

United States District Court
for the
Southern District of Florida

United States of America <i>ex rel</i>)	
Derek Lewis and Joey Neiman,)	
Plaintiffs,)	Civil Action No. 18-20394-Civ-Scola
v.)	
Community Health Systems, Inc.,)	
and others, Defendants.)	

Order Granting Motions to Dismiss

The Plaintiffs in this *qui tam* action, Relators Derek Lewis and Joey Neiman, complain the Defendants—Medhost, Inc., a health information technology company; 140 hospitals (the “Hospitals”);¹ CHSPSC, LLC (the “Management Company”); and Community Health Systems, Inc. (the “Holding Company”)—either submitted, or caused the submission of, hundreds of millions of dollars in false claims to the Department of Health and Human Services for federal incentive payments under the Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”). (Am. Compl., ECF No. 123.) After the United States declined to intervene, the Court unsealed the initial complaint and, thereafter, the Relators filed an amended complaint. Medhost, the Managing Company, the Hospitals, and the Holding Company have separately filed four motions to dismiss the amended complaint. (ECF Nos. 129, 132, 133, & 134.) They argue, among other things, that the complaint fails to state a claim upon which relief may be granted and fails to comply with the heightened pleading requirements for alleging fraud. The Relators have filed an amended consolidated response to these motions (ECF No. 151). The Managing Company, the Hospitals, and the Holding Company all replied (ECF No. 146, 147, & 148) before the Relators filed their amended response while Medhost filed a corrected reply (ECF No. 154) after the Relators’ amended response. After careful consideration, the Court **grants** the

¹ The individual hospitals are listed in Exhibit A to the Relators’ amended complaint (ECF No. 123-1). However, thirty of these hospitals have since filed for bankruptcy and thus, as to those hospitals, this case is stayed. (Order, ECF No. 156 (citing list of hospitals at ECF No. 155, 3–4).) Thus, when the Court refers to the Hospitals or the Defendants, collectively, throughout this order, it intends to include only the 110 hospitals who are not subject to the Court’s stay. If a hospital identified in the suggestion of bankruptcy is mentioned in this order, it is only in the context of evaluating the motions to dismiss as to the hospitals who are not subject to the bankruptcy stay.

Defendants' motions to dismiss with prejudice. (**ECF Nos. 129, 132, 133, & 134.**)

1. Background and Facts²

A. Basic Framework

Through the meaningful-use program, the federal government uses financial incentives to encourage hospitals to utilize electronic, as opposed to paper, health records. To earn these incentives, hospitals must “meaningfully use” electronic-health-records software that has been certified as meeting specifications that are detailed in federal regulations. Federal regulations also spell out what it means to meaningfully use such software and hospitals must attest to having met those requirements.

Beginning in 2010, Medhost sought certification for electronic-health-record technologies that would enable its health-care customers to claim incentive payments from HHS under the HITECH Act. (Am. Compl. at ¶ 75.) To do so, Medhost worked with Drummond Group Inc. which is both an accredited testing laboratory and a government authorized certification body. (*Id.* at ¶ 82.) Drummond requires vendors, such as Medhost, to pass a series of test scripts that are intended to demonstrate that the software under review meets the required certification criteria. (*Id.* at ¶ 83.) Drummond also requires that vendors attest to the use of certain standardized nomenclature and technical specifications; to the accuracy of the information submitted; and that the functions demonstrated during testing are typical of the regular functionality of the software. (*Id.*) New versions of previously certified software can “inherit” the certification of older software without re-testing if Drummond determines that the certification criteria have not been adversely affected by the updates. (*Id.* at ¶ 84.)

The Holding Company, the Management Company (together, the “Companies” or “Company”), and the Hospitals, apparently collectively, starting in 2012, implemented Medhost’s “2011 Edition software” and attested to meaningful use at 78 hospitals during the government’s “Stage 1” reporting period. (*Id.* at ¶ 85.) Thereafter in late 2013, the Companies and the Hospitals began to implement Medhost’s “2014 Edition” software at the hospitals that had used the 2011 Edition for Stage 1, while concurrently implementing the 2011 Edition software at hospitals that had not attested to meaningful use in

² The Court accepts the Relators’ factual allegations as true for the purposes of evaluating the Defendants’ motions to dismiss. *Brooks v. Blue Cross & Blue Shield of Fla., Inc.*, 116 F.3d 1364, 1369 (11th Cir. 1997).

Stage 1. (*Id.*) According to the Relators, the Companies and the Hospitals' goal was to implement certified electronic-health-record technology at as many of their hospitals as possible ahead of the 2014 meaningful use attestation reporting period.³ (*Id.*)

Starting in 2012, the Companies and the Hospitals "represented to the Government that dozens of its hospitals met the objectives and measures for Meaningful Use of certified [electronic-health-record] technology based on their use of Medhost's software." (*Id.* at ¶ 76.) Based on these representations, the Holding Company, the Management Company, and the Hospitals "received over \$385 million in Meaningful Use incentive payments between 2012 and 2014." (*Id.*)

B. General Problems Identified

According to the Relators, throughout 2014 and 2015, Company and Hospital employees "discovered that required functions were missing or broken in Medhost's software." (*Id.* at ¶ 88.) This prompted Anwar Hussain, vice president and chief medical information officer,⁴ to circulate educational memos to the hospitals that used Medhost software to describe problems with the software, the implications to patient safety, and any applicable workarounds. (*Id.*) The Relators also say that "[s]oon after the Medhost rollout began,"⁵ various "doctors and hospital administrators began to report that the updated Medhost software was not able to perform required functions accurately and reliably, and that the inadequate functionality was putting the safety of . . . patients at risk." (*Id.* at ¶ 90.) For example, an administrator at one Hospital, Deaconess Health Systems LLC, opined, in July 2014, that

³ According to the complaint, "[m]any of [the H]ospitals were scheduled to have a 90-day attestation period form July 1, 2014 through September 30, 2014 with attestation occurring on October 1, 2014." (*Id.* at ¶ 230.) No mention is made of the schedule for the other hospitals' attestation periods.

⁴ The Relators do not specify which entity—the Holding Company, the Management Company, or the Hospitals—Hussain was affiliated with. This is a common occurrence throughout the complaint where the Relators refer to people simply as employees or "CHS" employees. The Relators define "CHS," in their complaint and in their opposition as encompassing, collectively, the two Companies and the Hospitals. (*E.g.*, *id.* at 12 and ¶ 30; Pls.' Resp. at 1 n. 1.) For clarity, the Court will, in most cases, substitute "the Companies and the Hospitals" where the Relators refer to "CHS."

⁵ The Relators do not specify exactly when this "rollout" took place at each hospital, but they do generalize that the Companies and the Hospitals, collectively, "rolled out updated versions of Medhost software at numerous CHS hospitals" in "the months leading up to the 2014 Meaningful Use attestation reporting period." (Am. Compl. at ¶ 88.)

doctors were frustrated with the Medhost software and that the upgrades to the software had not resolved many issues. (*Id.*) The next day, a doctor from Deaconess expressed even more concerns with various safety issues, noting, by way of example, that the software provided no warning mechanism when medicines or tests had been duplicated. (*Id.*) In the same message, this doctor also complained that problems identified months earlier remained unresolved, warning that the providers' "list is growing, and frustration is not lessening." (*Id.*)

From May 2014 through November 2014, the Companies and Hospitals instituted weekly "critical issues" conference calls to discuss problems the hospitals were having with Medhost's software. (*Id.* at ¶ 91.) The calls were led by "corporate-level executives" and included "IT and clinical informatics personnel from each of the Medhost hospitals." (*Id.*) The Relators say that, on these calls, "the hospitals repeatedly voiced their concern about the [electronic health record's] lack of functionality and safety." (*Id.*) In conjunction with these calls, Hussain and another vice president, Pam Rudisill (who was also the "Chief Nursing Officer"), issued advisories to the medical staff and senior executives at the hospitals. (*Id.* at ¶ 92.) These advisories "warned of serious, unresolved problems with the Medhost . . . software and instructed the . . . hospitals to implement additional safety checks." (*Id.*) The advisories addressed, for example, the double checking of multi-dose medication administration and medication with multiple tablets dispensed and issues involving "Order Sets." (*Id.*)

C. Integration Issues Between Medhost's Products

Many of the problems the Relators complain of center on what they describe as integration failures between two Medhost software products: EDIS and Enterprise. (*Id.* at ¶ 102.) EDIS software is used in emergency departments and Enterprise is used in inpatient settings. (*Id.* at ¶ 33.) These two systems were both deployed at "numerous hospitals" which attested to meaningful use. (*Id.* at ¶ 102.) The Relators maintain, however, that, as Medhost, the Companies, and the Hospitals knew, "at all relevant times," EDIS and Enterprise were not integrated. (*Id.*) As a result, for patients who transferred to inpatient from emergent case, information recorded in EDIS did not pass to Enterprise "accurately and reliably" or, under certain circumstances, did not transfer at all. (*Id.* at ¶ 101–102.)

Some of the incompatibilities between EDIS and Enterprise arose as a result of the two programs' using different drug codification schemes. (*Id.* at ¶

112.) To work around this problem, EDIS and Enterprise used a text-matching algorithm to attempt to reconcile the two different drug codes. (*Id.* at ¶ 114.) The Relators describe this as a flawed system that frequently “caused failures with interaction checking.” (*Id.*) When the drugs entered into the EDIS system were transferred over (when a patient was admitted to a hospital from the emergency department), they appeared as different drugs, in different units, or with different methods of administrations in the Enterprise system. (*Id.* at ¶ 116.)

The Relators identify Company and Hospital “ClinRec Issues” calls in which this problem was addressed. (*Id.* at ¶ 118.) During three of these calls, in January, April, and July 2015, the faulty transfer of drug information between the two systems was highlighted. (*Id.* at ¶ 118–19.) Someone named Angela McKerrow described the interface as “junk” and said it had to be disabled. (*Id.* at ¶ 118.) Without an interface between the two programs, the medications were transferred from EDIS to Enterprise as uncodified and unstructured data that then had to be manually “cleaned[up]” by pharmacists. (*Id.*) On the July call, McKerrow referenced a mapping tool that was supposed to match seventy to eighty percent of the drugs from EDIS to Enterprise, but, she said, the number of unstructured data orders was still higher than expected. (*Id.* at ¶ 119.) The unstructured data caused downstream problems for nurses and doctors regarding drug dosages, frequencies, and interaction checking. (*Id.*) Someone named Amanda Dorr from Defendant Hospital Victoria of Texas LP (doing business as DeTar Hospital Navarro), complained, “patient safety issue had been horrendous without an EDIS interface.” (*Id.*) Some physicians described Medhost as “substandard” compared to two of its competitors. (*Id.*) McKerrow and someone named Tom Frundle explained the interface problem was the result of the acquisition of two different Medhost programs. (*Id.*) They explained the issues would be resolved by a promised Medhost mapping tool. (*Id.*) Interface failures persisted through October 27, 2015. (*Id.*)

There were also allergy importing errors with Enterprise, as noted in a “log from 2015.” (*Id.* at ¶ 120.) Medhost acknowledged that this functionality, when importing allergies from something called “CCD,” wasn’t working and that allergies needed to be entered manually. (*Id.*) The issue was slated to be fixed in later software releases which were not certified until June 2015 and November 2015. (*Id.*) Compounding this problem, Medhost “did not include many basic allergies in its coding.” (*Id.* at ¶ 121.) “This necessitated the creation of one-off hard coded additions to each hospital’s software.” (*Id.*) Someone from Defendant Lake Wales Hospital Corporation complained that the

facility had to manually update the software's allergy lists; otherwise, imported allergies would not be subject to allergy-interaction checking. (*Id.* at ¶ 121–22.) According to the representative from the Lake Wales hospital, many of the missing allergies were basic and should have already been a part of the standard software. (*Id.* at ¶ 121.)

