levy's misdiagnoses were responsible for at least 15 deaths.

The VA said Levy examined 34,000 veterans' pathology slides from 2005 to 2018. Based on its own review of those slides, the VA in its indictment said, "Almost 10% of the diagnoses he [Levy] made involved clinical errors." *(See "Arkansas Pathologist Faces Three Manslaughter Charges," TDR, Sept. 3, 2019.")*

The different state disciplinary actions and the federal criminal indictments that are in the public record may not tell the full story about Levy's medical career as a pathologist. In many states, the state medical licensing or review boards can discipline a physician and those actions often remain sealed to the public. Therefore, the full scope of Levy's problems with state medical boards throughout his career remains unknown.

A Cautionary Tale

The troubled career of pathologist Robert Morris Levy, as reflected in the public record, is a cautionary tale for all clinical labs and pathology groups. First, public records for physicians or a lab workers may not give full stories.

Second, if there is evidence of prior problems with job performance and diagnostic accuracy, the employing lab would be well-served to intensify the quality reviews of the diagnostic work performed by those individuals. TDR

Contact Jeffrey J. Sherrin at 518-462-5601 or jsherrin@oalaw.com.

Attorney Identifies Useful Lessons to be Learned from Levy Case for Clinical, Pathology Labs

IN A COMMENTARY ABOUT THE CASE INVOLVING THE NOW-JAILED PATHOLOGIST who previously worked at the Veterans Health Care System of the Ozarks, healthcare attorney Jeffrey J. Sherrin offered advice for clinical laboratories and anatomic pathology (AP) groups. Sherrin is an expert in clinical lab and anatomic pathology group management at **O'Connell and Aronowitz**, attorneys in Albany, N.Y.

"Robert Morris Levy, MD's, impairment—and the problems that ensued—are tragic, but by no means unpredictable," Sherrin wrote. "Alcohol and substance abuse addictions are pervasive and are significant problems for the licensed professions, of which pathologists are no exception. All or most states and medical societies have impaired physician programs, but they depend upon the voluntary reporting and participation of the physician.

"Levy's case highlights that the victims of such addictions or abuse are not limited to the impaired physicians, but tragically can extend to patients and, in some cases, can lead to unnecessary death. Civil lawsuits are to be expected when a physician or pathologist's impairment causes patient harm, but the Levy case brings the realization that criminal prosecutions may also stem from such professional misconduct.

"Because the integrity of a pathologist's reports is of such vital importance to the proper diagnosis of the patient's condition, laboratories must do everything they can to protect that integrity," Sherrin warned. "By the same token, it is not feasible for the lab to ensure at all times that its pathologist is not impaired when an interpretation is given.

"Employment law attorneys in labs' respective states should be consulted on the propriety of periodic toxicology screening, or of requiring such screening on an individual basis in specific circumstances," he advised. "Beyond that, labs should establish procedures to require employees who become aware—or have reason in good faith to believe—that a pathologist is impaired to report such concerns. Also, clinical labs and AP groups could establish procedures for the anonymous reporting or such impairment.

"If management of a lab becomes aware of such a situation—or even the strong possibility that a pathologist is working while impaired—the lab must take protective measures," he wrote. "These measures can vary by circumstance, but once the lab is put on notice, it risks liability for its failure to act, in addition to risking serious injury or the death of a patient.

"Appropriate steps can vary by the situation and state and federal law," advised Sherrin. "Such steps might include drug testing, monitoring, participating in an impaired-physician monitoring program, and suspension or termination depending, in part, on the physician's willingness to participate and cooperate.

"While actual knowledge then imposes additional responsibilities, labs must not bury their head in the sand to avoid such knowledge," he noted. "Risks to patient safety are too great and labs that do so can exacerbate their legal liability. What's more, clinical labs and AP groups must never alter records to hide incriminating information.

