STATE OF SOUTH DAKOTA	IN CIRCUIT COURT
COUNTY OF YANKTON	FIRST JUDICIAL CIRCUIT

MARY CLINE, Individually and as Personal Representative of the Estate of MAX CLINE, Plaintiff, v. YANKTON MEDICAL CLINIC, P.C., JOHN FRANK, M.D., and MICHAEL PIETILA, M.D., Defendants.	Civ. No. 14-355 **PLAINTIFF'S REPLY BRIEF IN SUPPORT OF MOTION TO COMPEL DEFENDANTS' RESPONSES TO PLAINTIFF'S REQUESTS FOR PRODUCTION OF DOCUMENTS #14 AND #15**

COMES NOW Plaintiff, by and through her attorney of record and respectfully submits this Reply Brief in Support of Plaintiff's Motion to Compel Defendants' Responses to Plaintiff's Requests for Production of Documents #14 and #15, and replies to Defendant's responsive brief as follows:

1. Defendants' misstate the factual background.

In an attempt to avoid the significance of the Decedent's audit trail, as not just the best evidence available, but perhaps the only available evidence to rebut Defendants' defense in this case, Defendants have mischaracterized the factual issues. Plaintiff's Amended Complaint actually reads as follows:

> 9. On November 19, 2012, Max was seen for follow-up chest x-ray by Pietila, who noted that although Max was symptom free, Max continued to have abnormal findings on chest x-ray.
> 10. On November 19, 2012, Pietila dictated his plan for Max to have a repeat chest CT in February, 2013.
> 11. Defendants never advised Max and/or Mary of any possible metastasis.

12. Defendants never advised Max and/or Mary of any recommended follow-up chest CT.
13. Defendants never took any steps to schedule Max for the recommended follow-up chest CT.

Defendants', however, morph the actual allegations into the factually unsupported assertion that Dr. Pietila "advised Cline to return for follow-up chest CT" and "Cline did not schedule or otherwise return for a follow-up chest CT as advised by Dr. Pietila." Defendants' Brief at pgs. 1-2.

In truth, the testimony in this case, from Max Cline's death bed, is as follows:

Q: Well, back in November of 2012 when they did that CT scan at Yankton Medical Clinic, did anybody ever tell you that they found nodules in both of your lungs in all four lobes?
A: No.
Q: Did anybody, back in November of 2012, tell you that those nodules, even though they thought they were infection at that time, possibly could be cancerous?
A: No.
Q: Did anybody tell you, back in November of 2012, that the radiologist, Dr. Eidsness, had recommended a follow-up CT scan in three months, which would have been February of 2013?
A: No.
Q: Did anybody tell you that Dr. Pietila, the pulmonologist, had recommended in his notes that you have a follow-up CT scan in February of 2013?
A: No.
Q: Who was your primary care physician up at Yankton Medical Clinic from November of 2012 through August 18th of 2014?
A: Dr. – Dr. Frank.
Q: And did Dr. Frank tell you any of those things?
A: No.
Q: And then back in November 2012 Dr. Pietila saw you a couple of times after they found these lung nodules. Did Dr. Pietila ever tell you that there's a possibility of cancer or that you needed a repeat CT scan in February of 2013?
A. No. No. No. No.

Affidavit of Counsel, Timothy L. James, Exhibit D (Max Cline Deposition at pgs. 24-25). Max testified:

Q. Max, I went through your medical records just briefly this morning and I – I noticed that from November of 2012 when the lung nodules were first notied on the CT scan through August 18, 2014 when you were diagnosed with the cancer

at Avera Hospital, that you had either called or visited Yankton Medical Clinic 21 times. And my question to you is, during any of those visits or calls after 2012, did anybody at Yankton Medical Clinic, Dr. Frank, Dr. Pietila, anybody, tell you that they had already found lung nodules in your lung back in November 2012 that could be potentially cancerous?

A: No.

Id. at p. 27.

Defendants' mischaracterization of Plaintiff's complaint is important. First, by falsely suggesting that Dr. Pietila actually advised Max to get a CT and that Max simply ignored the advice, allows Defendants to advance their claim that the audit trial is irrelevant. Second, it points up the Defenses' opportunity to manufacture a defense through medical records and convenient recollection without contradiction by the audit trail. It is an absurd twist on the concepts of justice and evidentiary principles that would allow the Defendants to utilize self-serving and modifiable medical records and untested testimony to call a dying man a liar when the truth may be found in the audit trail.

