**IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF GEORGIA
MACON DIVISION**

UNITED STATES OF AMERICA, ex rel. ALEX PERMENTER, ERIC RODIGHIERO, and CHRIS WHEELER,	)	
Plaintiffs,	)	
v.	)	**CIVIL ACTION NO. 5:18-cv-382 (MTT)**
eCLINICALWORKS, LLC,	)	
Defendant.	)	

ORDER

In this action under the False Claims Act ("FCA"), 31 U.S.C. § 3729, Defendant eClinicalWorks moves to dismiss the relators' amended complaint on the grounds that the relators fail to state a claim. Doc. 69. The one count amended complaint alleges two theories, and each theory is based on discrete flaws in eClinicalWorks' software. Doc. 34. eClinicalWorks does not move to strike specific allegations of flaws; it moves to dismiss the amended complaint in its entirety. Thus, relators maintain that if any one flaw supports a plausible theory of recovery, eClinicalWorks' motion must be denied. For the reasons discussed below, eClinicalWorks' motion (Doc. 69) is **DENIED**.

I. BACKGROUND

A. eClinicalWorks and the Relators

eClinicalWorks is a healthcare technology company whose principal business is developing and licensing electronic healthcare records ("EHR") software to healthcare providers such as physician practices and hospitals. Doc. 34 ¶¶ 14, 16. According to

eClinicalWorks, more than 130,000 healthcare providers use their software, making eClinicalWorks an industry leader. *Id.* ¶¶ 17-18. In 2017, eClinicalWorks settled an FCA claim alleging that eClinicalWorks' EHR software had numerous functional defects, including failing to reliably document and track medications administered to patients, failing to record and track patients' laboratory results, and failing to prevent editing of patient notes. *Id.* ¶ 19 (citing *United States ex rel. Delaney v. eClinicalWorks, LLC*, No. 2:15-cv-95, Doc. 1 ¶¶ 63-107 (D. Vt. May 1, 2015)). As part of the settlement of that FCA case, eClinicalWorks entered a Corporate Integrity Agreement ("CIA") with the Office of Inspector General of the U.S. Department of Health & Human Services ("HHS-OIG"). *Id.* ¶ 20.

The CIA went into effect on May 30, 2017 and remained in place five years. Docs. 34 ¶ 20; 17-1 at 2. As part of its obligations under the CIA, eClinicalWorks was required to provide "timely access to … relevant software, media, and code" to an independent software quality oversight organization ("SQOO") approved by the HHS-OIG. Doc. 17-1 at 34. One of the SQOO's express obligations under the CIA was "to ensure that eClinicalWorks and its EHR software … comply with applicable ONC Health IT Certification Program requirements." *Id.* at 32. In return for satisfying its obligations under the CIA, the HHS-OIG agreed not to seek eClinicalWorks' exclusion from participation in Medicare, Medicaid, or other federal healthcare programs.[1] Doc. 34 ¶ 20.

Relators are computer and information technology ("IT") specialists who live and work in Macon, Georgia. *Id.* ¶¶ 9-11. Relators' company, Alex's PC Solutions, provides

[1] "Relators stipulate that they will not pursue relief arising from the allegation that eClinicalWorks has violated its CIA." Doc. 75 at 35. Nonetheless, the CIA's terms, conditions, and scope remain relevant.

IT, telecom, and web services to eighty-five businesses in the Middle Georgia area, including many healthcare practices. *Id.* ¶ 9. Relators service and support their healthcare clients' EHR software, some of which is provided by eClinicalWorks. *Id.* ¶ 47. Through this work, the relators gained "substantial knowledge" and "technical expertise" of eClinicalWorks' EHR software. *Id.* ¶¶ 9-11. According to the relators, eClinicalWorks' EHR software suffers from "grave security vulnerabilities" that "allow malicious actors to access the Protected Health Information ('PHI'), social security numbers, and other private information of tens of millions of federal healthcare beneficiaries and other Americans." *Id.* ¶ 2. These "grave security vulnerabilities"—which are distinct from the deficiencies raised in *Delaney*—are the bases of the relators *qui tam* action. *Id.* ¶¶ 2, 19.

B. Alleged Flaws and Vulnerabilities in eClinicalWorks' EHR Software

The relators' 78-page amended complaint alleges numerous flaws and vulnerabilities in eClinicalWorks' flagship EHR software. *See* Doc. 34.

According to the relators, eClinicalWorks' EHR software cannot verify that anyone—whether authorized or unauthorized—is who they claim to be. *Id.* ¶¶ 56-86, 89-90, 95-102, 105-106. The relators claim eClinicalWorks' servers "include thousands of .jsp files," most of which are accessible through a web browser without logging into the system. *Id.* ¶ 56. As a result, a user, without administrator access, a login, or a password, can browse the website of a particular healthcare provider's eClinicalWorks server, execute a .jsp command, and obtain the usernames of the healthcare provider's administrators and the security parameters that govern administrators' passwords. *Id.* With that information, the relators contend "any motivated bad actor could easily and

quickly determine the actual passwords of individual practice administrators," which in turn would allow complete access to the provider's EHR and underlying PHI. *Id.* ¶ 57.