Similarly, when Enterprise was unable to find a match for the drug or allergy code being imported from EDIS, the code would be entered into Enterprise as unstructured data. (*Id.* at ¶124.) But Enterprise excludes unstructured data from medication and allergy lists that it uses for drug-interaction checks. (*Id.* at ¶ 125.) Medhost learned of one incident where this happened, at Defendant Cedar Park Health System LP's facility, in May 2014, when a drug administered through a "patient controlled administration" failed to flag as an allergy. (*Id.*) The Relators say that Medhost "was made aware that there were more examples where there were no alerts to an allergy." (*Id.* (cleaned up⁶.) Exacerbating these issues, were the Hospitals' frequent use of unstructured medication entries for medications brought in by patients from home. (*Id.* at ¶ 126.) When Enterprise imports a code as an unstructured data element, it fails to import along with it any information on "the route, frequency, or unit of measurement for the relevant medication." (*Id.*) The Relators says this can lead to errors if a doctor continues the home medication while the patient is in the hospital. (*Id.*) After multiple revisions, Medhost's text-matching algorithm worked less than seventy percent of the time under test conditions in the case of home medications. (*Id.* at ¶ 127.)

Further, Medhost's software's drug interaction checks do not function reliably with "custom and local medications." (*Id.* at ¶ 128.) These custom and local medications are often not "on the hospital formulary." (*Id.* at ¶ 129.) Because of this, they do not have identifiers in Enterprise. (*Id.*) Although providers can order such medications in Enterprise, those medication orders are not screened for drug interactions because they don't have identifiers. (*Id.*)

Lastly, the Relators say that Medhost's "Clinical Information Reconciliation software module"—"ClinRec"—did not function properly. (*Id.* at ¶ 136.) In late April or early May 2014, after a recent rollout to the Hospitals of new Enterprise features, the Hospitals noticed that when doctors tried to continue a medication that a patient was already taking, the entry showed up

⁶ The Court uses (cleaned up) to indicate that internal quotation marks, alterations, and citations have been omitted from quotations. See, e.g., *United States v. Reyes*, 866 F.3d 316, 321 (5th Cir. 2017).

as a new order, rather than as a continuation. (*Id.*) This could result in a whole host of problems, including overdoses. (*Id.*) When the Companies and the Hospitals notified Medhost of this problem in early May 2014, Medhost replied that the system was functioning as designed. (*Id.*)

Recognizing the severity of the problem, the Companies and the Hospitals implemented a workaround, using manual checks to account for the ClinRec issue. (*Id.* at ¶ 137.) Medhost began working on a resolution and deployed a software fix on June 11, 2014. (*Id.* at ¶ 138.) Despite this fix, in June 2015, the Companies and the Hospitals notified Medhost that the problem persisted. (*Id.* at ¶ 141.)

ClinRec also could not properly “reconcile home medications.” (*Id.* at ¶ 139.) The Companies and the Hospitals notified Medhost, in July 2014, that, when home medications were imported from EDIS into Enterprise and then reconciled using ClinRec, the software often populated forms with the incorrect units of measurement. (*Id.*) Further, these incorrect units could not be edited and became permanent parts of the patients’ home medication records. (*Id.*) Further, ClinRec was also not maintaining patient’s records of home medications throughout the entirety of their hospital stays. (*Id.* at ¶ 141.) This prevented doctors from being able to discharge patients with the same home medications they were taking before their hospital stay. (*Id.*) Further affecting discharge, the Hospitals noticed that the brand name and the generic name of the same drug would sometimes appear on the discharge ClinRec screen. (*Id.* at ¶ 140.) If the error wasn’t caught, this could result in a patient’s being instructed to take twice the amount of medication the doctor actually intended. (*Id.*) This particular issue was raised on a call with Medhost in April 2015. (*Id.*) Ultimately, say the Relators, despite all these problems with Medhost’s software, Medhost continued to certify and re-certify its software as to the Clinical Information Reconciliation criterion of meaningful use. (*Id.* at ¶ 142.)

D. Issues with Medhost’s Use of Computerized Provider Order Entries

The Relators say that, in their capacity as managers working on Company and Hospital teams to roll out and support health IT software, they were notified by physicians and other hospital personnel of the functional and safety issues with Medhost’s “computerized provider order entry” software. (*Id.* at ¶ 93.) These issues included “errors in medication selection and dose calculation, failure to trigger delivery of medications at the correct time, and inability to reliably perform drug-drug and drug-allergy checking.” (*Id.*) The

Relators say they “believe . . . this list of issues represents only a sample of the required functions that were lacking in [the] software.” (*Id.*)

More specifically, the Relators complain that Medhost’s software was incapable of recording medication orders in an accurate and reliable manner. (*Id.* at ¶ 154.) For example, they say, “under certain circumstances,” Medhost’s “ClinView module fails to calculate and record the dose for weight-based medications accurately.” (*Id.* at ¶ 155.) The Relators highlight one particular circumstance where this occurs: when the software calculates a dosage for weight-based medications requiring a “drip-rate,” which is the rate at which medications are to be administered through an intravenous drip. (*Id.*) Because of this flaw, the Companies and the Hospitals instructed their pharmacists not to rely on the Medhost software’s drip-rate calculations and to manually calculate the rate. (*Id.* at ¶ 156.)

This same ClinView application also, “[u]nder certain circumstances, . . . miscalculates the dose ordered by the user due to a medication name mismatch in its weight-based dosing window.” (*Id.* at ¶ 157.) This can occur when a doctor uses ClinView to calculate the dose for a weight-based medication, but the software calculates the dosage for a different medication. (*Id.*) Indeed, the Director of Pharmacy from the DeTar facility recognized this, in May 2014, when she alerted the Company and Hospital Software deployment team to the problem. (*Id.* at ¶ 158.) She advised the team, after a training session associated with the rollout of Medhost software updates, that when she tried to run the weight-based dosing feature, the program, at least twice, pulled the wrong medication for the calculation. (*Id.* at 158–59.)

There were also glitches with the functionality of a “Send Dose Now” checkbox feature in the ClinView application. (*Id.* at ¶ 160.) The feature was intended to enable doctors to order medications to be administered to a patient immediately. (*Id.*) However, the feature did not work as intended and instead defaulted to ordering that the medication be delivered to the patient at the next scheduled delivery. (*Id.*) At some point, perhaps prior to April 2014, the issue “was flagged as ‘high priority’ and ‘impacting all sites.’” (*Id.* at ¶ 162.) Medhost thereafter disabled the feature at the end of July 2014. (*Id.*) An August 2014 issue log reported the problem was resolved by disabling the checkbox and advising, “sites trained to not use button.” (*Id.*) In the meantime, the Companies and the Hospitals did not disable the defective checkbox on their own and instead told doctors to either call the pharmacy to clarify the orders or enter two separate orders for the medication. (*Id.* at ¶ 163.)

Other problems arose as a result of the way a patient's clinical history was stored. (*Id.* at ¶ 165.) Ordinarily, when patients are admitted to the hospital, information regarding their weight, body surface area, and creatinine levels are inputted as part of their clinical history profile. (*Id.*) This information can then be used to determine dosage calculations for certain medications. (*Id.*) However, these measurements can change over the course of an inpatient stay. (*Id.* at ¶ 166.) And while these new measurements can be entered into the software, the new measurements do not update the patient's clinical history profile. (*Id.*) The software then uses outdated measurements, from the clinical history profile, to calculate medication dosages. (*Id.*) In July 2014, or perhaps before, the Companies and the Hospitals, collectively, flagged this issue for Medhost. (*Id.* at ¶ 168.) During a "Physician Tools User Group" call, at the Companies and the Hospitals, in October 2014, the participants discussed how a change in a patient's weight that was updated in one module, did not update the weight in the patient's clinical history profile. Medhost "did nothing to remedy the issue." (*Id.*)

The Relators also identify an issue regarding medication orders that are to be administered on an as-needed basis. (*Id.* at ¶ 171.) In July 2014, the Director of Pharmacy at the Fallbrook Hospital—which is not listed as a defendant—wrote to Company and Hospital Pharmacy Informatics Manager Jeannie Bennet that the software was not processing "as-needed" medication orders properly. (*Id.* at ¶ 172.) Medhost described the problem with this functionality as a "limitation of the system." (*Id.* at ¶ 173.) Medhost did not fix the problem and one of its employees wrote the Companies and the Hospitals, saying, "[A]t some point nurses treating patients have to take some clinical responsibility because Medhost software cannot be made fool proof." (*Id.* (cleaned up).)

Other malfunctions involved various other software features: the Physician's Favorites lists; a drug-administration verification functionality; discharge medication reconciliation; and a variety of other medication-ordering tools. (*Id.* at ¶¶ 174–190.) Using the Physician Favorites tool resulted in errors when a hospital would change, for example, drug-specific information such as the applicable unit of measurement (for instance from grams to milligrams). (*Id.* at ¶ 176–77.) Although a doctor would be alerted to the change if she used the software's "normal" computerized-provider-order-entry interface, the doctor would not be alerted if she used the Physician Favorite tool. (*Id.* at ¶ 177.) Medhost assured Company and Hospital Pharmacy Informatics Manager Cliff Kolb, in June 2014, that the software would not allow a change to any drug

information if that drug was saved in a physician's favorites. (*Id.* at ¶ 178.) Some pharmacists, however, said they had entered changes to the unit of measurements for various drugs and the system allowed the changes even though the drugs were saved as favorites. (*Id.*)

Similarly, the Relators point to problems with Medhost's software and its ability to deal with medication orders calling for a partial dose of a drug—that is, a dose that is less than the normal full dose found in a hospital's formulary. (*Id.* at ¶ 181.) According to the Relators, when hospitals fill a medication order using an automated dispensing machine (such as a system called "Pyxis," which is used by the Companies and the Hospitals) for a partial dose of a drug, the machine automatically dispenses the full dose. (*Id.*) The system does not provide any alert that the dispensed dose is different from the ordered dose. (*Id.*) Medhost was notified, during an October 16, 2014, "issues call" that a patient at Defendant Lake Wales Hospital Corporation received an overdose of potassium because of the automated dispensing flaw. (*Id.* at ¶ 183.) The system failed to alert providers to other discrepancies between the dose ordered and the dose dispensed. For example, in May 2014, a nurse at Cedars Park alerted Company and Hospital "information systems personnel" about an issue with a particular drug dose. (*Id.* at ¶ 182.) In that case, a doctor had "entered an order for Xaralto 10 mg" into the Medhost software. (*Id.*) But, "because the physician put 1 tablet as the dose, Pyxis dispensed 'Xaralto 1 mg.'" (*Id.*) The nurse said this dosage error had occurred on multiple occasions. (*Id.*) Company and Hospital Chief Nursing Officer Rudisill said another flaw in the software involved a disconnect between the doses requested for automatically dispensed injectable drugs that were supposed to be administered as multiple doses. (*Id.* at ¶ 184.) For these drugs, Medhost's eMAR system ("electronic Medication Administration Record") recorded the medication as fully administered after the first of multiple units was scanned—regardless of the number of individual vials or units that comprised the dose. (*Id.*) The Relators say the Companies and Hospitals learned of this problem in January 2014. (*Id.*)

