G2 INTELLIGENCE
A DIVISION OF PLAIN LANGUAGE MEDIA

NATIONAL INTELLIGENCE REPORT™

Covering Government Policy For Diagnostic Testing & Related Medical Services

Celebrating Our 36th Year of Publication

Vol. 15, Iss. 22, December 17, 2015

INSIDE THIS ISSUE

www.G2Intelligence.com

CMS Software Glitch All But Stops Reference Lab Claim Payments

A glitch in updated software the Centers for Medicare & Medicaid Services (CMS) sent to its regional administrative contractors all but halted payments for reference lab claims submitted between Oct. 1 and the start of this month.

Sector officials say the mishap was tied to CMS' decision last May to require any reference claims be submitted with not only the CLIA number of the referring laboratory, but also the NPI number for the clinician or laboratory contractor that performed the test. However, virtually all of those claims were being rejected as not recognizing the NPI, according to JoAnne Glisson, senior vice president with the American Clinical Laboratory Association. The situation was so bad Glisson said that big national labs such as LabCorp were having reference claims rejected even when one of their own regional facilities performed a test.

"The computer systems (of Medicare administrative contractors) were recognizing NPIs before Oct. 1, and then they were not," Glisson said. She added that it was perhaps the most serious software issue regarding the Medicare program she had seen in the past 20 years.

Continued on page 2

Industry Comments on PAMA Guidelines Fairly Uniform

The comment period for the implementation of regulations specific to the Protecting Access to Medicare Act, (PAMA), concluded late last month. The concerns raised by laboratories, their lobbies and individuals were remarkably consistent.

The Centers for Medicare & Medicaid Services (CMS) received nearly 1,300 comments, many from specific individuals, but also from major lobbies including the American Clinical Laboratory Association (ACLA), the American Medical Association, the American Association for Clinical Chemistry (AACC), and even regional hospital associations. Large national and regional laboratories also chimed in.

The overall intent of PAMA is to come closer to equalizing payments between Medicare and private payers, the latter of which have been using their relative market power over labs to keep their rates down. The intent

Continued on page 7

CMS Software Glitch All But Stops Reference Lab Claim Payments, *from page 1*

The issue has held up millions of dollars worth of claims, according to Glisson and other officials, such as Francisco Velázquez, M.D., chief executive officer of Spokane, Wash.-based PAML, the largest laboratory in the Pacific Northwest. "PAML did experience a large number of denials specifically impacting work referred to our partner hospital laboratories. The denials were prevalent in the industry," Velázquez said in an email.

> *"PAML did experience a large number of denials specifically impacting work referred to our partner hospital laboratories. The denials were prevalent in the industry."*
>
> — Francisco Velázquez, M.D., CEO, PAML

The MACs apparently offered little help to resolve the issue. According to a letter Glisson sent to CMS on Nov. 20, "one contractor has acknowledged there are gaps in the PECOS file, but has requested that the affected laboratory call the contractor's customer service line and verify the NPI of each reference laboratory for which the laboratory is billing. So far, this laboratory ... has had to manually cull out 300 individual claims and is calling the contractor to verify the individual NPI code of each reference laboratory included on its claims. However, the contractor only allows the laboratory to verify three NPIs per call, which means it will require 100 individual calls to complete that task and there is no assurance that the effort will actually resolve the issue." Glisson did credit CMS for responding swiftly to the situation. She said agency officials responded the day after she sent the letter to set up a meeting.

On Dec. 10, less than three weeks after being notified about the issue, CMS forwarded the following announcement to the MACs: "A claims processing issue affecting claims for reference lab services and services subject to the anti-markup payment limitation, which were billed on or after October 1, 2015 has been resolved. Medicare Administrative Contractors (MACs) are reprocessing these claims. No further action is needed by providers/suppliers." Glisson said it was hoped the messed up claims would be paid before the end of the calendar year.

Remaining unresolved is the issue regarding the anti-markup rule. Under current Medicare rules, any reference claims are sent by the original lab, using the so-called "90 modifier" to indicate that the work was farmed out to another facility. The CMS' mandate to use the NPI number was intended to have labs comply with anti-markup rule. That rule was introduced in 2009 and was intended to limit payments labs can receive when testing or other ancillary services are performed by outside contractors.

Glisson's letter to CMS last month regarding the software issue noted that the anti-markup rule is "only applicable to services billed under the Medicare Physician Fee Schedule, whereas the reference laboratory services at issue here will usually be paid under the Clinical Laboratory Fee Schedule." Glisson said that while the ACLA has no objections to submitting NPI numbers with reference claims, it does have concerns that such claims would continue to be subject to the anti-markup rule. The suspension of the NPI editing rule is likely to be in place for a significant period of time. Glisson said that CMS indicated that it would be "well into the next calendar year" before a fix would be made. In the meantime, ACLA has made the highly unusual suggestion of having its member labs beta-test the software fix. Glisson said it was unclear if CMS would take the group up on its offer.