"At a minimum, therefore, all labs and AP groups must establish procedures, and train management and staff on the importance of not abusing substances, whether alcohol or otherwise, not to work under the influence, to report known or suspected cases, and to be aware of and take advantage of impairment programs that are available," he concluded. "It is best for all administrators and staff to keep your eyes open for any signs of impairment and act immediately."

Lab Briefs

Univ. of Miami Settles Lab Qui Tam Lawsuit for $22 Million

EARLIER THIS MONTH, THE FEDERAL **DEPARTMENT OF JUSTICE** (DOJ) announced a settlement with the **University of Miami** that resolves allegations that the university ordered medically-unnecessary tests and submitted false claims to federal healthcare programs.

In the settlement, the University of Miami will pay $22 million to resolve the claims and will enter into a five-year corporate integrity agreement with the **Department of Health and Human Services**.

Different whistleblowers filed three different *qui tam* lawsuits in 2013 and 2014 alleging similar violations of federal law. One case was filed by Jonathan Lord, MD, who was Chief Operating Officer at **UHealth**, the university's health system. A second *qui tam* action was filed by Philip Chen, MD, and Joshua Yellen, who were Vice Chair of Pathology and Vice Chairman for Administration, Dept. of Pathology, respectively at the University of Miami. The third *qui tam* case was filed by Mitchell Watson, now a former finance director for **Jackson Memorial Hospital**.

PathAI Generates $165 Million in New Funding from Investors

DIGITAL PATHOLOGY GOT ANOTHER MAJOR VOTE OF INVESTOR CONFIDENCE after Boston-based **PathAI** announced that its Series C funding round raised $165 million.

Some of the notable companies investing in this funding round were **Kaiser Permanente**, **Bristol-Myers Squibb**, **Labcorp**, and **Merck Global Health Innovation Fund**.

PathAI describes itself as a "provider of artificial intelligence-powered technology for pathology. The company said it will "deploy its new capital to accelerate product development while continuing to prioritize the improvement of patient outcomes with reliable AI-powered technology and meaningful collaboration with pharmaceutical and diagnostic partners."

FierceBiotech described PathAI's platform as using "machine learning and deep learning to improve both diagnostic and treatment capabilities by identifying disease biomarkers and predicting how individual patients will respond to various treatments."

One sign of PathAI's progress on developing algorithms to analyze digital pathology images is the collaboration it has with Labcorp, which expanded its existing relationship with PathAI earlier this year. *FierceBiotech* said that "the exended partnership will see Labcorp use PathAI's algorithms to identify disease-specific biomarkers and the biomarker-positive patients who will respond best to certain treatments to improve clinical trials managed by Labcorp's drug development arm."

November Return of Exec War College

ALL SIGNS ARE AUSPICIOUS THAT THE PANDEMIC in the United States has eased and restrictions on air travel and live conferences are lifting in state after state. Based on this, THE DARK REPORT is working with a hotel to produce a smaller-sized *Executive War College on Lab and Pathology Management*.

The likely site will be San Antonio and will happen in the first week of November, 2021. Our office hears regularly from lab professionals ready to attend this event and eager for the opportunity to network with peers and lab vendors while learning about new trends and developments in the lab and pathology marketplace. TDR

IVD, DIAGNOSTICS & INFORMATICS UPDATE

LIS Update

Pandemic Complicates Sales for Lab Info System Companies

The COVID-19 outbreak last March made it challenging to win new customers

HEALTHCARE INFORMATION TECHNOLOGY (IT) COMPANIES serving clinical laboratories and providers with laboratory information systems (LISs) and electronic health records (EHRs) shared recent financial reports on their businesses.

It is challenging to obtain information about the revenue growth and market share of the leading vendors of laboratory information systems because these LIS businesses are either a division of a large public corporation or are owned by a private company.

The following is current information about financial and market performance taken from quarterly earnings calls and public sources.