Another alleged flaw is eClinicalWorks' use of a "bogus CAPTCHA feature," which, according to the relators, is functionally useless and does "nothing to stop a bot from manipulating passwords and gaining access to the system." *Id.* ¶¶ 59-61. Similarly, the relators allege eClinicalWorks' software uses a cracked password algorithm, MD5, which is "generally recognized to be a weak hashing algorithm" that is below "standard industry security practices." *Id.* ¶¶ 62-68. By exploiting the MD5 algorithm, the relators "were able to determine the plain text passwords associated with 50% of the users' password hashes within 20 seconds." *Id.* ¶ 68.

The relators also allege eClinicalWorks' software is vulnerable to Structural Query Language ("SQL") injection attacks, which the relators note have led to some of the largest data breaches in history. *Id.* ¶¶ 69-71. Specifically, the relators contend eClinicalWorks' servers are vulnerable to this "widely known" type of attack because their servers "are misconfigured so that this extra language will execute a command on the web server rather than return a webpage." *Id.* ¶¶ 73-74 (internal quotation marks and citation omitted). After the relators' initial complaint was filed, eClinicalWorks released a security patch which purported to address the SQL injection attack vulnerability, but the relators allege that eClinicalWorks "used an extremely convoluted computer code to create the mere illusion" that the vulnerability had been remedied. *Id.* ¶ 85.

Further, the relators contend eClinicalWorks' EHR software "stores PHI—such as diagnostic tools used in connection with specific patients— 'locally,' meaning on the

physical computer on which the PHI is created." *Id.* ¶ 104. Because the locally stored PHI is not encrypted, the relators allege any person "with access to one of these computers could access the files containing locally stored PHI regardless of whether that person was logged into eClinicalWorks' EHR software." *Id.*

C. Relators' Theories of False Certification

The United States Department of Health and Human Services Office of the National Coordinator for Health Information Technology ("ONC") "administers the [government's EHR] certification program and creates certification requirements for EHR vendors." *Id.* ¶ 116. Under the certification program, eClinicalWorks, as an EHR vendor, "is required to certify to agents of the federal government, called 'authorized certification bodies' and 'accredited testing laboratories,' that the vendor's EHR technology satisfies ONC's certification requirements." *Id.* According to eClinicalWorks' website, "eClinicalWorks V11 is a 2015 Edition ONC Certified Health IT Product." *Id.* ¶ 119.

Relators allege that because of the flaws in eClinicalWorks' EHR software, eClinicalWorks necessarily made false representations to the government to obtain certification from the ONC. *Id.* ¶¶ 118-120. In turn, the relators contend eClinicalWorks caused healthcare providers to falsely certify that their EHR software complied with federal regulations, which allowed healthcare providers to obtain incentive payments or downward payment adjustments under various federal programs for which they would otherwise be ineligible. *Id.* ¶¶ 115-151. As a separate theory of FCA liability, the relators allege the security flaws in eClinicalWorks' EHR software make it impossible for

healthcare providers using the software to truthfully certify compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). *Id.* ¶¶ 107-114.

1. eClinicalWorks' EHR Software Allegedly Causes Healthcare Providers to Falsely Certify Compliance with Meaningful Use, MIPS, and PRQS Programs

Both the government's Meaningful Use Incentive Program and the Merit-Based Incentive Payment System ("MIPS") that replaced it offered hospitals and physicians financial incentives to implement modern EHR systems in their practices. *Id.* ¶¶ 130-131, 135-136. "The Medicare Meaningful Use program provided … incentive payments of as much as $43,720 [to] healthcare provider[s] who established meaningful use of certified EHR technology." *Id.* at ¶ 131. Similarly, Medicaid's Meaningful Use program offered incentive payments of up to $63,750 to healthcare providers. *Id.*

Although Medicare meaningful use payments ended in 2016 and Medicaid meaningful use payments ended in 2021, the MIPS program that followed offered similar financial incentives for the use of certified EHR technology. *Id.* ¶¶ 131, 135, 136. "Healthcare providers who participate in MIPS receive 'positive payment adjustments' while non-exempted healthcare providers who do not participate in MIPS or do not satisfy governing MIPS criteria receive 'negative payment adjustments.'" *Id.* ¶ 137. The payment adjustments, which took effect in January 2019, range from negative four percent to positive four percent. *Id.* Under MIPS, positive and negative adjustments are governed by various "performance categories." *Id.* ¶ 138. Relevant here, the "promoting interoperability" category requires the use of certified EHR technology, and accounts for twenty-five percent of a provider's final MIPS score. *Id.* ¶ 139.

To receive incentive payments under MIPS or the Meaningful Use Incentive Program that preceded it, the healthcare provider had to annually attest "to the federal

government that the healthcare provider used certified EHR technology and met [other] specified Meaningful Use objectives and measures." *Id.* ¶¶ 132, 141. Healthcare providers relied on the representations of the vendor, in this case eClinicalWorks, to know whether the EHR technology was certified. *Id.* ¶¶ 133, 142. For both programs, the receipt of federal incentive payments was contingent upon the use of certified EHR software. *Id.* ¶¶ 132, 141.

The Relators also contend payments under the Medicare Physician Quality Reporting System ("PQRS") were contingent upon the use of certified EHR software. *Id.* ¶ 149. Initiated in 2006, the PQRS applies a downward payment adjustment to healthcare providers who do not satisfactorily report data on quality measures for covered Medicare Physician Fee Schedule ("MPFS") services furnished to Medicare Part B Fee-for-Service ("FFS") beneficiaries. *Id.* ¶¶ 147-148. To avoid negative payment adjustments under the PQRS, participating healthcare providers had to certify their EHR software of choice was ONC compliant. *Id.* ¶¶ 149-150.