Takeaway: A minor software glitch created significant financial duress for labs that performed reference work. G2

focus on: *OIG Scrutiny of EHR*

OIG Escalates Attention to Medical Devices: Experts Advise Providers and Device Makers to Prioritize Cybersecurity

Cyber risk and health technology experts advise health care executives to prioritize cybersecurity and proactively evaluate how well their organizations' networked medical devices protect health information. Their counsel comes tangential to the Department of Health and Human Services' (HHS) Office of Inspector General (OIG) plan to review oversight of networked medical devices at hospitals by the U.S. Food and Drug Administration (FDA). The OIG announced in its 2016 Work Plan a new project to find out how well the FDA has ensured that the devices protect electronic protected health information (ePHI) and beneficiary safety.

> *"Health care providers should enhance and implement their cybersecurity risk management program, determine the network-connected medical devices with the highest risk within their environment, and develop risk-treatment plans that are time-boxed, practical, funded and tracked by executive leadership."*
>
> — Russell Jones, Partner, Deloitte Advisory

Given the OIG's focus, Lisa Gallagher, vice president, Technology Solutions, Healthcare Information and Management Systems Society (HIMSS) North America, expects the FDA to heighten scrutiny of computerized medical device cybersecurity. "Medical device manufacturers—with either a computerized medical device on the market or [who] want to put such a device on the market—need to pay attention," Gallagher told *National Intelligence Report*. As for health care organizations, Gallagher recommends evaluation of computerized medical device security controls and features. Medical device security (MDS2) forms, provided by medical device manufacturers, can aid providers in such due diligence, according to Gallagher, who adds that information about the forms is accessible at www.himss.org. The forms can help hospitals assess vulnerability and risks associated with information transmitted or maintained on the devices, the OIG pointed out in its Work Plan.

Russell Jones, partner, Deloitte Advisory, specializes in cyber risk for health sciences in the public sector. He told *National Intelligence Report* that the OIG's focus means providers need to better prioritize cybersecurity efforts on proactive, regular "cyber hygiene" activities for networked-connected medical devices as well as the overall network and information technology (IT) infrastructure.

"Health care providers should enhance and implement their cybersecurity risk management program, determine the network-connected medical devices with the highest risk within their environment, and develop risk-treatment plans that are time-boxed, practical, funded and tracked by executive leadership," he says. "This type of approach will give health care providers a better defensible position if they are selected by OIG for a random cybersecurity audit."

As laboratory leaders know, computerized medical devices enable physicians, often in partnership with pathologists, to monitor and maintain patients' health. But they have the propensity to do more than that. The OIG names in its work plan dialysis machines, radiology systems and medication dispensing systems as examples of medical devices integrated with electronic medical records (EMRs) and the larger health network. "They pose a growing threat to the security and privacy of personal health information. Such medical devices use hardware, software and networks to

monitor a patient's medical status and transmit and receive related data using wired or wireless communications," according to the OIG.

OIG services are aimed at protecting the integrity of HHS programs and well-being of programs' beneficiaries. Its oversight extends to the FDA.

Providers may see more medical device manufacturers deploying additional security controls and features and even upgraded pathways for medical device products, Gallagher told *NIR*. "The risks associated with use of such medical devices on the health care organization's network may be lowered as a result," she says. Jones encourages medical device manufacturers to focus on implementing "security by design" within their product development lifestyle. "They should develop a 'responsible disclosure' policy and associated processes and procedures related to security vulnerabilities that are discovered within their fielded medical devices," he says.

For its part, the FDA suggests collaboration to address device cybersecurity. Its complimentary workshop for stakeholders, set for Jan. 20 and 21 in Silver Spring, Maryland (and webcast), will focus on medical device cybersecurity, highlight past collaborative efforts and discuss unresolved gaps and challenges hampering progress in advancing medical device cybersecurity. The FDA last year said medical device manufacturers should consider cybersecurity risk as part of a device's design and development. "Some medical devices like computer systems, can be vulnerable to security breaches, impacting the safety and effectiveness of the device. By carefully considering possible cybersecurity risks while designing medical devices and having a plan to manage system or software updates, manufacturers can reduce the vulnerability in their medical devices," the FDA says in its guidance statement entitled, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices."