2. HIPAA protects patients.

Defendants' argument disregards the congressional intent of the privacy standards of HIPAA. Congress made it clear, by identifying as the very first stated purpose of the regulation, "to protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information." 65 FR 82461-82510, 82468 (12/28/2000). Fundamentally, issues of disclosure must be viewed in the context of the patient's right to access and control of his healthcare information which is the defining interest at the core of HIPAA. Max and his family have a compelling interest in accessing the audit trail information that may very well explain how Defendants failed Max. As Max testified:

Q: Max, how is – just tell us how you feel about the fact that you went from November 2012 to August 18, 2014 and nobody told you about the lung nodules, and here you are with Stage 4 lung and brain cancer?

A: I just feel – I feel like I went from having everything in life to being cut down to nothing, for no reason. I just – I don't understand how – how that could happen. I just don't understand.

Affidavit of Counsel, Timothy L. James, Exhibit D (Max Cline Deposition at pgs. 29-30).

Defendants cannot identify any reasonable competing interest to offset the compelling interest of Plaintiff in this case. Protecting Defendants' personal and financial interests by covering up their neglect is not a reasonable interest to deny Plaintiff access to the audit trail information, to further Plaintiff's understanding of what caused Max's death, and to prevent Defendants inappropriate use or modification of medical information to support their defense. In short, if Defendants have nothing to hide – why hide it? The reasonable inference is that Defendants have either falsified records or haven't complied with the HIPAA laws. HIPAA requires security measures to assure the integrity of healthcare information so that protected information is not improperly modified without detection. 45 CFR 164.304; see 45 CFR 164.312 (e)(2)(i). Congress specifically intended to protect Max's medical record from improper modification by these Defendants. Essentially, Defendants are asking this Court to render Congress' directive meaningless and allow Defendants to both modify the medical records and conceal the evidence of the modification.

Defendants' proposed disregard of the oversight established by Congress further erodes the confidence of patients in the health care system - which is one reason Congress imposed the oversight.

> Individuals cannot be expected to share the most intimate details of their lives unless they have confidence that such information will not be used or shared inappropriately. Privacy violations reduce consumers' trust in the health care system and institutions that serve them. Such a loss of faith can impede the quality of the health care they receive, and can harm the financial health of health care institutions.

> Patients who are worried about the possible misuse of their information often take steps to protect their privacy. Recent studies show that a person who does not believe his privacy will be protected is much less likely to participate fully in the diagnosis and treatment of his medical condition. A national survey conducted in January 1999 found that one in five Americans believe their health information is being used inappropriately. See California HealthCare Foundation, "National Survey: Confidentiality of Medical Records"(January, 1999) (http://www.chcf.org). More troubling is the fact that one in six Americans reported that they have taken some sort of evasive action to avoid the inappropriate use of their information by providing inaccurate information to a health care provider, changing physicians, or avoiding care altogether. Similarly, in its comments on our proposed rule, the Association of American Physicians and Surgeons reported 78 percent of its members reported withholding information from a patient's record due to privacy concerns and another 87 percent reported having had a patient request to withhold information from their records. For an example of this phenomenon in a particular demographic group, see Drs. Bearman, Ford, and Moody, "Foregone Health Care among Adolescents," *JAMA*, vol. 282, no. 23 (999); Cheng, T.L., et al., "Confidentiality in Health Care: A Survey of Knowledge, Perceptions, and Attitudes among High School Students," *JAMA*, vol. 269, no. 11 (1993), at 1404-1407.

65 FR 82461-82510, 82477, (12/28/2000).

HIPAA is intended, in part, to protect patients from providers. One of the purposes of HIPAA is the protection of confidentiality and security of healthcare information. This is a protection granted to the patient against the healthcare provider. The only way for the patient to be ensured of the confidentiality and security of his healthcare information is to be made privy to such information. However, the Defendants argue that the patient is not entitled to the only information that can confirm the patient's health records are safe. In simpler terms, Defendants argue that the purpose of HIPAA is to protect providers from patients – contrary to HIPAA's stated purpose.