2. eClinicalWorks Causes Healthcare Providers to Falsely Certify HIPAA Compliance

The relators' second theory of false certification alleges the use of eClinicalWorks' flawed EHR software causes healthcare providers to both expressly and impliedly violate HIPAA. *Id.* ¶¶ 107-114. For their express certification theory, the relators point to the Electronic Data Interchange ("EDI") Enrollment Agreement, which healthcare providers must execute before they are permitted to submit claims electronically for government payment. *Id.* ¶ 108. That EDI agreement, in relevant part, "requires the healthcare provider to expressly certify [to the Centers for Medicare & Medicaid Services ("CMS")] that the healthcare provider 'will use sufficient security

procedures … to ensure that all [electronically transmitted documents] are authorized and protect all beneficiary-specific data from improper access.'" Docs. 34 ¶ 109 (quoting 17-3 at 15). In addition to the express certification made through the EDI agreement, the relators allege eClinicalWorks' EHR software also causes healthcare providers to "impliedly certify their compliance with the HIPAA security regulations when they submit a claim for payment to CMS or one of CMS's contractors." *Id.* ¶ 110. Because HIPAA security regulations require healthcare providers to "[e]nsure the confidentiality, integrity and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits," and "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity" of electronic PHI, the relators allege no healthcare provider could possibly comply with these HIPAA regulatory requirements when using eClinicalWorks' EHR software. *Id.* ¶ 111 (citing 45 C.F.R. § 164.306(a)(1)-(2)).

D. Procedural Summary

Relators filed this FCA action on October 16, 2018. Doc. 3. On July 12, 2019, relators filed their amended complaint. Doc. 17. The Court granted the United States several extensions to decide whether it would intervene. Docs. 11; 16; 20; 23; 26; 29. Three years later, the United States ultimately declined to do so on October 18, 2021. Doc. 32. After the government declined to intervene, eClinicalWorks moved to transfer to the District of Massachusetts, which the Court denied.[2] Docs. 49; 64. eClinicalWorks

[2] In the Court's order denying eClinicalWorks' motion to transfer, the Court stated the relators filed their amended complaint on October 20, 2021. Doc. 64 at 2. That was incorrect. The relators' amended complaint was filed on July 12, 2019, and the *redacted* amended complaint was filed on October 20, 2021 after the government declined to intervene and the case was unsealed. Docs. 17; 34. In any event, the specific date the relators filed their amended complaint was immaterial to the Court's analysis in that order. *See* Doc. 64.

then moved to dismiss, and at the request of the parties, oral arguments were held. Docs. 69; 82; 83; 84.

II. STANDARD

The Federal Rules of Civil Procedure require that a pleading contain "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). To avoid dismissal pursuant to Rule12(b)(6), a complaint must contain sufficient factual matter to "state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A claim is facially plausible when "the court [can] draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id*. "Factual allegations that are merely consistent with a defendant's liability fall short of being facially plausible." *Chaparro v. Carnival Corp.*, 693 F.3d 1333, 1337 (11th Cir. 2012) (internal quotation marks and citations omitted).

At the motion to dismiss stage, "all well-pleaded facts are accepted as true, and the reasonable inferences therefrom are construed in the light most favorable to the plaintiff." *FindWhat Inv. Grp. v. FindWhat.com.*, 658 F.3d 1282, 1296 (11th Cir. 2011) (internal quotation marks and citations omitted). But "conclusory allegations, unwarranted deductions of facts or legal conclusions masquerading as facts will not prevent dismissal." *Wiersum v. U.S. Bank, N.A.,* 785 F.3d 483, 485 (11th Cir. 2015) (cleaned up). The complaint must "give the defendant fair notice of what the ... claim is and the grounds upon which it rests." *Twombly*, 550 U.S. at 555 (internal quotation marks and citation omitted). Where there are dispositive issues of law, a court may

dismiss a claim regardless of the alleged facts. *Patel v. Specialized Loan Servicing, LLC*, 904 F.3d 1314, 1321 (11th Cir. 2018) (citations omitted).

"The FCA is designed to protect the Government from fraud by imposing civil liability and penalties upon those who seek federal funds under false pretenses." *United States ex rel. Lesinski v. S. Fla. Water Mgmt. Dist.*, 739 F.3d 598, 600 (11th Cir. 2014). "As an enforcement mechanism, the FCA includes a *qui tam* provision under which private individuals, known as relators, can sue 'in the name of the [United States] Government' to recover money obtained in violation of § 3729." *United States ex rel. Bibby v. Mortg. Invs. Corp.,* 987 F.3d 1340, 1343 (11th Cir. 2021), *cert. denied*, 141 S. Ct. 2632 (2021). "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).