Cerner

CERNER CORPORATION: Q1-2021 Revenue was $1.4 Billion

Cerner Corporation said revenue in the first quarter was $1.4 billion, a decline of 2% compared to Q1 last year. Full-year 2020 revenue was $5.5 billion, which was down 3% compared to 2019 as a result of pandemic.

During an earnings call, Marc Naughton, Executive Vice President and Chief Financial Officer, addressed software revenue challenges. "Licensed software revenue in Q4 was flat year-over-year at $174 million. Full year licensed software revenue declined 4% from 2019 to $656 million due to pandemic-driven declines in traditional software."

Cerner executives commented on one trend that touches on how clinical laboratories serve hospitals, office-based physicians, and other providers. Donald Trigg, President, noted a need for information technologies to support integrating care beyond the hospital. "The biggest trend in provider healthcare—before, during, and after COVID—centers on the push for vertical integration beyond the four walls of a hospital." he commented.

"This mix of owned and affiliated physician practices, post-acute care facilities, and the home as venue are critical nodes on the health networks being built in every community.

"These health network strategies have diverse contractual frameworks and disparate technologies, and our HealtheIntent platform is purpose-built to integrate and manage them," Trigg continued.

A topic of interest to clinical laboratories using the Millennium LIS is that Cerner would like to move this product to the cloud in a stepwise fashion. "We've indicated [moving] Millennium [to the cloud] will be a process. We probably will never move all of Millennium," Naughton stated during the Q4-2020 conference call.

"There are elements of Millennium that will stay out there," he continued. "But the elements [of Millennium] that face the client—the elements that we benefit from being updated very quickly and frequently—those are the elements that will move to the cloud ... over some period of time."

EPIC SYSTEMS: Estimated Revenue of $3.2 Billion in 2020

Epic Systems Corporation, Verona, Wis., is privately held and not required to disclose financial information. Epic's flagship product is its electronic health record (EHR) system and it aggressively promotes its Epic Beaker LIS for both clinical and pathology laboratories.

Forbes Magazine reported Epic's 2020 revenue as $3.3 billion. In 2019, Epic had a 39% share of the more than 880,000 hospital beds in the U.S., according to estimates by the healthcare IT firm **KLAS Research**. KLAS also estimated Epic's EHR market share for acute care hospitals to be 29%.

ROPER TECHNOLOGIES–Sunquest Information Systems, CliniSys, Data Innovations: Q1 Brings Growth in LIS Market in Europe

Roper Technologies, the Sarasota, Fla.-based parent company of various laboratory IT companies, reported on first quarter 2021 (Q1 2021), calling it a "great start to 2021."

Clinical laboratory leaders are reminded that Roper's report on application software segment revenue includes data from **Sunquest Information Systems**, Tucson, Ariz.; **Data Innovations**, Colchester, Vt.; and **CliniSys Group**, based in the United Kingdom (UK).

In an earnings call, Roper explained that its reported Q1 2021 revenue of $1.5 billion—up 13%—was the "all-time record for a Roper quarter" and due to a revenue increase of 42% year-over-year in the application software division, which includes Roper's two LIS companies.

"Our results were enhanced a bit by approximately $40 million of accelerated payments that were the results of wins at our UK-based CliniSys laboratory software business," said Chief Financial Office Robert Crisci.

During the call, Roper executives described a booming market in Europe for its CliniSys laboratory information system (LIS). In the United States, the Sunquest LIS has maintained market share, even during the pandemic.

"[Sunquest] benefited last year and in this quarter with the COVID-19 tailwind, and how it stood up SARS-CoV-2 testing," explained Neil Hunn, President and CEO of Roper. [The Sunquest team] continues to invest in their public health offering and their molecular offering. The leadership team has done a nice job in that. So, that's good news. The unfortunate part of that news is that [the pandemic] delayed the bottoming of the [LIS] business, which [the COVID-19 pandemic] ... pushed out for a year or two ... [which will give Sunquest a] baseline from which it can grow."