3. Defendants Federal Register authority is outdated and revised.

Defendants rely on the outdated rule of the Department of Health and Human Services (hereinafter "Department") from 2000 (65 FR 82462-01, 82554) to claim that providers are not required to give patients access to their verifying audit material. Defendants' Brief at pg. 6. Defendants' limited definition of "designated record set" was declined by the Department of Health and Human Services (hereinafter "Department") that specifically interpreted to the health information to include the raw data of access found in "access logs" that "also may commonly be referred to as an "audit trail" in addition to an accounting of the disclosures. Dept. of Health and Human Services Notice of Proposed Rulemaking, 76 FR 31426-49, 31436. Noting that covered entities, like Yankton Medical Clinic, P.C., may have multiple systems with separate access logs, Secretary of the Department, Kathleen Sebelius, (hereinafter "Secretary") explained the Department's expectation that, data from each access log will be gathered and aggregated to generate a single access report (including data from business associates' systems.) *Id*. The Secretary specifically rejected Defendants' interpretation of a limited "designated record set" by stating:

> **We have included all electronic protected health information in a designated record set, rather than only EHR information**, because we believe that this greatly improves transparency and better facilitates compliance and enforcement, while placing a reasonable burden on covered entities and business associates. As discussed below, in accordance with the Security Rule, all electronic systems with designated record set information should be creating access logs with sufficient information to create an access report. **Regardless of whether the system qualifies as an EHR, we believe that it is reasonable to provide this access log information to individuals upon their request**.

Id. at 31437. (Emphasis added).

Significant modification to the outdated Federal Register authority relied upon by Defendants, began in 2009, with *The Health Information Technology for Economic and Clinical Health* (HITECH) Act, enacted as part of the *American Recovery and Reinvestment Act of 2009*, that was signed into law on February 17, 2009, "to promote the adoption and meaningful use of health information technology." As the Secretary noted in the Department's notice of proposed rulemaking to expand the accounting provisions of HIPAA and to implement HITECH:

> Section 13405(c) of the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111–5), provides that the exemption at § 164.528(a)(1)(i) of the Privacy Rule for disclosures to carry out treatment, payment, and health care operations no longer applies to disclosures 'through an electronic health record.' **Section 13400 of the HITECH Act defines an electronic health record (''EHR'') as 'an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.' Under section 13405(c), an individual has a right to receive an accounting of such disclosures made during the three years prior to the request**.

Id. at 34217. (Emphasis added). On its face, HITECH requires Defendants to provide Plaintiff with an accounting of all disclosures relating to disclosures of Max's EHR for three years prior to request. Defendants have refused and failed to comply with HITECH.

The Department gave notice to Defendants on May 31, 2011, of its intention to implement HITECH and expand HIPAA to include the patient's right to an "access report" in addition to an "accounting of disclosures". *Id*. The Department invited public comment, including providers. *Id*. In response, "[c]ommenters pointed out that the use of **audit trails** and the right to an accounting of disclosures improves the detection of breaches and assists with the identification of weaknesses in privacy and security practices." *Id*. (Emphasis added). At that time, the Department contemplated implementing HITECH and expanding the "Privacy Rule" in

the accounting disclosure provisions of 45 CFR §164.528. *Id*. The intent of the Department to expand the definition and scope of the protected health information, to which the patient is entitled, was expressed by the Secretary in her rationale for the proposed rule, as follows:

> We are proposing to revise §164.528 of the Privacy Rule by dividing it into two separate rights for individuals: paragraph (a) would set forth an individual's right to an accounting of disclosures and paragraph (b) would set forth an individual's right to an access report (which would include electronic access by both workforce members and persons outside the covered entity). Our revisions to the right to an accounting of disclosures are based on our general authority under HIPAA and are intended to improve the workability and effectiveness of the provision. The right to an access report is based in part on the requirement of section 13405(c) of the HITECH Act to provide individuals with information about disclosures through an EHR for treatment, payment, and health care operations. This right to an access report is also based in part on our general authority under HIPAA, in order to ensure that individuals are receiving the information that is of most interest.
>
> We believe that these changes to the accounting requirements will provide information of value to individuals while placing a reasonable burden on covered entities and business associates. The process of creating a full accounting of disclosures is generally a manual, expensive, and time consuming process for covered entities and business associates. In contrast, we believe that the process of creating an access report will be a more automated process that provides valuable information to individuals with less burden to covered entities and business associates. By limiting the access report to electronic access, the report will include information that a covered entity is already required to collect under the Security Rule. Under §§ 164.308(a)(1)(ii)(D) and 164.312(b) of the HIPAA Security Rule, a covered entity is required to record and examine activity in information systems and to regularly review records of such activity.