Rule 9(b) requires that the relator "must state with particularity the circumstances constituting fraud" but may generally allege scienter. To meet Rule 9(b)'s particularity requirements, a relator "must plead facts as to time, place, and substance of the defendant's alleged fraud, specifically the details of the defendants allegedly fraudulent acts, when they occurred, and who engaged in them." *U.S. ex rel. Clausen v. Lab'y Corp. of Am., Inc.*, 290 F.3d 1301, 1310 (11th Cir. 2002) (cleaned up). "Liability under the False Claims Act arises from the submission of a fraudulent claim to the government, not the disregard of government regulations or failure to maintain proper internal policies." *Corsello v. Lincare, Inc.*, 428 F.3d 1008, 1012 (11th Cir. 2005). "Indeed, the 'central question' regarding whether a relator's allegations state a claim under [§ 3729(a)(1)] is, did the defendant present (or caused to be presented) to the

government a false or fraudulent claim for payment?" *Urquilla-Diaz*, 780 F.3d at 1052 (quoting *Hopper v. Solvay Pharms., Inc.*, 588 F.3d 1318, 1326 (11th Cir. 2009)).

III. DISCUSSION

Relators have asserted only one count encompassing all their allegations. Doc. 34 ¶¶ 161-167. Where, as here, the relators' FCA claim advances a "false certification theory," the relators must allege: "(1) a false statement or fraudulent course of conduct, (2) made with scienter, (3) that was material, causing (4) the government to pay out money or forfeit moneys due." *Bibby,* 987 F.3d at 1346 (quoting *Urquilla-Diaz*, 780 F.3d at 1045).[3]

A. Relators Have Plausibly Pled False Representations

"The *sine qua non* of a False Claims Act violation is the submission of a false claim to the government." *Urquilla-Diaz*, 780 F.3d at 1045 (cleaned up). Here, eClinicalWorks contends relators have not plausibly alleged that eClinicalWorks caused the submission of any false claims because the relators' EHR certification and HIPAA compliance theories both fail. Doc. 69-1 at 22-23.

1. The Relators' EHR Certification Theory is Plausibly Pled

Although relators allege numerous flaws in eClinicalWorks' EHR software, eClinicalWorks focuses on four categories of flaws to support its motion to dismiss. Docs. 34; 69-1. Specifically, eClinicalWorks argues relators' EHR certification theory fails because (1) relators fail to adequately allege any violation related to user verification and access control requirements; (2) relators fail to adequately allege any

[3] The Eleventh Circuit in *Urquilla-Diaz* examined the 2006 version of the FCA that numbered sub-sections of § 3729 claims differently than the current version. *See* 780 F.3d at 1045 (quoting 2006 version). What was then § 3729(a)(1) is the equivalent to now § 3729(a)(1)(A), and what was § 3729(a)(2) is now § 3729(a)(1)(B). *Compare Urquilla-Diaz*, 780 F.3d at 1045, *with* §§ 3729(a)(1)(A)-(B).

violation concerning audit logs; (3) relators fail to adequately allege any violation concerning password hashing; and (4) relators fail to adequately allege any violation concerning local storage of PHI. Doc. 69-1 at 23-31.

User Verification and Access Control Requirements. Relators contend "[t]he security flaws in eClinicalWorks' software make it impossible for eClinicalWorks to verify that the person seeking access to electronic health information is the one claimed" in violation of 45 C.F.R. § 170.314(d)(1)(i). Doc. 34. ¶ 121. The ONC's access control requirement, as it stood in 2014, required EHR software to "[v]erify against a unique identifier(s) (e.g., username or number) that a *person* seeking access to electronic health information is the one claimed." 45 C.F.R. § 170.314(d)(1)(i) (emphasis added). In 2015, the word "person" was changed to "user," but no other changes were made. 45 C.F.R. § 170.315(d)(1)(i). eClinicalWorks contends this change was significant because it shows that the ONC's access control requirement only applies to *authorized* users, not malicious actors. Doc. 69-1 at 24-25. eClinicalWorks claims the qualification *authorized* is appropriate because "Title 45" defines "user" as "a person or entity with *authorized* access." *Id.* at 24 (citing 45 C.F.R. § 164.304). The relators counter that the definition of "user" in 45 C.F.R. § 164.304 is irrelevant because that definition expressly applies only when the word "is used in this subpart," which is not the subpart in which 2014 or 2015 EHR certification criteria appear.[4] Doc. 75 at 16 (quoting 45 C.F.R. § 164.304).

[4] The definition of "user" cited by eClinicalWorks, 45 C.F.R. § 164.304, is in Title 45, Subtitle A, Subchapter C, Part 164, Subpart C. The 2014 certification criteria, 45 C.F.R. § 170.314, is in Title 45, Subtitle A, Subchapter D, Part 170, Subpart C. The 2015 certification criteria, 45 C.F.R. § 170.315, is in Title 45, Subtitle A, Subchapter D, Part 170, Subpart C.

"Statutory interpretation must begin with the language of the statute, which must be interpreted in accordance with its plain meaning." *Blue Cross & Blue Shield of Ala. v. Weitz*, 913 F.2d 1544, 1548 (11th Cir. 1990) (cleaned up). Departure from a statute's official text is only warranted "if the language is unclear or if apparent clarity leads to absurd results when applied." *Id.* First, nothing about 45 C.F.R. § 170.315(d)(1)(i) is unclear—the regulation says user not authorized user. Had the ONC meant authorized user they would have said so; and they didn't just forget—the ONC specifically modified that section in 2015 but *only* changed "person" to "user." The ONC did not add "authorized," and it did not incorporate the definition of user found in 45 C.F.R. § 164.304. It is not appropriate for the Court to copy a definition of user from a part of the CFR in which it belongs and paste it into a part where it does not.