Another computerized-provider-order-entry problem involved medication orders placed for patients upon discharge from the hospital. (*Id.* at ¶¶ 185–86.) Medhost's software failed to "perform drug interaction checks when a provider continues or discontinues a medication during discharge reconciliation." (*Id.* at ¶ 186.) Other problems involved medication orders that doctors entered into the software, but which were never transmitted to a hospital's pharmacy. (*Id.* at ¶¶ 187–90.) Company and Hospital Pharmacy Informatics Manager Kolb complained of this issue occurring at Defendant Shelbyville Hospital Company

LLC, in March 2014, where a doctor would enter a medication order but, unbeknownst to either the doctor or the pharmacist, the order was not actually sent. (*Id.* at ¶ 187.) Similar issues were reported at the DeTar facility in May 2015 (medication orders not transmitted) and at Defendant Las Cruces Medical Center LLC in May 2014 (problems with “building IV packs”). (*Id.* at ¶¶ 188–89.) Someone named Teresa Stines at DeTar told Kolb, Bennet, and someone named Dale Resch, during a facility visit, that “pharmacists at her facility had to revise approximately 40% of medication orders entered electronically using Medhost.” (*Id.* at ¶ 190.) Company and Hospital Director of Clinical Informatics Connie Senseney was assigned to resolve this issue in Company and Hospital logs. (*Id.*)

Despite all these flaws, the Companies and the Hospitals continued to attest to meaningful use under the computerized-provider-order-entry measure and Medhost continued to obtain recertification of its software based on this criterion. (*Id.* at ¶¶ 156, 159, 164, 170, 173.) The Relators also say that “to [their] knowledge,” as of late 2016, Medhost had yet to fix various software flaws and yet continued to seek and receive certification of its software for the computerized-provider-order-entry criterion. (*Id.* at ¶ 173.)

E. Issues with the Companies and Hospitals’ “Order Sets”

The Relators explain that “[a]n order set is a curated selection of related medication and other orders—designed for application in a specific scenario—that a doctor can select quickly and easily using [computerized provider order entry].” (*Id.* at ¶ 194.) The order sets that the Companies and Hospitals created, however, “were rolled out to the hospitals with a large volume of dangerous errors.” (*Id.* at ¶ 196.) By way of examples, the Relators point to several instances where the order sets led to medication errors. (*Id.* at ¶¶ 197–99.)

For example, in September 2013, a “deployment team” at Defendant Marrion Hospital Corporation (doing business as Heartland Regional Medical Center),⁷ reported that “available pharmacy/formulary NDC code does not match the order set content.” (*Id.* at ¶ 197.) In March 2014, Kolb wrote to others on the Company and Hospital “implementation team” detailing various problems with the order sets being rolled out at six facilities. (*Id.* at ¶ 198.) One problem involved the drug Zofran: an entry ordering “Zofran 4 mg was mapped to the 40 mg vial not the 4 mg vial which could cause a 10[-]fold overdose.” (*Id.* at ¶ 198.) Also, orders requesting preservative-free hydromorphone and

⁷ This case is stayed with respect to this Defendant. (ECF No. 156.)

morphine “were mapped to regular form.” (*Id.*) A few weeks later, Company and Hospital Director Pharmacy Operations Jerry Reed told Company and Hospital Vice President of Operations Support Tim Park that using the order sets resulted in “acetaminophen suppositories[’ being] mapped to orally” and “normal saline is asking for weight[-]based dosing.” (*Id.* at ¶ 199.) In response, Park opined, “These medication sentences have **a very high potential** for causing a catastrophic event.” (*Id.* at ¶ 200 (emphasis in original).) To address these problems, the Companies and Hospitals “instructed non-clinical staff, including Relator Neiman, to resolve the safety issues while prioritizing strategies to meet the target dates for implementation to ensure that [the Companies and Hospitals] would receive Meaningful Use incentive payments.” (*Id.* at ¶ 201.)

F. Issues with Medhost’s Software’s Ability to Perform Clinical Decision Support

(1) The Software

Clinical decision support “is a process designed to aid directly in clinical decision making, in which characteristics of individual patients are used to generate patient-specific interventions, assessments, recommendations, or other forms of guidance.” (*Id.* at ¶ 205.) These interventions “are then presented to a decision-making recipient or recipients that can include clinicians, patients, and others involved in care delivery.” (*Id.*) The Relators say that Medhost’s Enterprise software “is unable to reliably perform [clinical decision support] or track when and whether [clinical-decision-support] rules have been enabled.” (*Id.* at ¶ 207.)

The Relators say the Companies and Hospitals learned that the clinical-decision-support “rules” had completely stopped working on August 14, 2014. (*Id.* at ¶ 208.) Relator Neiman, says, in September 2014, he “discovered that the [clinical-decision-support] rules were not working at any of the 17 hospitals he checked.” (*Id.*) Neiman created a help-desk ticket with Medhost to notify it of the problem, following up on September 18, 2014. (*Id.* at ¶ 210.) The Companies and Hospitals discussed the problem with Medhost during an “issue call” on September 30, 2014. (*Id.*) Medhost explained it would have to rebuild the clinical-decision-support code to resolve the problem. (*Id.*) Company and Hospital “Director of IS” Tim Moore, at something called “Quorum Health,” addressed the issue with Neiman several times throughout 2014 to “address the reporting and rule ‘not firing’ issues.” (*Id.*)

Although Medhost “rebuilt” the clinical-decision-support functionality in early October 2014, it continued not to function. (*Id.* at ¶ 211–12.) The Relators say that the Company and Hospital management learned, in late October 2014, that the clinical-decision-support functionality was still failing. (*Id.* at ¶ 212.) Company and Hospital Regional Clinical Informaticist Phyllis J. Fawcett emailed “the implementation team” on October 28, 2014, saying that “according to the Acknowledgment report,” “the triggers stopped firing on the 15th.” (*Id.*) She continued, explaining that “according to the status report the rules have not been active for 0 to 28 days.” (*Id.*) In an email responding to an “issue ticket” submitted by a hospital, Medhost acknowledged, on November 20, 2014, that clinical-decision-support rules’ “not showing on the ODS Acknowledgement Report is a known issue.” (*Id.* at ¶ 213.) At the same time, Medhost said it was working on a program fix that it believed would be completed and implemented “soon.” (*Id.*) As late as December 2014, Medhost still had “two software enhancement requests . . . open.” (*Id.* at ¶ 215.) Vice President and Deputy CIO Jay Skibinski maintained a list of these requests from November 2014 onward. (*Id.*)

Despite these clinical-decision-support issues, Medhost nevertheless repeatedly certified multiple versions of its software as to clinical decision support from November 2013 through August 2014. (*Id.* at ¶ 214.)

(2) Meaningful Use Issues

The Relators complain that the Companies and Hospitals’ clinical-decision-support rules and interventions didn’t meet meaningful-use objectives. (*Id.* at ¶ 220.) To begin with, the Relators say the Companies and Hospitals did not use Medhost’s rules engine, during stage 1, to program its intervention. (*Id.* at ¶ 221.) Instead, they say, the Companies and Hospitals used a “workaround” which involved an unrelated function of the electronic health records as though it were a clinical decision support. (*Id.*) This workaround relied on a protocol that nurses used to perform fall-risk assessments. (*Id.*)

This protocol was based on a Company and Hospital workflow guide that required nurses to identify the need to perform fall-risk assessments on patients. (*Id.* at ¶ 222.) Once a nurse decided to perform the assessment, the nurse would select an option in the electronic health record. (*Id.*) Once selected, the program would display a series of questions based on a common method to calculate fall risk. (*Id.*) Each question called for a numerical answer. (*Id.*) At the end of the assessment, the software would total the numbers and

produce a “Fall-Risk” score. (*Id.*) The nurse then had to select a check box, indicating whether the score was more or less than twenty-five. (*Id.* at ¶ 223.) If the nurse selected the checkbox for a score less than twenty-five, the assessment ended; if the nurse selected the checkbox for a score greater than twenty-five, the software prompted the nurse to select a care plan from a list of plans. (*Id.*) The nurse then had to manually add the care plan to the patient’s profile. (*Id.*)

The Relators claim the Companies and Hospitals were aware that this workaround “did not meet the objective and measure for [clinical-decision support]” based on an unnamed Company and Hospital employee’s explaining:

For stage 1 we did not have any actual CDS rules built [in the Medhost rules engine] because CPOE was not active. So, what we did was, we used the Nursing Fall risk assessment within Pt care. When a nurse completed the fall risk assessment then the assessment would prompt the nurse to create a risk specific care plan based on the fall risk score.

(*Id.* at ¶ 226 (alteration in original).) Further, say the Relators, the Companies and the Hospitals knew that they lacked the ability to track providers’ compliance with the care plan. (*Id.* at ¶ 227.) This alleged awareness is based on an email Company and Hospital Clinical IS Team Lead—Physical Tools Lisa Fitts sent on April 8, 2014. (*Id.* at ¶ 228.) In that email, which was sent to “several [Company and Hospital] employees,” Fitts opined, “It does not sound like the care plan would be captured on a CDS audit report. I say this because I don’t know that a care plan can be designated as a CDS rule [in the rules engine].” (*Id.*)

Second, the Relators say, when the Companies and Hospitals started using Medhost’s rules engine, during stage two, the rules engine did not work, as set forth above, for “much of” the attestation period. (*Id.* at ¶ 232.) To bypass this problem, the Relators explain that the Companies and Hospitals “turned to a ‘workaround’ to support [their] attestations.” (*Id.* at ¶ 233.) The Relators identify several Company and Hospital employees who either developed the workaround or who “were aware” the workaround would not comply with the clinical decision support objectives. (*Id.*) The workaround itself involved developing five static order sets that related to four or more clinical quality measures required for attestation. (*Id.*) But the content of these order sets was static and did not trigger alerts based on a patient’s problem list, medication list, demographics, vital signs, or lab results. (*Id.* at ¶ 234.) Further, the electronic health record did not spontaneously suggest particular order sets to

providers based on patient information. (*Id.*) Instead, providers had to choose the order sets manually from a wider list of available order sets in the system. (*Id.*)

Director of IT Internal Audit and Compliance Kristi Meyer realized, a week after the end of the attestation reporting period, on October 6, 2014, that “several of the hospitals did not have the five order sets that they intended to use for attestation.” (*Id.* at ¶ 236.) Relator Neiman says this prompted Meyer to ask him to investigate, apparently telling him:

[A]fter reviewing the evidence, we identified 8 hospitals that only had 3 of the “approved” order sets active the entire time. Therefore, could your team provide us with a listing of all active order sets from 7/1–9/30 for those 8 hospitals? Based on your output, we will work with OPS to determine the other order set to use for attestation.