OVATION.IO: Emerging LIS Firm Raises $21.5 Million in New Funding

Ovation.io of Cambridge, Massachusetts, announced a Series B funding of $21.5 million late last year. The company is a recent entrant into the LIS market and offers what it describes as a cloud-based laboratory information management system (LIMS).

The funding was announced by Ovation co-founder/CEO Barry Wark, PhD, in December, at the end of a pivotal year when Wark said the firm (established in 2017) doubled revenue as it leveraged its LIMS to support COVID-19 testing and more.

One of the five key funders called attention to Ovation's focus on molecular genomics labs and precision medicine.

"These labs need specialized software, and the real value is being able to stitch the data together to create a solution to go after targeted therapeutics," said Chris Scoggins, Venture Partner, **SignalFire**, in *Crunchbase News*. TDR

INTELLIGENCE

LATE & LATENT

Items too late to print, too early to report

With little fanfare, the company that was incorporated as **Laboratory Corporation of America Holdings** rebranded itself. It is now officially called **Labcorp** (with a lower case c). This won't be much of a change for the clinical laboratory profession, which has long seen the company use LabCorp (with an upper case C) in most marketing materials. Out goes the old logo:

LabCorp
Laboratory Corporation of America

In comes the new logo:

labcorp

MORE ON: *Labcorp Rebrand*

The name and logo change happened at the end of last year and may be one change enacted by Labcorp's new President and CEO, Adam H. Schechter, who assumed those duties in 2019 at the retirement of former President and CEO David King. Schechter also was named Labcorp's Chairman of the Board in May, 2020.

CUE HEALTH RAISES $235 MILLION FOR ITS POCT SYSTEM

On May 13, **Cue Health** of San Diego announced that it had raised $235 million in a private financing round. The company develops point-of-care tests and testing systems. In March, the **Food and Drug Administration** cleared Cue's at-home molecular COVID-19 test kit for consumer use. It is a single-use test that comes with a nasal sample-collection wand and a battery-powered cartridge reader that connects to a smartphone app. Results are generated within 20 minutes.

TRANSITIONS

- Douglas M. VanOort retired as CEO of **NeoGenomics Laboratories** of Fort Myers, Fla., earlier this year, a role he assumed in 2010. He will continue to serve as Chairman of NeoGenomics' Board of Directors. Previously, he held executive positions with **Conundrum Capital Partners**, **Quest Diagnostics**, and **Corning Incorporated**.

- **NeoGenomics Laboratories** announced that Mark Mallon is now its new CEO. Prior to joining NeoGenomics, Mallon served at **Ironwood Pharmaceuticals**, **AstraZeneca**, **Accenture**, and **Armstrong World Industries**.

- Pathologist Lawrence Weiss, MD, is the new Chief Medical Officer for **Fulgent Genetics**, based in Temple City, Calif. Formerly, he worked at **NeoGenomics**, **Clarient Diagnostic Services**, and **City of Hope Medical Center**.

- **IDbyDNA** of Salt Lake City, Utah, appointed Neil Gunn as Chief Executive Officer. Gunn's prior executive positions were with **Roche Molecular Systems**, **CaridianBCT**, **Chiron**, and **Pall Corporation**.

That's all the insider intelligence for this report. Look for the next briefing on Monday, June 14, 2021.

➤**Publisher:** Robert L. Michel
rmichel@darkreport.com

➤**Executive Publisher:** Bob Croce
bcroce@darkreport.com

➤**Editor-In-Chief:** Robert L. Michel
rmichel@darkreport.com

➤**Managing Editor:** Michael McBride
michaelmcbride58@gmail.com

➤**Senior Editor:** Joseph Burns
joeburns@capecod.net

➤**IVD Reporter:** Donna Marie Pocius
donna11019@att.net

➤**Legal/Compliance Reporter:** Kim Scott
kmscott2@verizon.net