Id. at 31428-29.

> In addition to the right to an accounting of disclosures, we are proposing to provide individuals with a right to receive an access report that indicates who has accessed their electronic designated record set information (this right does not extend to access to paper records). In the below discussion of the proposed right to an access

> report, we refer to both 'access logs' and 'access reports.' For purposes of this discussion, the access log is the raw data that an electronic system containing protected health information collects each time a user (as the term is defined in the Security Rule at § 164.304) accesses information. The access report is a document that a system administrator or other appropriate person generates from the access log in a format that is understandable to the individual. We note that an access log also may commonly be referred to as an 'audit trail' or 'audit log' and an access report is similar to an 'audit report.' We do not use the terms audit trail or audit log in order to distinguish the access report from documents that are generated by organizations for their internal auditing purposes. We also note that a covered entity will usually have electronic designated record set information in multiple systems which each maintain separate access logs. Our expectation is that data from each access log will be gathered and aggregated to generate a single access report (including data from business associates' systems).

Id. at 31436.

> We believe that the administrative burden on covered entities who are complying with the HIPAA Security Rule will be reasonable, in light of their existing obligation to log access to electronic protected health information. Section 164.312(b) of the Security Rule (Standard: Audit Controls) currently requires covered entities to 'implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.' Therefore, systems with designated record set information should already be configured to record activities such as when users access information. Additionally, § 164.308(a)(1)(ii)(D) of the Security Rule (Implementation specification: Information system activity review) currently requires covered entities to 'implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.' Accordingly, covered entities should already be logging access to electronic protected health information and regularly reviewing reports of such access.

Id. at 31437. Thus, the Affidavit of Jake Drotzman, propounded by Defendants to suggest that Yankton Medical Clinic, P.C. may not have maintained records required by the federal law, is

not a bar to producing the audit trail and other electronic health information as it exists. Rather, it is an admission that entitles Plaintiff to a remedy for spoliation of evidence.

As the Secretary noted, all of the proposed material is already contained in the protected health record by virtue of existing provisions required to be followed by Defendants. *Id*. Plaintiff's right to an accounting of disclosures relating to Max's protected health information is found at 45 CFR §164.528, while Plaintiff's right to access, to wit: inspect and obtain a copy of Max's protected health information is found at 45 CFR § 164.524. Max's protected health information, as contemplated by the Department, necessarily includes the audit information required to be monitored and maintained by Yankton Medical Clinic, P.C. pursuant to 45 CFR § 164.304 (requirement to security incidents of access, use, disclosure, modification, or destruction of health information); 45 CFR § 164.306 (requirement to ensure integrity of health information); 45 CFR § 164.312(b) and (c) (requirement to employ mechanisms to **record** system activity in electronic protected health information and protection from alteration or destruction) and §§ 164.308(a)(1)(ii)(D) and 164.312(b) of the HIPAA Security Rule, (requirement to record and examine activity in information systems and to regularly review records of such activity).

On January 25, 2013, the Department expanded HITECH and the Privacy Rule to include access to the entirety of a patient's health information, including the audit information already required to be maintained by Defendants. In so doing, the Department explicitly included access to any designated record set electronically maintained by Defendants in addition to the EHR as follows:

> Section 13405(e) applies by its terms only to protected health information in EHRs. However, incorporating these new provisions in such a limited manner in the Privacy Rule could result in a complex set of disparate requirements for access to

> protected health information in EHR systems versus other types of electronic records systems. As such, the Department proposed to use its authority under section 264(c) of HIPAA to prescribe the rights individuals should have with respect to their individually identifiable health information to **strengthen the right of access** as provided under section 13405(e) of the HITECH Act more uniformly to all protected health information maintained in one or more designated record sets electronically, regardless of whether the designated record set is an EHR.