(*Id.*) Three weeks later, on October 30, 2014, Meyer sent an update, stating that the eight facilities were still in “limbo,” lacking sufficient order sets for attestation. (*Id.* at ¶ 237.) She thereafter “determined to add the fall risk assessments, which [the Companies and Hospitals] had relied upon for Stage 1, as a final intervention.” (*Id.*)

Despite these stage two issues, on November 1, 2014, the Hospitals submitted their attestations to the Centers for Medicare and Medicaid Services using the described workaround for the order sets. (*Id.* at ¶ 237–38.)

G. Issues with Medhost’s Electronic Prescribing Feature

Medhost relied on “outside e-prescribing software, DrFirst Rcopia, for its e-prescribing certification.” (*Id.* at ¶ 242.) But, say the Relators, sometimes, “[w]hen users created a prescription electronically using Medhost [software], the information in that prescription often would not cross over to DrFirst [for] transmi[ssion] to the pharmacy.” (*Id.* at ¶ 243.) Other times, “the information that crossed over to DrFirst would be different than the information in the prescription the user had created in [the Medhost software].” (*Id.*)

The Companies and the Hospitals, between 2014 and 2016, tested Medhost’s e-prescribing function, but, apparently because of these issues, found it unreliable and decided not to implement it. (*Id.* at ¶ 244.) Relator Neiman says that he attended a meeting, in early 2014, where Medhost’s demonstration of the functionality showed “that medication information recorded for a patient . . . sometimes would not appear . . . in DrFirst.” (*Id.*) Later, in September or October 2015, Company and Hospital Vice President

and Deputy CIO Skibinski, reported that, after testing, the Companies and Hospitals found that prescriptions did not necessarily cross from Medhost's software to DrFirst accurately. (*Id.* at ¶ 245.) Based on Skibinski's assessment, the Companies and Hospitals did not adopt Medhost's software with DrFirst for e-prescribing. (*Id.*)

H. Issues with Medhost's "Auditable Events and Tamper Resistance"

The Relators say Medhost's software allowed all users to access, view, and modify patient and other electronic health information, without, under some circumstances, an audit record. (*Id.* at ¶¶ 249, 251.) As explained by the Relators, patient and financial data is stored on "AS400 servers that run the back-end portion of Medhost's software." (*Id.* at ¶ 250.) "These servers also store all of the patient and other financial data used and generated by Medhost software in various database tables." (*Id.*) According to the Relators, this "vulnerability arises from the way Medhost software handles 'objects' on the back-end servers." (*Id.* at ¶ 252.) They say "the data tables are configured with a setting: 'Public Authority *all'" which "allows access to the data tables for any individual with Medhost credentials and allows both viewing and changing of the data." (*Id.*) As the Relators further detail, "this method of object handling [allows] any user [to] use FTP, ODBC, or JDBC connections to view and modify the data tables." (*Id.* at ¶ 253.) Further, they say, "any access or changes made to data table[s] using these methods will not be captured by Medhost's audit logging." (*Id.*)

Company and Hospital employee Jim Berryhill described the issue to Relator Lewis in 2009. (*Id.* at ¶ 254.) The Relators say the "issue continued to exist through at least August 2015, when Company and Hospital Senior Vice President and CIO Manish Shah convened a meeting to discuss how to address the issue. (*Id.*) The Relators also relay that Medhost "knew about the issue no later than October 2014." (*Id.*)

I. Issues Related to the HMA Hospitals

In January 2014, the Companies and Hospitals acquired Health Management Associates, a for-profit hospital chain. (*Id.* at ¶ 255.) This added seventy-one facilities to the Companies and Hospitals' network of hospitals. (*Id.* at ¶ 255.) These "HMA" hospitals used modular electronic health record technologies. (*Id.* at ¶ 256.) Sixty of the HMA hospitals submitted meaningful use attestations and were paid a total of \$206 million in incentive payments. (*Id.* at ¶ 258.)

According to the Relators, the modular technologies on which the HMA hospitals relied failed to make clinical information stored in one system reliably accessible to other systems. (*Id.* at ¶ 259.) For example, the HMA hospitals' emergency department information systems "did not interface" with their inpatient system to transmit information. (*Id.* at ¶ 260.) Except for a patient's demographic information, billing information, laboratory order and results, and radiology order and results, all other essential data would have to be transferred from the emergency department to the inpatient facility using printed copies of a patient's records. (*Id.* at ¶¶ 260–61.) The printed records would then be used to hand-type the information into the inpatient system. (*Id.* at ¶ 261.) During the admission process, which would take place before the records were fully transferred, the admitting nurse would receive a condensed patient file from the emergency department via fax. (*Id.*)

Further, the HMA hospitals' inpatient software "did not provide a medication order interface with the hospitals' [computerized-provider-order-entry] application," called "PatientKeeper." (*Id.* at ¶ 262.) Instead, medication orders entered into PatientKeeper by doctors had to be printed out so that the orders could be reviewed by the nursing staff. (*Id.*) Additionally, the admitting doctor would need to re-enter medication orders initially placed in the emergency department, in PatientKeeper, if the admitting doctor wanted to continue or modify those medications. (*Id.*) Because of these issues, the HMA hospitals programmed PatientKeeper to print all medication orders automatically. (*Id.*)

A third issue that arose as a result of the HMA hospitals' use of modular technologies was because of a lack of an interface between PatientKeeper and a pharmacy management system called Horizon Meds Manager. (*Id.* at ¶ 263.) When a doctor entered an order into PatientKeeper, it did not appear in Horizon. (*Id.*) Instead, PatientKeeper generated an email to the pharmacist who would then have to transcribe the contents into Horizon for processing. (*Id.*)

Another problem with the lack of interoperability of the HMA hospitals' technologies, say the Relators, is that it prevented users from being able to "reconcile clinical information." (*Id.* at ¶ 269.) This is because the HMA hospitals store active medication lists, problem lists, and medication allergy lists in a system that doctors do not have access rights to. (*Id.*) Instead, for doctors to reconcile the clinical information in that system with clinical information from other sources, "a nurse must print the patient's medication reconciliation form for the physician to complete by hand." (*Id.*) Upon

completion of the form, the nurse would then have to manually re-enter the contents of the form into the first system. (*Id.*)

Despite these flaws, the Relators say the HMA hospitals nonetheless submitted meaningful-use attestations during stages one “and/or” two. (*Id.* at ¶ 271.) The Relators say the Companies and Hospitals knew about all these shortcomings based on a number of reports and complaints they received. (*Id.* at ¶ 272.) First, prior to its acquisition of the HMA hospitals, the Companies and Hospitals hired a consulting firm to evaluate HMA’s “readiness to meet Stage 2 requirements.” (*Id.*) The consulting firm, in a December 3, 2013 report, identified several issues: “HMA’s complex application portfolio results in excessive potential points of failure and limits key functionality”; “medication orders [that] were ‘highly fragmented involving duplicate data entry and manual workarounds that increase the potential for errors’”; “the number of order entry systems and complex set of clinical workflows that have been created increase the opportunity for more gaps in care and patient safety risks.” (*Id.* (cleaned up).) The firm concluded the HMA hospitals were not close to meeting stage two requirements. (*Id.* at ¶ 273.) It noted HMA hospitals “had deployed PatientKeeper at only 32 of its 71 hospitals and was not scheduled to complete deployment at the remaining hospitals until May 27, 2014”; “Clinical Decision Support . . . is currently not implemented in MAP nor evident in product roadmap”; “the fragmentation of applications, workflows and clinical processes impacts patient safety and potentially creates significant financial risks (MU Stage 2 and HIPAA compliance).” (*Id.*)

In a later report to the Companies and Hospitals, on January 6, 2014, the firm “found that significant applications remained in development.” (*Id.* at ¶ 274.) In this regard, the firm noted certain software lacked functionality for “transitions of care, data portability, consolidated clinical document architecture, . . . and interfaces with other applications.” (*Id.*)

Furthermore, continue the Relators, the HMA hospitals knew their electronic-health-record systems lacked required functionality and alerted the Companies and Hospitals. (*Id.* at ¶ 276.) As evidence of this knowledge, the Relators point to issues involving an HMA hospital—Midwest Regional Medical Center—in Midwest City, Oklahoma. (*Id.* at ¶¶ 276–80.) The Relators say that the Companies and Hospitals had received numerous complaints from Midwest Regional about its inpatient software’s “cumbersome workflows, unsafe functionality, and unstable infrastructure.” (*Id.* at ¶ 276.) Various doctors, additionally, were threatening to stop referring patients to Midwest Regional if the problems persisted. (*Id.*) In June 2015, Relator Lewis joined two of the

leaders of the Companies and Hospitals’ deployment team—Vice President Michael Yzerman and Vice President of Information Systems Steve Hernandez—on a visit to Midwest Regional in order to “evaluate whether to transition Midwest Regional to a different [electronic-health-record] system.” (*Id.*)

During the visit, doctors told the Company and Hospital executives that Midwest Regional was relying on paper records and printouts to bridge gaps between different systems used throughout the facility. (*Id.* at ¶ 277.) Additionally, doctors in the cardiology department said “medication reconciliation” was a “huge patient safety concern” that they feared would “kill a patient.” (*Id.* at ¶278.) One cardiologist in particular told the Company and Hospital executives that doctors had to use paper to reconcile medication lists because they did not have access to the inpatient software that the nurses used. (*Id.*) Continuing, the cardiologist said this led to various errors relating to medication orders. (*Id.*)

Relator Lewis attended meetings at Midwest Regional where its CFO and “NP and Pulse champion” “reported many specific concerns about PULSE [the inpatient software] in relation to patient safety.” (*Id.* at ¶ 279.) The CFO, frustrated with the inpatient software, even threatened to leave Midwest Regional if the software failures were not resolved immediately. (*Id.*) The CFO “was directly involved with the hospital’s Meaningful Use attestation and may have signed the attestation packet submitted to the government.” (*Id.*) At the time of the June 2015 visit, “Midwest Regional had attested to its meaningful use of certified [electronic-health-record] technology on four occasions and received \$5.95 million in Meaningful Use incentive payments from the Government.” (*Id.* at ¶ 280.) The Relators maintain that these issues were not isolated to Midwest Regional. (*Id.*) They say that Company and Hospital Vice President of IT and Vice President of Data Analysis “had direct and substantial knowledge of [inpatient software] failures across many [Company and Hospital] facilities.” (*Id.*)

J. Medhost’s Provision of Free Software, an Equity Interest, and Discounts to the Companies and Hospitals

Medhost began providing the Companies and Hospitals, “no later than 2013,” with free financial software. (*Id.* at ¶ 281.) Prior to this, for nearly three decades, the Companies and Hospitals had used and paid for the software—which can perform hospital accounting, billing, and other management functions—at most of their hospitals. (*Id.* at ¶¶ 281–82.) Medhost provided free licenses for its financial software package to “at least” nineteen Hospitals. (*Id.* at ¶ 281.) With each license being worth approximately \$250,000, this

amounted to a value of around \$4,750,000. (*Id.*) The Relators say Medhost's free provision of the software coincided with Medhost's expansion into clinical software. (*Id.* at ¶ 283.)

