



DIVISION OF
CORPORATION FINANCE

No Act

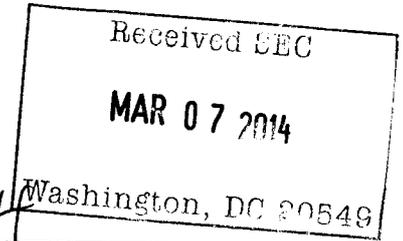
UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

P.E. 1/17/14



14005562

March 7, 2014



Craig L. Evans
Stinson Leonard Street LLP
craig.evans@stinsonleonard.com

Act: 1934
Section: _____
Rule: 14a-8 (ODS)
Public _____
Availability: 3-7-14

Re: Cerner Corporation

Dear Mr. Evans:

This is in regard to your letter dated March 7, 2014 concerning the shareholder proposal submitted by Arjuna Capital/Baldwin Brothers Inc. on behalf of Steven Schewel for inclusion in Cerner's proxy materials for its upcoming annual meeting of security holders. Your letter indicates that the proponent has withdrawn the proposal and that Cerner therefore withdraws its January 17, 2014 request for a no-action letter from the Division. Because the matter is now moot, we will have no further comment.

Copies of all of the correspondence related to this matter will be made available on our website at <http://www.sec.gov/divisions/corpfin/cf-noaction/14a-8.shtml>. For your reference, a brief discussion of the Division's informal procedures regarding shareholder proposals is also available at the same website address.

Sincerely,

Adam F. Turk
Attorney-Adviser

cc: Natasha Lamb
Arjuna Capital/Baldwin Brothers Inc.
natasha@arjuna-capital.com



Craig L. Evans
816.691.3186 DIRECT
816.412.1129 DIRECT FAX
craig.evans@stinsonleonard.com

March 7, 2014

Via electronic mail (shareholderproposals@sec.gov)

U.S. Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
100 F Street, N.E.
Washington, D.C. 20549

Re: Cerner Corporation
Withdrawal of No-Action Request Regarding
the Shareholder Proposal of Steven Schewel
Exchange Act of 1934 – Rule 14a-8

Ladies and Gentlemen:

In a letter dated January 17, 2014, we requested that the staff of the Division of Corporation Finance concur that our client, Cerner Corporation (the “Company”), could exclude from its proxy materials for its 2014 Annual Meeting of Shareholders a shareholder proposal (the “Shareholder Proposal”) and statement in support thereof submitted by Steven Schewel and his designated proxy Natasha Lamb of Arjuna Capital/Baldwin Brothers Inc. (collectively, the “Proponent”).

Enclosed as Exhibit A is a letter from the Proponent, dated March 7, 2014, withdrawing the Shareholder Proposal. In reliance on the letter from the Proponent, we hereby withdraw our January 17, 2014 no-action letter request relating to the Company’s ability to exclude the Shareholder Proposal pursuant to Rule 14a-8 under the Securities Exchange Act of 1934.

Please do not hesitate to contact me at (816) 691-3186 with any questions in this regard.

Sincerely,

Stinson Leonard Street LLP

A handwritten signature in black ink, appearing to read "Craig L. Evans", with a stylized flourish at the end.

Craig L. Evans

cc: Natasha Lamb, Director of Equity Research & Shareholder Engagement — Arjuna
Capital/Baldwin Brothers Inc. (as proxy for Steven Schewel)
Randy Sims, Senior Vice President, Chief Legal Officer and Secretary — Cerner
Corporation

U.S. Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
March 7, 2014
Page 2

Exhibit A

See attached letter.



VIA E-MAIL TO amy.abrams@cerner.com

March 7, 2014

Amy C. Abrams
Corporate Counsel
Cerner Corporation

Re: Shareholder Proposal for the 2014 Annual Meeting

Dear Ms. Abrams,

This letter is being submitted by Arjuna Capital ("Arjuna Capital") on behalf of Stephen Matthew Schewel (the "Proponent") with respect to a shareholder proposal (the "Proposal") submitted to Cerner Corporation (the "Company") by Arjuna Capital on behalf of the Proponent on December 11, 2013.

On behalf of the Proponent, Arjuna Capital hereby withdraws the Proposal. This is due to changes that the Company has made to its governance instruments to include privacy and data security oversight in the Board Audit Committee Charter in response to the Proposal.

The Board is to be commended for its action that will serve the best interests of the Company and its shareholders.

Sincerely,

A handwritten signature in black ink, appearing to read 'NL', is written over a horizontal line.

Natasha Lamb

Director of Equity Research & Shareholder Engagement

February 17, 2014

VIA e-mail: shareholderproposals@sec.gov

Office of Chief Counsel
Division of Corporation Finance
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549

Re: Cerner Corp's January 17, 2014 Request to Exclude Shareholder Proposal of Arjuna Capital/Baldwin Brothers Inc. on behalf of Steven Schewel.
Securities and Exchange Act of 1934—Rule 14a-8

Dear Sir/Madam:

This letter is submitted on behalf of Steven Schewel by Arjuna Capital/Baldwin Brothers Inc., as their designated representative in this matter (hereinafter referred to as the "Proponent"), who is the beneficial owner of shares of common stock of Cerner Corp (hereinafter referred to as "Cerner" or the "Company"), and who has submitted a shareholder proposal (hereinafter referred to as "the Proposal") to Cerner, to respond to the letter dated January 17, 2014 sent to the Office of Chief Counsel by the Company, in which Cerner contends that the Proposal may be excluded from the Company's 2014 proxy statement under Rules 14a-8(j).