78 FR 5566-5702, 5631 (Emphasis added).

The final rule as adopted and applied at 45 CFR § 164.524(c)(2)(ii) requires that,

> … if an individual requests an electronic copy of protected health information that is maintained electronically in one or more designated record sets, the covered entity must provide the individual with access to the electronic information in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual. In such cases, to the extent possible, we expect covered entities to provide the individual with a machine readable copy of the individual's protected health information. The Department considers machine readable data to mean digital information stored in a standard format enabling the information to be processed and analyzed by computer. For example, this would include providing the individual with an electronic copy of the protected health information in the format of MS Word or Excel, text, HTML, or text-based PDF, among other formats.

Id.

When asked to clarify what constitutes an EHR, the Secretary reiterated that a patient's access to the electronic record is not limited to the EHR, and responded as follows:

> Under this final rule, the requirement to provide individuals with access to an electronic copy **includes all protected health information maintained in an electronic designated record set** held by a covered entity. Because **we are not limiting the right of electronic access to EHRs**, we do not believe there is a need to define or further clarify the term at this time.

Id. at 5631-32. (Emphasis added). The final rule was effective on March 26, 2013, and Defendants were required to comply with the final rule by September 23, 2013. *Id*. at 5566. Defendants were required to provide access to Plaintiff in 30 days, if not sooner, with a one-time extension of 30 days including a written notice to the Plaintiff of the reasons for the delay and the expected date by which Defendants would complete action on Plaintiff's request. *Id*. at 5637. To date, Defendants have failed and refused to comply with the federal requirements.

Defendants, in citing the 2000 Federal Register discussion from prior to the updated rules changes at 65 CFR 82884 (2000), suggest a circumvention of the applicable law by virtue of a "quality control" and "peer review" analysis. However, such an analysis was specifically rejected by the Secretary in adopting the final rule, as follows:

> We clarify that this HIPAA electronic right of access requirement does preempt contrary State law unless such law is more stringent. In the case of right of access, more stringent means that such State law permits greater rights of access to the individual.

Id. at 5632. Recently, in *Andrews v. Ridco & Twin City Fire Ins. Co.*, 2015 S.D. 24 (2015), our Supreme Court expressed its disfavor of the practice of comingling privileged and unprivileged information and then attempting to assert the protections of the privilege. In *Andrews*, the issue was whether the defendant insurer waived the attorney-client privilege in discovery, "by embedding attorney-client privileged communications in the claim file notes and then redacting the communications." The Court ordered the defendant insurer to produce all documents in un-redacted form. Similarly, Defendants in this instance are attempting to intermingle data in an effort to create a privilege and use the audit trail as a shield and a sword. Our Supreme Court in *Andrews* refused to allow a similar tactic and noted that, "Any other rule would enable the client

to use as a sword the protection which is awarded him as a shield." *Caster v. Moeller*, 126 N.W.2d 485 (Neb. 1964).

4. Defendants' miscellaneous arguments.

Defendants cite as authority the ruling of the Honorable Scott P. Myren, Circuit Court Judge, in the matter captioned, *Morris v. Avera St. Luke's*, et. al, 5th Jud. Cir., S.D., Civ. 08-1171, (Motions Hearing, February 12, 2014), for the proposition that a patient's audit trail is not a part of the patient's medical record. The record of the subject motions hearing, however, clearly reflects that the applicable Federal Regulations were not provided to, argued to, or considered by Judge Myron. Affidavit of Counsel, Timothy L. James, Exhibit E (Transcript of Motions Hearing, Civ. 08-1171). In fact, counsel for the provider argued contrary to the applicable law, stating, "They do not have a right to the **designated record set**." *Id*. Exhibit E, at pg. 11. (Emphasis added). However, in the instant case, we know the "designated record set" argument is without merit because, "… if an individual requests an electronic copy of protected health information that is maintained electronically **in one or more designated record sets**, the covered entity must provide the individual with access to the electronic information in the electronic form and format requested by the individual. 78 FR 5566-5702, 5631 (Emphasis added). In fact, this point was reiterated by the Secretary as follows:

> Under this final rule, the requirement to provide individuals with access to an electronic copy **includes all protected health information maintained in an electronic designated record set** held by a covered entity. Because **we are not limiting the right of electronic access to EHRs**, we do not believe there is a need to define or further clarify the term at this time.