The Relators also maintain Medhost offered the free financial software to all the Hospitals. (*Id.*) "For each hospital, Medhost only required that [the Companies and Hospitals] pay approximately \$137,000 for accompanying software products and interfaces, including Advanced Security, eArchive, Insurance Eligibility, and SSI Electronic Billing." (*Id.*) Company and Hospital employees, say the Relators, discussed amongst themselves "that Medhost's offer was intended to induce [the Companies and Hospitals] to continue doing business with Medhost and, specifically, to purchase Medhost Enterprise," Medhost's clinical software (which could then be used by the hospitals to attest to meaningful use). (*Id.* at ¶ 284.) The Relators believe that, "[e]ven for . . . hospitals that continued to use third-party [electronic-health records], Medhost's goal was to maintain a software presence at the hospitals to increase the likelihood that [the Companies and Hospitals] would convert those hospitals to the Medhost [electronic-health records] in the future." (*Id.*)

After a couple of years, in September 2015, the Companies and Hospitals entered into an agreement with Medhost "to pay \$25 million to Medhost to convert ten . . . Tier-1 facilities to software and services offered by Medhost and purchase Medhost's surgical software suite . . . for all [Company and Hospital] facilities." (*Id.* at ¶ 285.) The Relators says that "[a]s part of [this] purchase, [the Companies and Hospitals] and Medhost entered into a side[]agreement whereby [the Companies and Hospitals] obtained equity in Medhost." (*Id.* at ¶ 285.)

Regarding the equity agreement, Relator Lewis says someone named Mr. Hanson told him that Company and Hospital Chief Financial Officer Larry Cash "insisted on completing the \$25 million [surgical software]/Tier 1 conversion in order for [the Companies and Hospitals] to obtain \$25 million in equity in Medhost." (*Id.* at ¶ 286.) None of the surgical software/Tier 1 purchase documents that Relator Lewis reviewed, however, included any reference to the \$25 million equity exchange. (*Id.*) Hanson also "continually questioned why [the Companies and Hospitals] insisted on spending capital on Medhost." (*Id.* at ¶ 287.)

Medhost also regularly offered discounts to the Company and Hospitals for its "software and maintenance." (*Id.*) The Relators say Chief Information Officer Gary Seay was "aware of these negotiated discounts for future business agreements between [the Companies and Hospitals] and Medhost." (*Id.*) In late

2016, when a Company and Hospital facility in Key West converted its electronic-health-records software to Medhost, Hanson questioned the move as “a superior product” “could have [been] implemented” “for an equivalent or lesser price.” (*Id.*) The Relators says that, “[o]n multiple occasions, [Company and Hospital] corporate leadership chose the Medhost [electronic-health] records software] for hospitals over the objection of [Company and Hospital] implementation and hospital staff.” (*Id.* at ¶ 288.) Medhost was chosen despite staff concerns about Medhost’s software’s “poor track record and a strong preference by doctors for other [electronic health records] that were of similar cost.” (*Id.*) By way of explanation, the Companies and Hospitals told Relators and other employees that the Companies and Hospitals “needed to ‘take care of its friends’ . . . and ‘make sure they get some business.’” (*Id.*) The Relators say that as an “example, Medhost Senior Vice President of Corporate Accounts Ken Williamson frequently took . . . Larry Cash to play golf where the [surgical] software purchase . . . and other Medhost software purchases . . . were negotiated.” (*Id.*)

2. Legal Standards

When considering a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6), the Court must accept all the complaint’s allegations as true, construing them in the light most favorable to the plaintiff. *Pielage v. McConnell*, 516 F.3d 1282, 1284 (11th Cir. 2008). Under Federal Rule of Civil Procedure 8, a pleading need only contain “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). The plaintiff must nevertheless articulate “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1949 (2009). “Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.” *Id.* Thus, a pleading that offers mere “labels and conclusions” or “a formulaic recitation of the elements of a cause of action” will not survive dismissal. *Id.* In applying the Supreme Court’s directives in *Twombly* and *Iqbal*, the Eleventh Circuit has provided the following guidance to the district courts:

In considering a motion to dismiss, a court should 1) eliminate any allegations in the complaint that are merely legal conclusions; and 2) where there are well-pleaded factual allegations, assume their

veracity and then determine whether they plausibly give rise to an entitlement to relief. Further, courts may infer from the factual allegations in the complaint obvious alternative explanation[s], which suggest lawful conduct rather than the unlawful conduct the plaintiff would ask the court to infer.

Kivisto v. Miller, Canfield, Paddock & Stone, PLC, 413 F. App'x 136, 138 (11th Cir. 2011) (citations omitted).

“In an action under the False Claims Act, Rule 8’s pleading standard is supplemented but not supplanted by Federal Rule of Civil Procedure 9(b).” *Urquilla-Diaz v. Kaplan Univ.*, 780 F.3d 1039, 1051 (11th Cir. 2015). Under Rule 9(b), “a party must state with particularity the circumstances constituting fraud or mistake,” although “conditions of a person’s mind,” such as malice, intent, and knowledge, may be alleged generally. Fed. R. Civ. P. 9(b). “The ‘particularity’ requirement serves an important purpose in fraud actions by alerting defendants to the precise misconduct with which they are charged and protecting defendants against spurious charges of immoral and fraudulent behavior.” *W. Coast Roofing & Waterproofing, Inc. v. Johns Manville, Inc.*, 287 F. App'x 81, 86 (11th Cir. 2008) (citations omitted). “When a plaintiff does not specifically plead the minimum elements of their allegation, it enables them to learn the complaint’s bare essentials through discovery and may needlessly harm a defendant’s goodwill and reputation by bringing a suit that is, at best, missing some of its core underpinnings, and, at worst, [grounded on] baseless allegations used to extract settlements.” *U.S. ex rel. Clausen v. Lab. Corp. of Am., Inc.*, 290 F.3d 1301, 1313 n.24 (11th Cir. 2002). Thus, the Rule’s “particularity” requirement is not satisfied by “conclusory allegations that certain statements were fraudulent; it requires that a complaint plead facts giving rise to an inference of fraud.” *W. Coast Roofing & Waterproofing*, 287 F. App'x at 86. “To satisfy this heightened-pleading standard in a False Claims Act action, the relator has to allege facts as to time, place, and substance of the defendant’s alleged fraud, particularly, the details of the defendants’ allegedly fraudulent acts, when they occurred, and who engaged in them.” *Urquilla-Diaz*, 780 F.3d at 1051 (cleaned up).

3. False Claims Act Claims Based on Meaningful-Use Attestations

Under the FCA, private citizens can recover damages on the federal government’s behalf from defendants who have made or caused false claims for government payment. The Relators explain the “theory of the[ir] case is simple: the [Company and Hospital] Entities presented, and Medhost caused to be presented, claims for federal subsidy payments under the Medicare ‘Meaningful

Use' incentive program knowing that the [electronic-health-record] software systems being used did not meet mandatory requirements.” (Pls.’ Resp. at 10.)

In particular, the Relators allege four distinct FCA claims against all the Defendants: (1) a presentment claim, which imposes liability when one “knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval” using federal funds, 31 U.S.C. § 3729(a)(1)(A); (2) a false-statements claim, which imposes liability when one “knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim,” *id.* at § 3729(a)(1)(B); (3) a conspiracy claim, which imposes liability when one “conspires to commit a violation” of the FCA, *id.* at § 3729(a)(1)(C); and (4) a reverse-false-claims count which imposes liability when one “knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the government,” *id.* at § 3729(a)(1)(G). (Am. Compl. at ¶¶ 299–302.)

A. Medhost

To summarize, the Relators contend Medhost defrauded the federal government into certifying its software and making meaningful-use incentive payments to the Hospitals that were not justified because of problems with Medhost’s software. The allegations against Medhost concern software that was designed by Medhost, certified under the Office of the National Coordinator for Health Information Technology criteria by a third party, Drummond Group Inc., and installed and used by the Hospitals, as described in detail, above. The Hospitals, in turn, attested to meaningful-use incentives based on their employment of that software.

Over the course of over 100 pages and over 300 paragraphs, the Relators allege essentially five basic problems with Medhost’s software. First, they complain two of Medhost’s software products, its emergency-department software—EDIS—and its inpatient software—Enterprise—were not interoperable with each other. The Relators maintain this lack of interoperability prevented departments using EDIS from communicating with departments that used Enterprise. Second, the Relators say these two software products did not reliably allow doctors to make use of computerized provider order entries, including functionalities involving order sets. Third, the Relators point out problems with the functionality of the Enterprise software’s clinical decision support functionality. Fourth, they allege Medhost’s electronic prescribing functionality was defective. And, finally, the Relators allege

Medhost's software was not adequately secure in that it failed to properly limit who could view and modify patient information.

More broadly, with respect to meaningful use, the Relators' FCA claims are based on the following: (1) Medhost fraudulently secured certification for its software from Drummond, knowing the software did not meet mandatory requirements; (2) the Hospitals then used those fraudulently obtained certifications to make attestations of meaningful use; and (3) based on these attestations, the government made improper incentive payments to the Hospitals.

To begin with, the Relators fail to allege their claims against Medhost with the particularity required under Rule 9(b). As Medhost points out, the Relators do not allege specific facts showing (1) precisely *what* misrepresentations were made by Medhost; (2) *where* and *when* those particular misrepresentations were made; (3) *who* made the misrepresentations; or (4) *how* any of Medhost's statement were misleading. (Medhost's Mot. at 18.) In response, the Relators maintain Medhost's software could not preform the functions required for certification, Medhost knew this, and yet, during the certification process, nonetheless represented that its software could perform the required functions safely and reliably. (Pls.' Resp. at 4.) The Relators, in their opposition, cite to dozens of paragraphs in their complaint that they say support their claims against Medhost. The Court has carefully reviewed every single paragraph, and finds the allegations presented are either conclusory, set forth facts that the Relators never sufficiently link to the fraudulent activity they accuse Medhost of, or lack the particularity required under Rule 9(b). Ultimately, the Relators' complaint fails to set forth facts that provide a nexus between what Medhost knew about its software and the Relators' allegations of fraud.