More Steps to Medical Device Safety and Security

In addition to review of MDS2 forms, HIMSS' Gallagher counsels health care executives to: 1) make certain the organization's risk analysis and risk management strategy includes all networked devices; 2) consider segmenting the network so there is a dedicated network for networked medical devices; 3) deploy patch management and/or upgrades for the networked medical device in a timely manner; and 4) make sure the health care organization procures a networked medical device with appropriate security controls and features, again reviewing the MDS2 form.

Also New on OIG's radar in 2016

Consistent with its focus on EHR issues, the OIG also announced in its 2016 Work Plan a new commitment to reviewing adequacy of the Office for Civil Rights' (OCR) oversight of security of ePHI. And this intent by the OIG may come as no surprise to readers.

DOJ Reports $1.9 Billion in Health Care False Claims Act Recoveries for FY 2015

Given the large False Claims settlements the laboratory sector has seen this year (for example, in the Health Diagnostic Laboratory and Singulex cases) and the major nationwide Takedown initiatives, it's no surprise to hear the Department of Justice (DOJ) recovered $1.9 billion in health care False Claims Act cases in fiscal year (FY) 2015. That's more than half of the aggregate $3.5 billion the DOJ reported recovering under all False Claims Act cases for the fiscal year ending Sept. 30. And that's just the federal recoveries. The Department also took credit for assisting in millions of dollars of state Medicaid recoveries.

This year's $1.9 billion brings the total health care recoveries under the False Claims Act since January 2009 to almost $16.5 billion. The DOJ highlighted dialysis providers, hospitals, health systems, and pharmaceutical companies for the largest recoveries from organizations. The diagnostics industry took the spotlight, however, when it came to discussing individual accountability. Noting the Yates memo's call to hold individuals responsible for corporate wrongdoing, the DOJ highlighted the individuals being pursued as a result of the cases against cardiovascular testing laboratories Health Diagnostic Laboratory (HDL) and Singulex. The government settled with HDL and Singulex for $48.5 million and has intervened in *qui tam* actions brought against individual owners and founders of the entities involved.

Whistleblowers played a key role in these recoveries. The DOJ reports that of the $3.5 billion recovered under the act, $2.8 billion were linked to *qui tam* actions. In FY 2015, there were 638 whistleblower or *qui tam* actions filed. Whistleblowers received $597 million in awards for bringing these actions.

National Intelligence Report highlighted in our Oct. 8 issue OIG report findings, pointing to OCR's inadequate oversight of compliance with HIPAA's privacy rule and its poor follow-up on reported breaches of protected health information. OIG said it discovered: 1) a reactive approach by OCR in response to complaints as opposed to proactive one; 2) incomplete documentation and follow-up on security breaches; 3) limited search functionality in OCR's case tracking; 4) many providers noncompliant with HIPAA; and 5) inconsistent background checks on investigated entities.

Continued EHR Investigation by OIG

EHR programs set for OIG investigation, continuing from last year's work plan, include:

Use of EHRs to support care coordination through accountable care organizations. "We will also assess providers' use of EHRs to identify best practices and possible challenges to the exchange and use of health data, such as degree of interoperability, financial barriers, or information blocking," the OIG plans states.

Medicare and Medicaid incentive payments for adopting EHRs. The OIG is on a mission to find payments that did not meet meaningful use (the use of certified EHR technology in a meaningful manner). Corrective action, it says, will be taken as erroneous Medicare payments are revealed. The Medicare EHR incentive payments totaled more than $20 billion effective July 2015, while the Medicaid incentive payments reached about $9 billion effective July 2015, the work plans points out.

Security of certified EHR technology under meaningful use. "We will perform audits of various covered entities receiving EHR incentive payments from Centers for Medicare and Medicaid Services to determine whether they adequately protect electronic health information created or maintained by certified EHR technology," the OIG says.

Takeaway: As the OIG continues its focus on EHR security, so, too, should health care organizations. Industry experts expect heightened scrutiny of medical device cybersecurity. OIG also plans commitment to oversight of compliance with HIPAA by the OCR and continuing with EHR projects relating to accountable care organizations, incentive payments and certified technology. G2

Study Shows Better Patient Matching Across Care Continuum Possible; Organizations Seek Input on a Framework

It is possible for providers and other health care organizations to achieve a 95% accuracy rate in matching patients to their electronic health records. That's a key finding from a recently released study by The Sequoia Project and the Care Connectivity Consortium (CCC). Patient matching is important to laboratories that also track orders and coordinate diagnostics data across health care systems and organizations in a vast care continuum.