Id. at 5631-32. (Emphasis added).

Counsel in *Morris* also suggested to Judge Myron that disclosure of the audit trails would "create this huge bulk of discovery" and argued that the makers of HIPAA

"decided we've got to have a limit somewhere." Affidavit of Counsel, Timothy L. James, Exhibit E at pg. 16-17. That suggestion along with the Defendants' unduly burdensome arguments were dispelled by the Secretary as follows, "[w]ith regard to the additional burdens on covered entities, we note that providing access to protected health information held in electronic designated record sets was already required under the Privacy Rule at § 164.524, … ." 78 FR 5566-5702, 5631. The Secretary further stated:

> … covered entities must provide an electronic copy of all protected health information about the individual in an electronically maintained designated record set, except as otherwise provided at § 164.524(a). If the designated record set includes electronic links to images or other data, the images or data that is linked to the designated record set must also be included in the electronic copy provided to the individual. The electronic copy must contain all protected health information electronically maintained in the designated record set at the time the request is fulfilled.

Id. at 5633.

The remainder of Defendants' CFR interpretation arguments are similarly based on outdated authority and are debunked by the Department's explicit interpretation that, under federal law, the protected health information is not limited to the EHR and includes all data that Defendants are required to maintain in the electronic record pursuant to 45 CFR, et.seq.

Defendants argue the curious position that patients were not entitled to an audit trail during the "paper days" and, thus, patients are not entitled to an audit trail in the electronic age, despite the Department's clear mandate to the contrary. Clearly, the rights of today's patients are not based on the limitations of previous technology and Defendants' bare assertion does not trump the Department's interpretation and regulation.

Finally, Defendants argue that the complete electronic record is not relevant. There is no law to support Defendants' theory. In fact, before a relevance analysis is itself relevant,

Defendants must explain their blatant disregard of the federal rules governing disclosure of Max's electronic medical record, including the audit trail and raw data. Pursuant to the federal law, Defendants were required to produce the entirety of electronic data associated with Max's electronic medical record including links to other data, such as, Yankton Medical Clinic, P.C.'s link to the electronic medical record at Avera Sacred Heart Hospital. Defendants have failed to produce the electronic record within 30 days or request a written extension for an additional 30 days. In other words, Plaintiff is entitled to all of the electronic data even if it isn't relevant. Yet, the data could not be more relevant where Defendants may create requests for testing that never existed. If such requests did exist – they would be recorded in the electronic medical record. Because the request either don't exist or the medical record was tampered with to show they exist – the complete electronic medical record and associated data is extremely relevant. In addition, Max had multiple encounters with Defendants during the period Defendants were failing to inform Max that he may have cancer and required a CT scan. Each time Max's electronic record was accessed, by whom and for what reason, chronicles the Defendants' failures and is relevant.

5. Internet Information Relating To NextGen.

Defendants utilize the NextGen software according to the Affidvit of Jake Drotzman. NextGen advertises its EHR system as "simple. smart. fast." Affidavit of Timothy L. James, Exhibit F (various pages of NextGen internet marketing material). In fact, as soon as the physician opens the electronic chart, meaningful information relating to the patient appears, including reason for the visit and orders. *Id*. at pg. 7. The system also allows, "real-time access to up-to-the-minute patient data." *Id*. at 10. Generating reports is an easily performed task with

the NextGen system. Affidavit of Counsel, Timothy L. James, Exhibit G, (various pages of an internet power point presentation showing NextGen screens to describe report generation).