Moreover, eClinicalWorks' interpretation of the ONC's user verification and access control requirements leads to absurd results. The relators allege numerous ways bad actors can bypass the controls that are supposed to stop access. Doc. 34 ¶¶ 56-86, 89-90, 95-102, 105-106. Under eClinicalWorks' interpretation of the ONC's regulatory requirements, that is perfectly fine because the software keeps authorized users out. To read the ONC's regulatory requirements in such a manner renders them meaningless. *See Weitz*, 913 F.2d at 1548.

The relators plausibly allege eClinicalWorks fails to comply with ONC's user verification and access control requirements set forth in 45 C.F.R. § 170.314(d)(1)(i), and as later codified in 45 C.F.R. § 170.315(d)(1)(i).

Audit Log Requirements. Relators allege malicious actors can "bypass the eClinicalWorks application altogether," which would result in "eClinicalWorks' audit logs

completely fail[ing] to record any of the malicious actor's downloads, uploads, or alterations of patient records," or any tampering with "the audit logs themselves" in violation of 45 C.F.R. § 170.314(d)(2)(i)(A)-(B). Doc. 34 ¶ 122. Here again, eClinicalWorks contends the ONC's certification criteria only requires EHR software to log actions taken by authorized users. Doc. 69-1 at 25-28. Under the ONC's 2014 certification criteria, EHR software must "[r]ecord actions related to electronic health information in accordance with the standard specified in [45 C.F.R.] § 170.210(e)(1) [and] [r]ecord the audit log status (enabled or disabled) in accordance with the standard specified in [45 C.F.R.] § 170.210(e)(2)." 45 C.F.R. § 170.314(d)(2)(i)(A)-(B). Sections 170.210(e)(1) and (2), in turn, both establish the ASTM as the standard for EHR audit logging capabilities. *See* 45 C.F.R. §170.210(e)(1)-(2), (h) (adopting ASTM §§ 7.2-7.4, 7.6-7.7). Relevant here, ASTM § 7.4 requires EHR software to record the "[u]nique identification of the user of the health information system" for all actions taken. Doc. 69-6 § 7.4.

Here though, eClinicalWorks finds some traction for its argument because the ASTM *does* provide an applicable definition of user. Specifically, the ASTM defines "user" as "a person *authorized* to use the information contained in an information system as specified by their job function." Doc. 69-6 § 3.1.15 (emphasis added). Clearly, malicious actors fall outside of that definition. But the suspect plausibility of that one allegation does not warrant dismissal of the relators' entire amended complaint.

Password Hashing and Encryption Requirements. Relators allege that eClinicalWorks violated 45 C.F.R. § 170.314(e)(1)(i) because the passwords stored on eClinicalWorks' servers were not encrypted with a sufficiently complex algorithm. Doc.

34 ¶¶ 123-127. As a starting point, the 2014 version of that code section states "EHR technology must provide patients (and their authorized representatives) with an online means to view, download, and transmit to a 3rd party [certain specified PHI]. Access to these capabilities must be through a secure channel that ensures all content is encrypted and integrity-protected in accordance with the standard for encryption and hashing algorithms specified at § 170.210(f)." 45 C.F.R. § 170.314(e)(1)(i). The 2014 version of § 170.210(f), titled "[e]ncryption and hashing of electronic health information," provides the specified encryption and hashing algorithms as "[a]ny encryption and hashing algorithm identified by the National Institute of Standards and Technology (NIST)[.]" 45 C.F.R. § 170.210(f).

eClinicalWorks doesn't argue that its MD5 password hashing algorithm meets NIST standards. *See* Doc. 69-1 at 28-30. Rather, citing the above regulations and ONC's comments during the rule making process, eClinicalWorks argues that the regulations the relators claim were violated only require EHR software to encrypt PHI—not the passwords that protect that information—using one of the specified hashing algorithms in 45 C.F.R. § 170.210. Doc. 69-1 at 28-29 (citing 77 Fed. Reg. at 54181). Specifically, eClinicalWorks points to the ONC's comment that it would not "prescribe a particular form or 'level of assurance' for authentication" because "there is significant innovation taking place with respect to authentication," and "requiring a particular form in this certification criterion would be overly prescriptive." *Id.* at 29 (quoting 77 Fed. Reg. at 54181). But in the same paragraph the ONC also stated that it did not "disagree that some form of authentication will be necessary when EHR technology certified to this certification criterion is implemented" and that "EHR technology must be able to

establish a secure channel through which a patient can access the capabilities to view, download, and transmit their electronic health information." 77 Fed. Reg. at 54181.

At best, the regulations and ONC's comments during the rule making process are ambiguous. But if, as the relators allege, they exploited the MD5 algorithm and "were able to determine the plain text passwords associated with 50% of the users' password hashes within 20 seconds," and that "[a]s soon as a malicious actor obtained one such username and password, the malicious actor would be able to download or alter PHI with complete autonomy and without detection," it plausibly follows that eClinicalWorks' use of a cracked algorithm means PHI cannot be transmitted "through a secure channel" as required by 45 C.F.R. § 170.314(e)(1)(i). *See* Doc. 34 ¶¶ 68, 123-127.

The relators plausibly allege eClinicalWorks fails to comply with ONC certification requirements set forth in 45 C.F.R. § 170.314(e)(1)(i).