In support of their contention that "Medhost knew that its software failed to provide required functionality and misrepresented its software's ability to regularly perform functions required for . . . certification," the Relators cite to paragraphs 9 through 11 and 73 through 75 of the complaint. But these paragraphs do not in any way present facts that support the Relators' claims. Instead, these paragraphs set forth immaterial generalities,⁸ conclusory

⁸ (*E.g.*, Am. Compl. at ¶ 9 ("This case concerns [electronic-health-record] technologies developed and sold by . . . Medhost to hospitals nationwide, including numerous hospitals owned and operated by [the Companies and Hospitals].").)

allegations,⁹ and facts that are not connected to any particular fraud allegations.¹⁰ The Relators also direct the Court’s attention to over a dozen other paragraphs that they say show Medhost’s software was “substandard and dangerous” and could not perform its “required functions . . . safely or even at all.” (Pls.’ Resp. at 13 (citing Am. Compl. at ¶¶ 113–14, 124, 128–30, 138–39, 157, 159, 162, 173, 182).) But these allegations also fall well short of properly alleging either Medhost’s knowledge of the alleged fraud or the particularity required to allege fraud against Medhost. That is, to the extent the Relators allege actual facts, as opposed to conclusory allegations of wrongdoing, these facts are left dangling, unconnected to the Relators’ fraud allegations. For example, the Relators recount that the lack of interoperability between EDIS and Enterprise “caused failures with [drug] interaction checking with stunning frequency.” (Am. Compl. at ¶ 114.) The Relators also maintain, for instance, that, in July 2014, the Companies and Hospitals “notified Medhost” about issues with the software’s not “properly reconcil[ing] home medications,” which “caused a significant risk of incorrect dosing.” (*Id.* at ¶ 139.) The Relators also point out software failures that occurred “[u]nder certain circumstances.” (*Id.* at ¶ 157.) These allegations, and the others like them, though, do not set forth actual *facts* alleging that Medhost had knowledge of fraud or misrepresentations made to the government. *See U.S. ex rel. Barrett v. Beauty Basics, Inc.*, 2:13-CV-1989-SLB, 2015 WL 3650960, at *5 (N.D. Ala. June 11, 2015) (“Relators’ complaint must contain some facts creating an inference that the individual(s) who submitted the alleged false certifications to the government did so with knowledge of their falsity.”).

Intertwined with the conclusory nature of these allegations, is that the allegations also fail to allege the particularity required under Rule 9(b). Instead, to the extent specifics are provided, the Relators only point to some, unnamed, people within Medhost who knew about various problems with Medhost’s software; but they do not connect the problems these people were aware of to any specific false claim. For instance, in opposing Medhost’s motion to dismiss, the Relators point to an allegation detailing a complaint from a nurse at one hospital who alerted Company and Hospital “information systems personnel” of a dangerous drug dosage mix up in May 2014. (Am. Compl. at ¶ 182.) The

⁹ (*E.g.*, *id.* at ¶ 11 (“Medhost knew that its software failed to provide required functionality but sought certification of the software nonetheless.”); ¶ 75 (“Medhost misrepresented the ability of its software to perform functions required for the software to be eligible for certification”)).

¹⁰ (*E.g.*, *id.* at ¶ 10 (“Medhost’s software promised to enable users to create medication orders electronically, for example, but contained numerous flaws that meant that many of the orders that users created were recorded incorrectly.”)).

Relators fail, however, to connect this detail, and others like it, to the who, what, when, where, and how of *Medhost's* role in the alleged fraudulent conduct.

By way of another example, the Relators say the lack of interoperability between EDIS and Enterprise was discussed on multiple calls, in 2015, within the Companies and Hospitals. (*Id.* at ¶ 118.) In support, they name specific Company and Hospital employees who complained, internally, about problems with the software in various scenarios. (*Id.* at ¶¶ 118–19.) They then claim Medhost, as a whole, was aware of the problems because a Medhost “log” reflected “an error” and that Medhost advised it would fix the faulty allergy and drug interaction indicator. (*Id.* at ¶¶ 120–21.) From this the Relators then conclude Medhost fraudulently represented its software “met the requisite regulatory criterion.” (*Id.* at ¶ 120.) But who in particular at Medhost knew this? When did this person learn it? And how does this knowledge, in any event, fit into the Relators’ generalized allegations that the submitted claims were false? Were the people who were aware of the functionality failures also aware that those failures prevented the software from meeting the required criteria for certification? Did the people at Medhost who were involved in the certification process know about these software failures? When did they learn of them? How were these issues covered up during certification? In other words, where are the facts tying all these unconnected dots together with the fraud the Relators allege against Medhost? Who at Medhost had actual knowledge or reasonably should have known of the facts that allegedly made any of the specific claims at issue false? Nothing in the Relators’ complaint answers these questions.¹¹ At most the Relators’ allegations are merely consistent with Medhost’s software’s having been certified when it should not have been; but this is not enough to state a claim under the False Claims Act. See *Urquilla-Diaz*, 780 F.3d at 1056 (“At most, [the relator’s] allegations were

¹¹ Many of the complaint’s paragraphs the Relators cite to in their opposition to the motions to dismiss refer only to Medhost, generally, as having knowledge about or being aware of certain software functionality problems and failures. (*E.g.*, Am. Compl. at ¶¶ 210 (“Relator Neiman created a help desk ticket with Medhost to notify Medhost of the problem” and “Medhost acknowledged the issue”), 254 (“Medhost . . . knew about the issue no later than October 2014.”) In addition to referring to Medhost only generally, many of the Relators’ allegations are also wholly conclusory, devoid of the underlying facts necessary to survive dismissal. (*E.g.*, *id.* at ¶¶ 11 (“Medhost knew that its software failed to provide required functionality but sought certification of the software nonetheless.”); 95 (“Medhost knew that the technology did not enable users to perform the required functions but nonetheless represented to Drummond that its products were capable of performing those functions.”); 290 (“Medhost knowingly misrepresented to customers and to Drummond Group . . . that its [software] satisfied federal Meaningful Use requirements.”).

merely consistent with [the defendant's] having violated th[e] rule, but that is not enough to state a claim under the False Claims Act.”). The Relators allege facts showing that the rollout of Medhost’s software at the Hospitals was problematic, even chaotic, and that many features did not work properly, endangering patients, when used by a number of facilities. But these allegations do not amount to a showing of fraud. *Clausen, Inc.*, 290 F.3d at 1313 (noting that requiring plaintiffs to plead fraud without particularity prevents “them [from] learn[ing] the complaint’s bare essentials through discovery” and “needlessly harm[ing] a defendant’s goodwill and reputation by bringing a suit that is, at best, missing some of its core underpinnings, and, at worst, . . . used to extract settlement[.]”)

Furthermore, the cases on which the Relators rely are inapposite. For example, the Relators rely on *U.S. ex rel. Osheroff v. Tenet Healthcare Corp.* to demonstrate they have properly alleged the particularity required by Rule 9(b). 09-22253-CIV, 2012 WL 2871264 (S.D. Fla. July 12, 2012) (Huck, J.). But the portion of that decision the Relators rely on merely opines on whether the relator there had sufficiently alleged that the defendants had submitted actionable claims to the government. *Id.* at *5–6. Here, there is no dispute that the Relators have identified claims that were submitted to the government. The issue is the link between problems with the software, the specific falsity of the claims submitted and, with respect to Medhost, the knowledge of that falsity. *United States v. Kaman Precision Products, Inc.*, is equally unavailing. 609CV1911ORL18GJK, 2010 WL 11626636 (M.D. Fla. Apr. 19, 2010). There, the court found the government had sufficiently alleged a particular person who “had actual knowledge of the facts that made the [claim at issue] false.” *Id.* at *5. Here, in contrast, the Relators have failed to provide particularized examples of any Medhost employee’s specific knowledge that is linked to any particular false claim. Unlike in *Kaman*, here, the Relators’ complaint falls short because they do not allege any particular Medhost employee’s wrongdoing. *See id.* at *6 (finding complaint sufficient where it alleged a defendant employee manipulated computer records to cover up the use of non-conforming parts used in fuzes for bombs sold to the government); *see also, e.g., Grand Union Co. v. United States*, 696 F.2d 888, 890 (11th Cir. 1983) (finding sufficient allegations of wrongdoing where the complaint set forth facts showing check-out cashiers at the defendant grocer knowingly permitted the purchase of ineligible non-food items with food stamps).

In sum, the Relators have set forth various facts showing that an assortment of software functionalities did not work properly and that Medhost,

therefore, should not have been able to get its software certified. But in doing so, the Relators merely “provide[] the ‘who,’ ‘what,’ ‘where,’ ‘when,’ and ‘how’ of improper practices, but . . . fail[] to allege the ‘who,’ ‘what,’ ‘where,’ ‘when,’ and ‘how’ of *fraudulent* submissions to the government.” *Corsello v. Lincare, Inc.*, 428 F.3d 1008, 1014 (11th Cir. 2005) (emphasis added). And while the facts the Relators allege show they have first-hand knowledge of many issues that appear to render the software non-compliant with federal regulations, at least when it was used in various hospital settings, that knowledge does not amount to anything more than speculation with respect to the vast fraud they allege against Medhost. For the foregoing reasons, the Court dismisses the Relators’ claims against Medhost.

B. The Managing Company and the Hospitals

The Relators insist they have properly “identified the who, what, when, where and how of the false claims” they allege against the Managing Company and the Hospitals. (Pls.’ Resp. at 18.) In support, they point primarily to exhibit B, attached to their complaint, which they describe as identifying (1) each “hospital that claimed Meaningful Use subsidies by attesting to Meaningful Use based on relevant Medhost or PULSE software, (2) the date of each claim, (3) the relevant certification criteria the hospital attested to meeting for each claim, and (4) the amount the Government paid the hospital from the claim.” (*Id.*) They further point out that they alleged Medhost’s electronic-health-record software was “incapable of recording medication orders” and “was ineligible for certification for CPOE.” (*Id.* at 19 (citing Am. Compl. at ¶ 154).) The Relators then explain that, through their complaint, they have identified the specific software at issue and have linked that to a particular hospital and a particular meaningful-use attestation, identifying the date of the attestation and the amount of money that hospital received from the government. (Pls.’ Resp. at 19.) Based on this information, and what they describe as “[s]imilar details . . . repeated throughout [the complaint] and Exhibit B for scores of additional false claims,” the Relators maintain they have “provide[d] more than sufficient detail in the [complaint] for Defendants to be put on notice as to who, what, when, where, and how they caused a false claim to be submitted to the Government.” (*Id.*) The Court disagrees.

To begin with, the Relators’ complaint is particularly lacking with respect to the “who” part of the fraud equation. The Relators say they have “alleged the identities of individual [Company and Hospital] participants in the fraud” and then they list twenty paragraphs in the complaint in support. (*Id.* at 28.) These

paragraphs indeed reveal the names of a number of employees, although mostly from the Managing Company.¹² The Relators describe various roles the named Managing Company employees performed: some were responsible for the implementation and monitoring of the electronic-health-record software (Am. Compl. at ¶¶ 86, 89); some participated in various meetings and calls about defects in the software (*id.* at ¶¶ 87, 91); some circulated memos and advisories about software problems (*id.* at ¶¶ 88, 92); some noted or recognized issues with the software (*id.* at ¶¶ 137, 199, 228, 245, 259, 280); some were told about software issues or were tasked with resolving or logging them (*id.* at ¶¶ 190, 199, 215); some came up with “workarounds” for the identified software issues (*id.* at ¶ 233); some visited one of the HMA hospitals that complained about the software functionality (*id.* at ¶ 276); one was aware of a \$25 million equity exchange for software adoption that Medhost offered the Companies and Hospitals (*id.* at ¶ 286); one was aware of discounts Medhost offered the Companies and Hospitals for future business (*id.* at ¶ 287); some believed the Companies and Hospitals could have implemented a superior software product for the same or lower price (*id.* at ¶¶ 287, 288); and, finally, one was frequently taken golfing by a Medhost employee where Medhost software purchases were negotiated (*id.* at ¶ 288). In contrast, the Relators, in the cited paragraphs, identify only a handful of Hospital employees: some from the DeTar facility who complained about software issues (*id.* at ¶ 190); and some from Midwest Regional who reported issues with the PULSE software—one of whom “may have signed the attestation packet submitted to the government” (*id.* at ¶ 279).¹³ While the Relators acknowledge that most of the

¹² The Court assumes they are Managing Company employees, but the Relators don’t explicitly say so, instead merely labeling them “CHS” employees. It is ordinarily difficult to parse what the Relators mean when they refer simply to “CHS”; here, though, it appears when they refer to “CHS” employees, they mean Managing Company employees.