The Appointment List & Task List, such as scheduling a CT for Max Cline, is usually set to appear as soon as NextGen is opened. Affidavit of Counsel, Timothy L. James, Exhibit H, (various pages of an internet power point presentation showing NextGen Appointment List & Task Lists). Not only does the NextGen system allow a provider to identify his own tasks, he can send task to other physicians, nurses, schedulers or work groups; receive a task; assign a priority to the task; assign a due date to the task; send a reminder for the task; attach part of the patient's chart to the task; and check to see if the task is completed. *Id*. With all the available provisions in the NextGen system to ensure that Max was notified of, scheduled, and completed the CT scan, it is critical to receive the electronic record and associated audit trail to determine if the task was even entered and if so, who ignored it, why and when. In addition, it is important to know if the task was documented as a task on the electronic record each time Max had one of his 21 subsequent encounters with Yankton Medical Clinic, P.C.

The NextGen system includes the potential for a patient portal where patients would have computer access to some limited information from their medical record. Affidavit of Counsel, Timothy L. James, Exhibit I, (NextGen Patient Portal User Guide). Interestingly, the Patient Portal includes an "Audit History" that shows the patient the identity of any person who viewed his chart, the event description of the login, and the event date. *Id*. These Defendants have refused to even disclose this basic information relating to Max Cline even though it is available on the NextGen Patient Portal. Why would NextGen advertise its Patient Portal, that includes the Audit History, if disclosure of audit information is prohibited by law as Defendants suggest?

More importantly, why would Defendants have the capability to provide the Patient Portal information to its patients but then keep it a secret?

NextGen has a provision for an "Addendum (EHR)" that allows a supplement to a locked encounter that shows the date of a subsequent addition of images or documents. Affidavit of Counsel, Timothy L. James, Exhibit J, (NextGen, eLearning Resource Center, glossary of terms). Thus, while the paper copy of Max's medical record would show a contemporaneous image or document, the audit trail would show if the item was actually inserted into the record at a later date, for example after notice of a potential lawsuit.

NextGen has a provision for an "Alert" signifying issues pertaining to a patient about which the provider or practice must be made aware. *Id*. Like the "Tasks", the electronic records and audit trail are relevant to determine the failure of creating the Alert or the failure to act on the Alert concerning Max Cline's follow-up CT.

NextGen defines both the "EHR" Electronic Health Record (more than one health care organization) and "EMR" Electronic Medical Record (single organization) and identifies that both can be created, managed and consulted. *Id*. In addition, the NextGen system allows for an "Encounter Custom (EHR)" as follows:

> A Custom Encounter is an encounter that a user creates in a patient's chart for a specific date that has already past. All components of the medical records module can be used in a custom encounter. Custom encounters cannot be created for future dates. When a custom encounter is created, the encounter displays in the Encounter View window with the date the user has specified, but the properties of the encounter will show the actual date and time it was created.

Id. Since all components of the medical record system can be customized, it is important and relevant to see the system properties for when the customization occurred. Identification of users

with access to NextGen and the extent of that access is available from the authorized users list pursuant to the "Authentication" process. *Id*.

Finally, NextGen has a provision for an "Audit Trail" defined as:

> **A means of tracing all activities affecting data from the time it is entered into a system to the time it is entered into a system to the time it is removed. An audit trail makes it possible to document who made changes to a particular record and when**.

Id. (Emphasis added). Thus, we know it exists on the NextGen system, we know what it does, we know it is available, we know the law requires it, and we know it is relevant.

CONCLUSION

WHEREFORE, Plaintiff respectfully requests the Court to require Defendant to answer the disputed discovery within a reasonable time and for Plaintiff's costs and attorney's fees in pursuing this Motion.

Dated this 3rd day of May, 2015.

JAMES LAW, P.C.

/s/Timothy L. James
Timothy L. James
P.O. Box 879 – 311 Walnut Street
Yankton, SD 57078
Phone: (605) 665-0594
Email: tim@timjameslaw.com
Attorneys for Plaintiff

CERTIFICATE OF SERVICE

This is to certify that a true and correct copy of the foregoing Plaintiff's Reply Brief in Support of Motion to Compel was served by Odyssey on May 3, 2015, to the following attorneys of record:

Shane Eden
SEden@dehs.com
Edwin Evans
eevans@dehs.com
Davenport, Evans, Hurwitz & Smith, L.L.P.
P.O. Box 1030
Sioux Falls, SD 57101-1030

*/s/Timothy L. James*_____
Timothy L. James