But lack of effective patient data matching hinders seamless information exchange between organizations, according to the study. Organizations may have a "blind spot" when it comes to patient matching, according to authors of the white paper, "A Framework for Cross-Organizational Patient Identity Management." They likely have acceptable patient match rates within the enterprise (i.e., hospital or integrated delivery network). "But patient matching across organizations is a very different problem," the paper points out. Factors out of an organization's direct control in-

clude data quality and completeness, software, consents, human and system workflows and corporate cultures, the study found.

The multi-year study was aimed at analyzing best practices for patient matching for health information exchange partners. The white paper, available on The Sequoia Project web site (www.sequoiaproject.org), presents a case study at Intermountain Healthcare (a CCC member), shares a proposed matching maturity model, and suggests a national patient matching framework.

The research suggests that how data is entered seems to be just as important as to what is entered—when it comes to patient matching, that is. Mariann Yeager, CEO of The Sequoia Project, told *National Intelligence Report* that use of consistent representations of data is probably the biggest "quick win" for the industry. "For example, using a standardized representation of the patient's address, telephone number, and name makes those data more comparable and provides a significant improvement in patient matching success," she says.

"For example, using a standardized representation of the patient's address, telephone number, and name makes those data more comparable and provides a significant improvement in patient matching success."

— Mariann Yeager, CEO, The Sequoia Project

She advises labs to align staff workflows to increase the quality of patient matching by: 1) searching for an existing patient record in the laboratory information management system (LIMS) before creating a new patient record; and 2) entering complete and accurate demographic information when creating or updating a patient record in the LIMS.

As to the findings at Intermountain, the case study showed the Salt Lake City, Utah-based system (which has reportedly invested heavily in health care IT), had a 10 per cent success rate in accurately matching patient records across its care continuum. So, how did it eventually achieve a 95 percent accuracy rate? The research points to: 1) algorithmic performance and refinement; 2) human workflow and data entry improvements resulting in a boost to 62 percent accuracy; 3) algorithmic, authorization/consent, network and IT issues and inconsistent encoding improvements that together further escalated the match rate to 85 percent; and 4) best practices that ultimately helped the organization achieve 95 percent accuracy in matching patients records across organizations. Patient matching systems should not use exact, character-by-character matching algorithms, the case study research suggests.

The report's maturity model lists five levels for patient identity management starting at level zero for organizations with ad hoc processes and no management oversight and level one for those with basic processes and limited oversight. At level two, organizations are increasing algorithm use, gathering quality metrics and using standards, while those on level three use advanced technologies and have management controls and community involvement. Level four is for innovators that regularly optimize and have senior management involvement. Yeager encourages labs to use the model to self-assess maturity level and plan for improvement.

The Sequoia Project is a non-profit chartered to advance implementation of interoperable nationwide health information exchange. And the CCC is an interoperability collaboration aimed at advancing technology available for electronic heath information exchange.

Takeaway: A national study suggests dramatic improvements in matching patients to their health records and among providers and other organizations is possible. G2

Industry Comments on PAMA Guidelines Fairly Uniform, *Continued from bottom of p.1*

of PAMA is to shave about $5 billion in lab-related costs from the Medicare program over the next decade. Under the proposed regulations, labs with a significant amount of business under the Clinical Laboratory Fee Schedule ($50,000 or more) would have to submit their claims data to CMS. The agency would then use that data to flatten out Medicare reimbursement rates.

Virtually to a person, the comments raised the same concerns: Not all laboratories were being included under the proposed regulations. The definition of an advanced diagnostic laboratory test (ADLT) was wanting. The proposed timetable for implementation was too stringent. And, some smaller labs were concerned about the lack of resources for gathering and transmitting claims data and whether CMS will be fully transparent regarding how it formulates new rates. The biggest concern appears to be the exclusion of hospital laboratories from the reporting requirements. Hospitals tend to obtain higher reimbursement rates from Medicare than standalone labs.

"We agree that hospital inpatient and bundled payments should not be reported, since laboratory payments cannot be separated from overall hospital reimbursement under these payment models. However, many hospitals conduct outreach testing that can and should be subject to the reporting requirements," the AACC said in its comments. The AACC cited an Office of the Inspector General report released last September noting that hospital labs account for nearly a quarter of all Part B laboratory payments the Medicare program makes for lab testing.

"The proposed rule's definition of 'applicable laboratory' would exclude much of the laboratory market in reporting pricing, and is at odds with both the statutory language and Congressional intent," said ACLA President Alan Mertz, in a statement. "This flawed definition will result in skewed data and Medicare rates that do not reflect the market."

LabCorp suggested a streamlined reporting requirement. "CMS should revise the definition of applicable laboratory in the final rule to mean a facility identified by a CLIA number, and allow the data of such applicable laboratories to be reported in the most efficient manner possible, including allowing entities owning multiple applicable laboratories to submit one combined report on their behalf," it said in its comments.