Local Storage of PHI. Because eClinicalWorks' EHR software stores PHI locally, the relators allege the software violates 45 C.F.R. § 170.315(d)(7)(i)-(ii). Doc. 34 ¶ 128. Under that regulation, the ONC provides that EHR software must (1) "encrypt the electronic health information stored on [end-user] devices after use of the technology on those devices stops," if it is "designed to locally store electronic health information on end-user devices"; or (2) be "designed to prevent electronic health information from being locally stored on end-user devices after use of the technology on those devices stops." 45 C.F.R. § 170.315(d)(7)(i)(A), (ii). eClinicalWorks argues that because the relators do not allege that eClinicalWorks fails to encrypt PHI "after use of the technology … stops," they have failed to state a viable theory that the local storage of PHI violates any ONC certification requirement. Doc. 69-1 at 30-31.

The relators, in effect, argue this is nit-picking at its worst. Docs. 75 at 13; 85 at 61:16-62:10. In paragraph 104 of the amended complaint, the relators allege "eClinicalWorks' EHR software stores [nonencrypted] PHI locally [which a person can access] regardless of whether that person was logged into eClinicalWorks' EHR software." Doc. 34 ¶ 104. Any reasonable person, they argue, would read their allegation to mean that eClinicalWorks fails to encrypt PHI "after use of the technology … stops." Doc. 75 at 6-7, 13. Nonetheless, at oral argument, the Court instructed the relators to provide a red-lined proposed amended complaint that addressed why the existing allegations were sufficient, and the language of a proposed amendment, to the extent the Court deemed an additional amendment necessary. Doc. 85 at 61:16-62:10; *see* Attachment 1.

The Court agrees that in paragraph 104 the relators plausibly allege eClinicalWorks fails to comply with ONC certification requirements set forth in 45 C.F.R. § 170.315(d)(7)(i)-(ii). However, to reassure eClinicalWorks, the relators shall file a second amended complaint adding only the proposed revised paragraph 104. Once filed, eClinicalWorks shall only respond to amended paragraph 104.

2. The Relators' HIPAA Compliance Theory is Plausibly Pled

The HIPAA Security Rule, in relevant part, requires healthcare providers "[e]nsure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits," and "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity of such information." 45 C.F.R. § 164.306(a)(1)-(2). According to the relators, eClinicalWorks caused its customers to both expressly and impliedly

submit false certifications of compliance with the HIPAA Security Rule because the "security vulnerabilities" in eClinicalWorks' software "make it impossible for a healthcare provider using the software to ensure the confidentiality, safety, and integrity of Protected Health Information stored in eClinicalWorks' EHR." Doc. 34 ¶¶ 107-114. The relators support their "impossibility" allegation with their allegations of specific flaws in eClinicalWorks' EHR software. *Id.* ¶¶ 56-86, 89-90, 95-102, 105-106.

The relators' HIPAA compliance theory is straightforward, perhaps deceptively so. The theory is not dependent on the disclosure of health information, which could be problematic. *See U.S. ex rel. Sheldon v. Kettering Health Network*, 816 F.3d 399 (6th Cir. 2016). Rather, to get paid, providers had to certify compliance with the HIPAA Security Rule, and the numerous flaws in eClinicalWorks' EHR software rendered their certifications false. Doc. 34 ¶¶ 107-114. Intuitively, for lack of a better word, the theory seems suspect. There is a near total dearth of authority suggesting that the arguably vague HIPAA Security Rule can be the basis for an FCA claim. But eClinicalWorks does not make a legal argument to that effect. *See* Doc. 69-1 at 32 n.9. In fact, they don't make a legal argument at all. Rather, they mount a cursory and poorly aimed factual attack on the relator's breach allegations. The HIPAA Security Rule, eClinicalWorks argues, does not require providers to "fully mitigate all risks of e-PHI breaches." Doc. 69-1 at 31 (quoting *Sheldon*, 816 F.3d at 409). The easy response to that argument is that the relators don't base their theory on false certifications that *all* risks of breach have been eliminated. Doc. 34 ¶¶ 107-114. Rather, they allege that because of the many flaws in eClinicalWorks' EHR software, it is impossible for providers to truthfully certify they complied with the HIPAA Security Rule. *Id.* One may

be skeptical that the relator's HIPAA compliance theory can stand. But for now, the Court can only address the argument eClinicalWorks makes and that argument fails.[5]

B. Relators Have Plausibly Pled Scienter

"With regard to scienter, a relator must show that the defendant acted 'knowingly,' which the FCA defines as either 'actual knowledge,' 'deliberate ignorance,' or 'reckless disregard.'" *United States ex rel. Phalp v. Lincare Holdings, Inc.*, 857 F.3d 1148, 1155 (11th Cir. 2017) (quoting 31 U.S.C. § 3729(a)(1)(A)-(B). Although relators "must state with particularity the circumstances constituting fraud," they may generally allege scienter. *Urquilla-Diaz,* 780 F.3d at 1051; *United States ex rel. Matheny v. Medco Health Sols., Inc.*, 671 F.3d 1217, 1224 (11th Cir. 2012). With respect to corporations, all material facts known by its officers and agents who are working for the corporation's benefit are imputed to the corporation. *Badger v. S. Farm Bureau Life Ins. Co.*, 612 F.3d 1334, 1347 (11th Cir. 2010). Thus, "where the [complaint] gives specific, detailed notice to [the] defendant of what wrongdoing it is alleged to have engaged in, and which of its agents or representatives were purportedly involved," the complaint need not "identify a particular corporate agent who made a certain statement or decision" to satisfy Rule 9(b). *United States v. Crumb*, 2016 WL 4480690, at *21 (S.D. Ala. Aug. 24, 2016).