¹³ The Relators identify various other Hospital and Company employees throughout their complaint as well. But the Court mentions these employees, in particular, here, because these are the ones the Relators focus on to show they have properly alleged the “who” part of their fraud claims. The Court has, nonetheless, considered the references to all the other employees, as well, in considering the Hospitals and Managing Company’s motions to dismiss. (*E.g.*, Am. Compl. at ¶¶ 118 (named Managing Company employee who noted that a software interface was “junk”), 119 (named DeTar facility employee and various, unnamed physicians who complained about the software and a named Managing Company employee who explained the origin of a particular software problem), 158–59 (named DeTar facility employee who complained about a software problem with dosing), 188 (similar), 172 (named employee at Fallbrook Hospital who complained about software flaws), 178 (named Managing Company employee who knew about serious software problems), 184, 187–89, 196, 198, 200, 210, 212, 254, 259 (all similar), 262 (identifying HMA nurses and physicians, generally and by name, who complained about the software), 278, 279 (both similar).)

employees identified worked only for “corporate CHS,” they maintain their claims against the Hospitals are nonetheless sufficient as well. (Pls.’ Resp. at 28.) This is so, they insist, because “the Hospital Defendants . . . submitted the false claims and were merely ‘spokes’ of the ‘wheel’ of Medhost’s and CHS’s centralized fraud.” (*Id.* at 28 (citing *United States ex rel. Anita Silingo v. WellPoint, Inc.*, 904 F.3d 667, 677–78 (9th Cir. 2018))). Simply put, however, what the Relators have set forth, in their amended complaint and their opposition to the Defendants’ motions to dismiss, is not nearly enough to allege the “who” part of a fraud claim against any of the Hospitals—even the two that they specifically single out in their response—or the Managing Company—despite specifically identifying dozens of employees. What they fail to do is provide a nexus between all these employees, what they knew, and the fraud alleged.

In keeping with its purpose of providing “fair notice,” Rule 9(b) requires plaintiffs to distinguish between multiple defendants and “inform each defendant of the nature of his alleged participation in the fraud.” *Ambrosia Coal & Const. Co. v. Pages Morales*, 482 F.3d 1309, 1317 (11th Cir. 2007) (quoting *Brooks*, 116 F.3d at 1381). Thus, a complaint alleging fraud perpetrated by multiple defendants must differentiate among them, with allegations particular to each defendant, in order to survive dismissal. In other words, a complaint cannot “attribute[] fraudulent representations and conduct to multiple defendants generally, in a group pleading fashion.” *Streambend Properties II, LLC v. Ivy Tower Minneapolis, LLC*, 781 F.3d 1003, 1013 (8th Cir. 2015). In a case like this one, involving multiple defendants, “with different actors playing different parts, it is not enough to ‘lump’ together the dissimilar defendants and assert that ‘everyone did everything.’” *Silingo*, 904 F.3d at 677 (quoting *Destfino v. Reiswig*, 630 F.3d 952, 958 (9th Cir. 2011).)

Here, the vast majority of the Relators’ actual fraud allegations are directed towards either “Defendants” or to the Company and Hospital Defendants, collectively, without distinguishing among the over one-hundred Hospitals, the HMA hospitals, the Managing Company, or the Holding Company. Indeed, the Relators fail to identify any employee at any Hospital or Company who knew a particular Hospital’s attestation was false. No specifically named Hospital employee (of which there are very few) or Company employee is alleged to have hidden or manipulated any concerns or knowledge of relevant software defects. And the amended complaint fails to set forth any allegation that any particular employee knew or should have known, in relation to the

software issues they were aware of, that any particular attestation was actually false.

Instead, the complaint is replete with broad allegations against, lumped together, the Companies and the Hospitals. For example, the Relators allege “CHS [(the Companies and Hospitals, combined)] deployed the combination of EDIS and Enterprise at numerous hospitals nationwide” and the poor integration of the two led the Companies and the Hospitals to “falsely attest[] to Meaningful Use knowing that EDIS and Enterprise did not meet the requirement of certified [electronic-health record] technology.” (Am. Compl. at ¶¶ 102–03.) Similar generalized references appear repeatedly throughout the complaint. (See, e.g., *id.* at ¶¶ 70 (alleging the Company and Hospital attestations, collectively, “were false”); 95, 103, 220, 225–27 (all similar); 124–26 (alleging the Enterprise system had issues related to “the frequent use of unstructured medication entries at CHS hospitals”); 136 (alleging that Company and Hospital “facilities,” collectively, noticed software problems and that the Companies and Hospitals, collectively, notified Medhost of the issues), 139–41, 156, 168 (all similar); 137 (alleging the Companies and Hospitals, collectively, improperly “implemented a workaround” for a software issue), 156, 163, 184, 224, 233 (all similar); 159 (alleging the Companies and Hospitals, collectively, “continued to attest” to the software despite its problems); 170 (similar); 162 (alleging the Companies, Hospitals, *and* Medhost, collectively, all “became aware” of software malfunctions); 102, 117, 197 (similar); 190 (alleging that the Companies, Hospitals, *and* Medhost, collectively, all “knew that the inadequate [software] functions at CHS hospitals were creating patient safety issues”); 234 (alleging the Company and Hospital “order sets did not meet the objectives or measures” for attestation); 272 (alleging the Companies and Hospitals “knew that [electronic-health record] technology at the HMA hospitals was seriously flawed”). In the complaint’s final paragraphs, the Relators set forth all four claims under the FCA, under one amalgamated claim, incorporating all 296 paragraphs that preceded it. (*Id.* at ¶¶ 297–306.) The Relators then repeatedly refer to the “Defendants,” altogether, alleging that all of them, collectively, violated four provision of the FCA.¹⁴

The closest the Relators come to making particularized allegations against the Hospitals is to reference exhibit B of the amended complaint. (Am.

¹⁴ To be sure, even if the Court were to conclude that the Relators had managed to state a claim and had satisfied the particularity requirements of Rule 9(b), it would nonetheless require the Relators to replead because their complaint, for all the reasons the Defendants point out, is, as these final paragraphs highlight, a textbook shotgun pleading in many respects.

Compl, Ex. B, ECF No. 123-2). But this chart, even in combination with the 100-page complaint, does not satisfy Rule 9(b)'s high pleading standard. Even though the chart identifies every single Hospital and lists all the attestations, generally, that each made, the thirty-nine-page chart nonetheless still fails to identify who, in particular, made the false submissions, what, in particular, was false about them, or who knew or even should have known about the particular falsities of those statements.

Simply identifying broad categories of features that were attested to and then summarily claiming that each broad category was falsely attested to, based on series of defects that a handful of disconnected employees, during disjointed time periods were aware of and complained about, does not put any particular Defendant on notice of what it did wrong and why it is accused of fraud. It does not suffice for the Relators to "lump together the dissimilar defendants and assert that everyone did everything." *Silingo*, 904 F.3d at 677 (cleaned up). What, specifically, rendered each one of the hundreds of attestations listed in exhibit B false? Which particular aspect of the broad criteria identified did each Hospital fail to meet? Why did each Hospital fail to meet those criteria? Who at the Managing Company and each Hospital was aware, or should have been aware, that the criteria were not met? When was a particular software problem recognized in relation to when a particular attestation was made? The Relators list a number of software failures that many employees were aware of, at various times and in various places; they also identify extensive lists of technical criteria that must be met for various attestations; they then catalog hundreds of general attestations that were submitted to the government, also at various times, both before, during, and after the software problems were recognized. But what is the actual link, the factual nexus, between this hodgepodge of facts, these isolated incidents, these generalized conclusions, and the Relators' summary allegations of actual fraud against the Defendants? The Relators never say and this is fatal to the viability of all their fraud claims.¹⁵ Their complaint is due for dismissal because it fails to state a claim based on anything other than conclusory allegations and fails to allege its FCA claims with the particularity required by Rule 9(b).

¹⁵ Because the Relators' substantive claims fail, their allegations of a conspiracy, based on those underlying substantive claims, also fail. The Relators have not set forth any non-conclusory allegations that would establish an agreement to violate the FCA. In the only allegation in the complaint that references any sort of agreement, the Relators merely allege, "Defendants knowingly conspired with others to violate the FCA [and] took substantial steps toward the completion of the goals of that conspiracy." (Am. Compl. at ¶ 302.) This falls woefully short of alleging facts supporting a conspiracy.

C. The Holding Company

The analysis set forth above, regarding the Hospitals and Managing Company, is no less applicable in the context of the fraud allegations against the Holding Company as well. The fraud claims against the Holding Company, however, are due to be dismissed for the additional reason that it cannot be held liable merely by virtue of its status as an owner, direct or indirect, of the Managing Company and the Hospitals.

In opposition, the Relators maintain, puzzlingly, that inquiry into the “relative” culpability of the Holding Company “is simply not appropriate at the motion to dismiss stage.” (Pls.’ Resp. at 14.) Regardless, what is appropriate, is for the Court to determine whether the Relators have alleged facts sufficient to state a claim against the Holding Company and whether, in so doing, they have complied with the particularity requirements of Rule 9(b).¹⁶ They have done neither.

To begin with, the acts of one corporation cannot generally be imputed to another, even in the parent-subsidary context. *See United States v. Bestfoods*, 524 U.S. 51, 61 (1998) (“It is a general principle of corporate law . . . that a parent corporation . . . is not liable for the acts of its subsidiaries.”). Indeed, “merely being a parent corporation of a subsidiary that commits a FCA violation, without some degree of participation by the parent in the claims process, is not enough to support a claim against the parent for the subsidiary’s FCA violation.” *U.S. ex rel. Hockett v. Columbia/HCA Healthcare Corp.*, 498 F. Supp. 2d 25, 59–60 (D.D.C. 2007) (cleaned up). And, certainly, “the bare assertion that [a corporate defendant] ‘operated, directed, and conspired’ with the hospital does not satisfy Rule 9’s particularity standard.” *United States ex rel. Martinez v. KPC Healthcare Inc.*, 815CV01521JLSDFM, 2017 WL 10439030, at *6 (C.D. Cal. June 8, 2017). Here, the Relators do not allege any facts that show the Holding Company actually participated in the alleged fraud.