The $50,000 reporting bar was also a concern to the Coalition for 21st Century Medicine, which suggested it could stifle innovation. "Unlike most reference labs that offer a wide array of tests, most developers of ADLTs offer a single test or a very limited menu of tests, especially initially when they are just starting out. In the early years of a company, sales volumes, particularly Medicare sales volumes may be low or zero," the organization observed in its comments. "Only after obtaining Medicare coverage will these new ADLTs begin to experience physician adoption and reimbursement (especially if the test has a relatively limited Medicare population). It may take a laboratory offering an ADLT substantial time—weeks, months or even years—before it realizes $50,000 in Medicare CLFS revenues."

Congress Asks CMS to Delay PAMA Implementation

As we were going to press, forty-four members of Congress signed a letter sent Dec. 16, 2015 to Acting Administrator Andy Slavitt at the Centers for Medicare & Medicaid Services expressing concern "that laboratories will be unable to comply with the proposed implementation timeline." The letter notes rulemaking delays leave labs little time to prepare to report "upwards of millions of data points based on a yet-to-be-released set of agency requirements." It argues proteins should be included in the criteria defining Advanced Diagnostic Laboratory Tests and the labs reporting should be "more inclusive" and "allow any laboratory to voluntarily report."

Many concerns were raised about excluding proteomics testing from the definition of an ADLT. Easily the sharpest remarks came from Bruce Quinn, M.D., a senior director with Faegre BD Consulting in Washington, D.C. The proposed CMS regulations include RNA and DNA testing, but not proteomics.

"It is essential that CMS explain how it derived new payment rates."

— Chris Boggess, Boston Heart Laboratories

"If I tell my daughter, 'Come home on the bus, subway, or taxi' it does not require her to come home only on the bus or subway. The grammar of ADLTs is the same simple English," Quinn remarked. He later added that "CMS has built nearly a house of cards ... in its logic and assertions that ADLT, viewed as a whole, almost magically excludes protein only ADLT tests. It defies belief that such a tortured logical path of assumptions and semantic inferences—not even very well justified ones, and unexplained in the proposed rule itself—was the main and simple intent of Congress in writing and signing the definition as we have it."

The AACC also took issue with the proposal that ADLTs provide new clinical diagnostic information that cannot be derived from any other test or combination of tests. It noted that "the CMS language may limit test innovation by excluding tests that may provide the same data as another test, but can identify a condition more quickly and/or accurately. These test improvements can be equally vital to advancing and improving patient care."

Chris Boggess, vice president of marketing and development for Boston Heart Laboratories, noted that "community laboratories like mine have far less resources than national laboratories to meet the requirements outlined in the proposed rule. Meeting these requirements will require an overhaul of our information systems, require new staff or for us to repurpose and train current limited staff, and take significant time and focus in order to ensure the accuracy of the data we submit."

Boggess also wanted more transparency in the new rate-setting process. "It is essential that CMS explain how it derived new payment rates. Rather than simply announcing revised prices, we urge the agency to allow for notice and comment rulemaking to provide an opportunity for the agency to outline what data it received, from how many laboratories and their type(s), the variances in the data, and how CMS reconciled any variances."

Many of the commenters also asked for more time to gather the claims data and for the implementation of the changes. The consensus appeared to be for data gathering to start no earlier than mid-2016, with implementation anywhere from mid-2017 to early 2018. CMS is expected to issue the final PAMA regulations sometime next year.

Takeaway: Many labs and laboratorians have expressed concerns regarding the implementation of PAMA regulations by the Centers for Medicare & Medicaid Services.

National Intelligence Report (ISSN 2332-1466) is published by G2 Intelligence, Plain Language Media, LLLP, 15 Shaw Street, New London, CT, 06320. Phone: 1-888-729-2315 • Fax: 1-855-649-1623. Web site: www.G2Intelligence.com.

Kelly A. Briganti, JD, Editorial Director, Kelly@plainlanguagemedia.com; Barbara Manning Grimm, Managing Editor; Donna Pocius, Contributing Writer; Ron Shinkman, Contributing Writer; Stephanie Murg, Managing Director; Kim Punter, Director of Conferences & Events; Randy Cochran, Corporate Licensing Manager; Michael Sherman, Director of Marketing; Jim Pearmain, General Manager; Pete Stowe, Managing Partner; Mark T. Ziebarth, Publisher.

Receiving duplicate issues? Have a billing question? Need to have your renewal dates coordinated? We'd be glad to help you. Call customer service at 1-888-729-2315.