Under those well-established pleading standards, the relators plausibly plead scienter. *See* Doc. 34 ¶ 165. eClinicalWorks' main argument to the contrary relies on *United States ex rel. Lewis v. Cmty. Health Sys., Inc.*, 2020 WL 3103994 (S.D. Fla.

[5] eClinicalWorks does not argue, as they do for the relators' EHR certification theory, that the relators have failed to plausibly allege scienter and materiality with respect to their HIPAA compliance theory. *See* Doc. 69-1 at 33-41.

June 11, 2020). Doc. 69-1 at 40-41. In *Lewis*, the relators alleged "that an assortment of [EHR] software functionalities did not work properly and that [the defendant], therefore, should not have been able to get its software certified [by the ONC]." 2020 WL3103994, at *17. While the majority of the alleged software flaws in *Lewis* related to functionality as opposed to security, the relators there did allege the EHR software's inability "to properly limit who could view and modify patient information," a similar allegation to those raised here. *Id.* at *15. Although the relators in *Lewis* alleged that the defendant "knew that its software failed to provide required functionality and misrepresented its software's ability to regularly perform functions required for … certification," the court held that such "immaterial generalities" and "conclusory allegations" were not accompanied by "actual *facts* … that [defendant] had knowledge of fraud or misrepresentations made to the government." *Id.* To the extent actual facts were alleged, those facts were "left dangling, unconnected to the [r]elators' fraud allegations." *Id.* Moreover, the court reasoned, even if the defendant had "first-hand knowledge of many issues that appear[ed] to render the software non-compliant with federal regulations," that "do[es] not amount to a showing of fraud." *Id.* at *16-17.

Unlike *Lewis*, where the relators named the EHR technology company, 140 hospitals, a management company, and the holding company, here the relators contend only eClinicalWorks is liable for violations of the FCA for its allegedly flawed software. *Id.* at *1; Doc. 34. Put differently, in *Lewis* it was the implausible, conclusory nature of the relators' allegations against multiple defendants that undercut the complaint. *See Twombly*, 550 U.S. at 570 ("Because the plaintiffs here have not nudged their claims across the line from conceivable to plausible, their complaint must be dismissed.");

Iqbal, 556 U.S. at 681 ("It is the conclusory nature of respondent's allegations, rather than their extravagantly fanciful nature, that disentitles them to the presumption of truth."). This case *only* concerns software, designed, developed, and marketed by eClinicalWorks. Among other things, the relators allege "the security flaws in eClinicalWorks' EHR software are so basic and obvious that they are known to eClinicalWorks' now and were known to eClinicalWorks when [the] [r]elators filed their initial Complaint." Doc. 34 ¶ 2. The relators then back up that allegation with specific factual details. For example, the relators allege eClinicalWorks designed the software to store unencrypted PHI locally. *Id.* ¶¶ 104, 128. Because such a design choice violates ONC certification requirements, eClinicalWorks knew that its attestations to the contrary were false. *See Badger*, 612 F.3d at 1347. And where the relators' allegations provide specific examples of wrongdoing, as they do here, the relators' failure to identify specific corporate officers who engaged in wrongdoing is not fatal. *See Crumb*, 2016 WL 4480690, at *21. Indeed, it is logical to infer that because eClinicalWorks' EHR software is its flagship product, its highest-ranking employees would be aware of the software capabilities, limitations, and flaws—including those flaws that flouted ONC certification requirements. *See* Doc. 34 ¶¶ 15-18.

The relators have plausibly pled scienter.

C. Relators Have Plausibly Pled Materiality

FCA claims can only be supported by material misrepresentations. *Universal Health Servs., Inc., v. United States ex rel. Escobar*, 579 U.S. 176, 192 (2016). The FCA "defines 'material' to mean 'having a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property.'" *Id*. at 182 (quoting 31

U.S.C. § 3729(b)(4)). The materiality requirement is "rigorous" and "demanding." *Id*. at 192, 194. "And while several factors can be relevant to the analysis, 'materiality cannot rest on a single fact or occurrence as always determinative.'" *Bibby,* 987 F.3d at 1347 (citing *Escobar,* 579 U.S. at 191). Although "no single factor is dispositive, some factors that are relevant to the materiality analysis include: (1) whether the requirement is a condition of the government's payment, (2) whether the misrepresentations went to the essence of the bargain with the government, and (3) to the extent the government had actual knowledge of the misrepresentations, the effect on the government's behavior."[6] *Id.*

For the first *Bibby* factor, "the Government's decision to expressly identify a provision as a condition of payment is relevant, but not automatically dispositive" of materiality. *Id.* (citing *Escobar*, 579 U.S. at 194). Here, the relators allege that EHR vendors must expressly certify their software meets the ONC's regulatory requirements, and providers must attest that they are using certified software to receive federal payments under Meaningful Use, MIPS, and PRQS. Doc. 34 ¶¶ 116, 132, 139, 149. Because these programs specifically provided various forms of incentive payments or downward adjustments for the use of certified EHR software, it follows that the use of software that met ONC certification requirements was a condition of payment. This factor weighs in favor of materiality.