Thus, in order to implicate the Holding Company, the Relators would have to allege the Managing Company or the Hospitals were the Holding

¹⁶ The Relators say, “Rule 9(b) does not apply to the scenario where the parent company and its subsidiaries all participated in a fraud.” (Pls.’ Resp. at 23.) In support, they direct the Court’s attention to *U.S. ex rel. White v. Gentiva Health Services, Inc.*, 3:10-CV-394-PLR-CCS, 2014 WL 2893223, at *16 (E.D. Tenn. June 25, 2014). The Relators’ position and supporting citation are concerning. Nothing in that opinion stands for the proposition stated. In fact, the opinion explicitly states the opposite, dismissing a number of that relator’s claims because, pointedly, certain of her allegations could not “survive Rule 9(b)’s more stringent pleading requirements” and she had “fail[ed] to allege [a certain] scheme with the specificity required by Rule 9(b).” *Id.* at *15.

Company's mere instrumentalities. To do so, absent actual participation, a "relator must be able to demonstrate either that the defendant is liable under a veil piercing or alter ego theory." *U.S. ex rel. Holbrook v. Brink's Co.*, 2:13-CV-873, 2015 WL 196424, at *25 (S.D. Ohio Jan. 15, 2015) (cleaned up). The burden for establishing this is quite high and such findings are considered "rare." *Runton v. Brookdale Senior Living, Inc.*, 17-60664-CIV, 2018 WL 1057436, at *7 (S.D. Fla. Feb. 2, 2018) (Altonaga, J.). Not only must a party seeking to pierce the corporate veil prove that the subsidiary was a "mere instrumentality" of the parent, but the party must also show "that the parent engaged in improper conduct through its organization or use of the subsidiary." *Id.* (quoting *Johnson Enters. of Jacksonville, Inc. v. FPL Grp., Inc.*, 162 F.3d 1290, 1320 (11th Cir. 1998) (cleaned up)). Here, the Relators have alleged none of this and so, for this additional reason, their claims against the Holding Company must be dismissed.

4. False Claims Act Claims Based on the Anti-Kickback Statute

The Relators also allege a separate theory under the federal Anti-Kickback Statute, 42 U.S.C. § 1320a-7b(b)(2). Claims for government payment that result from AKS violations are actionable under the FCA. The Relators claim the Defendants violated the AKS (1) "[b]y arranging for Medhost to provide [the Companies and Hospitals] with valuable financial software for free in return for [the Companies and Hospital's] purchase of full licenses of Medhost's [electronic-health record] software suite" (Am. Compl. at ¶ 295); (2) based on the Company and Hospital CFO's insistence on completing a \$25 million equity exchange that Medhost offered the Companies and the Hospitals related to the purchasing of certain software (*id.* at ¶ 286); (3) the Company and Hospital's decision to choose Medhost's software over higher quality products that were of similar cost (*id.* at ¶ 288); and (4) by having a Medhost Senior Vice President take a Company and Hospital CFO golfing where the software purchase was negotiated (*id.*). The Defendants universally maintain any FCA claim based on the alleged violations of the AKS must be dismissed for a failure to state a claim and a failure to comply with Rule 9(b)'s particularity requirements. After careful review, the Court agrees.

As relevant here, the AKS prohibits knowingly and willfully paying remuneration with the intent to induce the ordering of items or services reimbursable under any federal health care program. 42 U.S.C. § 1320a-7b(b)(2). In turn, claims for government payment that result from AKS violations are actionable under the FCA. And since they are brought under the

FCA, such claims must also be pleaded with particularity under Rule 9(b).! *United States ex rel. Childress v. Ocala Heart Inst., Inc.*, 5:13-CV-470-OC-22PRL, 2015 WL 13793109, at *4 (M.D. Fla. July 2, 2015). Accordingly, the Relators must allege, with particularity, the Defendants knowingly and willfully offered or paid remuneration “in cash or in kind to any person to induce such person . . . to purchase, lease, order, or arrange for or recommend purchasing, leasing, or ordering any good, facility, service, or item for which payment may be made in whole or in part under a [f]ederal health care program.” 42 U.S.C.A. § 1320a-7b(b)(2).

The AKS, in another statutory section, broadly defines “remuneration” as “transfers of items or services for free or for other than fair market value.” 42 U.S.C. § 1320a-7a(i)(6). Although the Relators say Medhost provided its financial software for “free,” they describe this transaction as merely part of the Company and Hospital’s decision to purchase licenses for Medhost’s electronic-health record software suite. And nowhere do the Relators allege that doing so rendered the entire exchange to be below fair market value. Accordingly, since there is no allegation that Medhost’s provision of the combination of its electronic-health-record software and its financial software were for below fair-market value, there can be no violation of the AKS.

Furthermore, conceptually, the Relators’ allegations do not fit within the AKS. Medhost offered its software product for sale to the Companies and the Hospitals in what appears to be a competitive market. (*See, e.g.*, Am. Compl. at ¶ 288.) It would therefore be expected that the Companies and the Hospitals would seek to optimize the quality of the product while minimizing costs and that Medhost would seek to maximize its profits in convincing the Companies and the Hospitals to choose its software. That Medhost offered its financial software for free as an enticement to the very entities it was negotiating with,¹⁷ does not run afoul of the AKS. If Medhost had, for example, offered free individual tax software to the heads of all the Hospitals and the executives of the Companies, personally, in order to get them to arrange for the Companies and the Hospitals to purchase the electronic-health-record software, then the Relators might have a claim—or at least a framework for one. But, as presented, they have merely described business entities—Medhost and the monolith of “CHS”—negotiating an arms-length transaction for the bona fide sale and purchase of software. The Relators present no allegations that any

¹⁷ The Relators say, for example, that Medhost “provide[d] CHS with free financial software for the purpose of inducing CHS to purchase full licenses of its . . . software suite” (Am. Compl. at ¶ 281 (emphasis added)) and “offered discounts to CHS for its software and maintenance to induce CHS to continue to purchase its software” (*id.* at ¶ 287 (emphasis added).)

remuneration took place outside of the transaction itself. No one was offered or paid any separate remuneration to induce them to purchase or recommend the purchase of software from Medhost. Further, practically speaking, the kickback scheme the Relators allege is internally inconsistent: on the one hand they allege Medhost's offer of a discount on its products amounted to a kickback; on the other, they allege the Companies and the Hospitals overpaid for the software, in light of its subpar quality. From this, no improper remuneration can be discerned.

The Relators also fail to explain how the Company and Hospital CFO's proclaimed insistence that the companies effectuate the software conversion "in order for [the Companies and the Hospitals] to obtain \$25 million in equity in Medhost" violates the AKS. (*Id.* at ¶ 286.) Again, the Relators have not alleged anything that was provided at below fair-market value and have not alleged that any such remuneration was offered outside the entities who were engaged in negotiating a business transaction. Without allegations of actual remuneration being offered or paid to someone to induce the software purchase, the Relators have not set forth an AKS violation.

Likewise, the Relators' allegation that some employees would have preferred what they viewed as a better product for the same cost also falls far wide of the mark. (*Id.* at ¶ 288.) That the Companies and the Hospitals could have purchased a better product for the same price does not even come close to alleging any remuneration changed hands with, or was offered to, outside parties to induce the software purchase. It just means some employees thought the Companies and the Hospitals overpaid for a subpar product. This alleges, at most, business judgment disagreement, and does not in any appreciable way support a claim that the Defendants violated the AKS.

Finally, the Relators' allegation that a Medhost executive "frequently took [the Company and Hospital] Chief Financial Officer . . . to play golf where . . . software purchases for [the Company and Hospitals] were negotiated" also falls well short of alleging a kickback. (*Id.*) When and where did the golf outings take place? Did the Medhost executive even pay for the outings? If so, how much? How was the golf outing used to induce the Company and Hospitals' purchase of the software? None of these essential elements is even referenced, never mind specifically alleged.

Not only have the realtors failed to set forth a framework remotely resembling any kind of kickback scheme, they have also failed to set forth the particularity required under Rule 9(b). To allege a kickback scheme, the Relators must make particularized allegations that include, "the names of the

people who received the incentives, the names of the defendants' employees who negotiated the incentives, precisely what the incentives were, when they were provided, why they were provided, and why they were illegal." *United States v. Choudhry*, 262 F. Supp. 3d 1299, 1307 (M.D. Fla. 2017) (cleaned up). The Relators' allegations fall well short of these requirements. Their FCA claims based upon violations of the AKS cannot, therefore, proceed.

5. Conclusion


While the Relators have indeed poured forth heaps of alleged facts, interwoven with conclusory allegations of wrongdoing, the resulting complaint is nonetheless fatally flawed. This is because, even when construing the universe of facts presented in light most favorable to the Relators, the Court is unable to reasonably infer that the Defendants have engaged in the alleged misconduct. This failure is compounded by the Relators' failure to comply with Rule 9(b)'s particularity requirements. Accordingly, the Court **grants** the Defendants' motions to dismiss (**ECF Nos. 129, 132, 133, 134.**)

The Court dismisses the Relators' claim on the merits, without leave to amend and therefore the dismissal is **with prejudice**. Within their opposition to the Defendants' four motions to dismiss, the Relators, as an apparent afterthought, ask for leave to once again amend their complaint. (Pls.' Resp. at 28 ("If Relators discover more facts in discovery that further elaborate on CHS's corporate shell game, they can amend the pleadings to conform to the facts."), 31 n. 8 ("Relators will amend the complaint to plead these facts, if necessary."), 47 n. 15 ("If the Court grants any of the motions to dismiss, Relators respectfully request that the Court grant them leave to replead any pleading deficiency.")). The Relators' request for leave to amend their complaint lacks merit. They have failed to cite any legal authority or factual support that would justify amendment. The Relators reliance on *Vibe Micro, Inc. v. Shabanets*, 878 F.3d 1291, 1296 (11th Cir. 2018), is misplaced. In *Vibe Micro*, the Eleventh Circuit held that a district court must sua sponte give a plaintiff "one chance to replead before dismissing his case with prejudice on non-merits shotgun pleading grounds." *Id.* Although the complaint here is indeed a shotgun pleading, the Court was nonetheless able to determine that the Relators' claims are due to be dismissed on substantive grounds, as detailed in the analyses, above. Further, the Relators' motion is improperly presented. See *Newton v. Duke Energy Florida, LLC*, 895 F.3d 1270, 1277 (11th Cir. 2018) ("[W]here a request for leave to file an amended complaint simply is imbedded within an opposition memorandum, the issue has not been raised properly."); *Avena v.*

Imperial Salon & Spa, Inc., 740 Fed. App'x 679, 683 (11th Cir. 2018) (“[W]e’ve rejected the idea that a party can await a ruling on a motion to dismiss before filing a motion for leave to amend.”) (noting also that “a motion for leave to amend should either set forth the substance of the proposed amendment or attach a copy of the proposed amendment”) (quotations omitted). The Court denies the Relators’ request for leave to amend because the request lacks merit and is, additionally, procedurally defective.

This case is otherwise **stayed** with respect to the thirty Hospital Defendants identified in their suggestion of bankruptcy. (ECF No. 155.) The Court therefore directs the Clerk to **close** this case until the bankruptcies of those Defendants is concluded or the stay is otherwise lifted and the parties seek to reopen. Any pending motions are **denied as moot**.

Done and ordered in Miami, Florida on June 11, 2020.


Robert N. Scola, Jr.
United States District Judge