Second, the relators plausibly allege the security vulnerabilities identified here go "to the essence of the bargain with the government." *Bibby*, 987 F.3d at 1347. Most significantly, the type of security vulnerabilities alleged by the relators—vulnerabilities

[6] eClinicalWorks relies heavily on *Bibby*, which is indeed instructive. Doc. 81 at 18-22. *Bibby* also involved a motion for summary judgment based on a developed record. 987 F.3d at 1344-46.

that leave the social security numbers and medical history of patients exposed—have been the focus of the ONC's regulatory certification requirements since they were first enacted in 2010. 45 C.F.R. § 170.302(o)-(v). And if there was any doubt that compliance with ONC certification requirements go to the "essence of the bargain," the relators' amended complaint cites *Delaney*, a separate FCA case where the relator alleged, and eClinicalWorks ultimately settled, allegations that "eClinicalWorks falsely represented to customers that its EHR software complied with applicable federal regulations while concealing fundamental defects in the system." Doc. 34 ¶ 19. Thus, the second factor also weighs in favor of materiality.

But *Delaney* is potentially problematic for the relators when it comes to the third factor—the extent of the government's knowledge of the alleged misrepresentations. In *Delaney*, the government intervened and after eClinicalWorks settled, the government required eClinicalWorks to enter the CIA with HHS-OIG. *Id.* ¶ 20. The CIA required eClinicalWorks to provide "timely access to … relevant software, media, and code" to the HHS-OIG approved SQOO. Doc. 17-1 at 34. One of the SQOO's express obligations under the CIA was "to ensure that eClinicalWorks and its EHR software … comply with applicable ONC Health IT Certification Program requirements." *Id.* at 32. In turn, the SQOO provided a formal report to the HHS every six months that documented its activities and findings. *Id.* at 35-37. Because eClinicalWorks was subject to the oversight of the SQOO, eClinicalWorks argues the supposed security vulnerabilities would have been discoverable even before relators commenced suit. Doc. 69-1 at 36-37. And even if the security vulnerabilities were not discovered until the relators filed their initial complaint in 2018, eClinicalWorks contends the fact that the

government continues to certify eClinicalWorks' EHR software and reimburse claims by healthcare providers who use it is strong—if not dispositive—evidence that the software vulnerabilities alleged by the relators are not material to the government's decision to pay. *Id.* at 36-39.

Factually, once developed, that could be a compelling argument, but knowledge of allegations or assumptions about what the government knew does not warrant dismissal as a matter of law. Indeed, as the Eleventh Circuit acknowledged, it has "not … addressed whether the government's knowledge of allegations is tantamount to knowledge of violations for purposes of the materiality analysis." *Bibby*, 987 F.3d at 1349. The logical answer would seemingly be no because a contrary conclusion would likely compel dismissal on materiality grounds in any case where the government declined to intervene. It could be, as eClinicalWorks seems to contend, that the government, after a thorough investigation, decided the relators' allegations were meritless.[7] Discovery may tell. But for now, it is only necessary that the relators plausibly allege materiality.

In any event, even a "finding" of materiality by the "factfinder" does not require the government to have taken "the strongest possible action," only that some enforcement action is taken. *Bibby*, 987 F.3d at 1352. Here, the relators allege the government did take *some* action. Docs. 34 ¶¶ 23-24; 69-3.

[7] The government, could of course, have moved to dismiss, and for what it's worth, it likely still can. 31 U.S.C. § 3730(c)(2)(A); *see Polansky v. Exec. Health Res. Inc*, 17 F.4th 376, 383-388 (3d Cir. 2021), *cert. granted* 142 S. Ct. 2834 (2022). If declining to intervene can be some evidence of lack of materiality, declining to seek dismissal, it seems, would undercut that evidence.

On December 6, 2018—less than two months after the relators sued—the government notified eClinicalWorks that it had "recently received information suggesting that eClinicalWorks' EHR technology may have dangerous security vulnerabilities" and directed eClinicalWorks to "immediately address any such security vulnerabilities." Doc. 69-3 at 4. Specifically, the government's letter outlined nine specific allegations—which largely trace the relators' complaint—and then stated that "the severity of these possible security issues, and the potential for patient harm, alarm us," and directed eClinicalWorks to confirm that it was "acting with all due speed to investigate and address such issues."[8] *Id.* at 4-6. That alleged government action alone sufficiently supports the relators' allegation of materiality as to the third factor.

In sum, the relators have plausibly alleged materiality.

IV. CONCLUSION

No argument raised by eClinicalWorks requires the dismissal of the relators' amended complaint. Accordingly, eClinicalWorks' motion to dismiss (Doc. 69) is **DENIED**. The relators shall file their second amended complaint, submitting their revised paragraph 104, by December 16, 2022.

SO ORDERED, this 6th day of December, 2022.

S/ Marc T. Treadwell
MARC T. TREADWELL, CHIEF JUDGE
UNITED STATES DISTRICT COURT

[8] The government, apparently, did more. Shortly before the Court issued this order, the relators, with no objection from eClinicalWorks, moved to supplement the record with an October 1, 2019, demand for stipulated penalties sent by HHS-OIG to eClinicalWorks for violations of eClinicalWorks' CIA. Docs. 86; 86-1; 87. Because eClinicalWorks does not object, the relators' motion to supplement (Doc. 86) is **GRANTED**.