We have reviewed the Proposal and the Company's letter, and based upon the foregoing, as well as upon a review of Rule 14a-8, it is our opinion that the Proposal must be included in Cerner's 2014 proxy statement because the subject matter of the Proposal transcends the ordinary business of the Company by focusing on a significant social policy issue confronting the Company. Therefore, we respectfully request that the Staff not issue the no-action letter sought by the Company.

Pursuant to Staff Legal Bulletin 14D (November 7, 2008) we are filing our response via e-mail in lieu of paper copies and are providing a copy to Craig Evans, Office of Chief Counsel, via email at craig.evans@stinsonleonard.com and Cerner's Chief Legal Officer and Secretary, Randy Sims via e-mail at rsims@cerner.com.

The Proposal

The Proposal, the full text of which is attached as Attachment A, requests that:

...the Board of Directors publish a report, at reasonable expense and excluding confidential or proprietary information, explaining how the Board is overseeing privacy and data security risks.

The Supporting Statement clarifies:

It should be emphasized that the Proposal is not asking the Company to disclose risks, specific incidents, or legal compliance procedures, but rather, we believe investors need to understand more fully how the Board is overseeing the concerns described above.

The Company asserts that the Proposal is excludable pursuant to Rule 14a-8(i)(7), as addressing the Company's ordinary business -- the policing of privacy and data security. Although prior Staff decisions have allowed similar exclusions, this Proposal addresses a transcendent social policy issue. Cerner is the world's largest stand-alone maker of health care information technology solutions, which are licensed to more than 10,000 facilities around the world. In just the last four years, the health care industry has experienced a dramatic acceleration in the deployment of digital technologies for patient information. While these technologies are widely seen as encouraging greater efficiency, they have also often been challenged by legislators, regulators and patient advocates for their potential failure to secure the Protected Health Information (PHI) of millions of health care recipients. Accordingly, in this instance, the issue of board oversight of privacy and data, and the catastrophic risks associated with a failure of such oversight, is a very significant social policy issue. Therefore, the Proposal addresses a transcendent social policy issue with a clear nexus to the Company. Further, as an inquiry into the Company's oversight process, the Proposal does not micromanage. Accordingly, it is not excludable pursuant to Rule 14a-8(i)(7).

The Proposal is focused on a significant policy issue and does not seek to micro-manage the Company

In 1998, the Commission explained:

The policy underlying the ordinary business exclusion rests on two central considerations. The first relates to the subject matter of the proposal. Certain tasks are so fundamental to management's ability to run a company on a day-to-day basis that they could not, as a practical matter, be subject to direct shareholder oversight. Examples include the management of the workforce, such as the hiring, promotion, and termination of employees, decisions on production quality and quantity, and the retention of suppliers. However, proposals relating to such matters but focusing on sufficiently significant social policy issues (e.g., significant discrimination matters) generally would not be considered to be excludable, because the proposals would transcend the day-to-day business matters and raise policy issues so significant that it would be appropriate for a shareholder vote.

The second consideration relates to the degree to which the proposal seeks to "micro-manage" the company by probing too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment. This consideration may come into play in a number of

circumstances, such as where the proposal involves intricate detail, or seeks to impose specific time-frames or methods for implementing complex policies.¹

Consequently, a key question for consideration in determining the permissibility of a proposal is what does the proposal focus on. As the staff explained in Staff Legal Bulletin 14A (July 12, 2002), "proposals that relate to ordinary business matters but that focus on 'sufficiently significant social policy issues . . . would not be considered to be excludable because the proposals would transcend the day-to-day business matters.'"

Background

An explosion in digital technology in just the past four years has changed the landscape in the health care industry and given rise to an exponential increase in concern over privacy and data security.

For example, according to data recently released by the U.S. Department of Health and Human Services, more than half of America's doctors have now adopted electronic health records (EHRs), and the number of doctors and hospitals using EHRs continues to increase dramatically.² This growth can be traced to the 2009 American Reinvestment and Recovery Act, which provided for incentive payments under Medicare and Medicaid to doctors and hospitals that adopted and meaningfully used EHRs. Passage of the Affordable Care Act has added significant momentum to these trends.

As a result, Cerner is now a leading supplier of health care information technology solutions, services, devices and hardware. According to the company, these solutions are licensed by approximately 10,000 facilities around the world, including more than 2,700 hospitals; 4,150 physician practices; 45,000 physicians; 550 ambulatory facilities, such as laboratories, ambulatory centers, behavioral health centers, cardiac facilities, radiology clinics and surgery centers; 800 home health facilities; 45 employer sites and 1,750 retail pharmacies.

Under the Staff's decision-making process, an issue may not be considered a significant policy issue one year, but can rise to such a status if the issue has congressional, public and media attention, and a clear nexus to the company. This has happened in recent years on various other issues including net neutrality, antibiotics in animal feed, and climate change. With this proposal, we believe the Staff should make the same determination regarding privacy and data security at Cerner.

¹ Exchange Act Release No. 34-40018 (May 21, 1998) (the "1998 Release").

² <http://www.hhs.gov/news/press/2013pres/05/20130522a.html>

³ <http://www.hhs.gov/news/press/2013pres/05/20130522a.html>
<http://www.bloomberg.com/news/2015-11-20/nsa-spying-risks-35-billion-in-u-s-technology-sales.html>

Privacy and Data Security as a Public Policy Issue

Digital technologies and the Internet offer enormous opportunities, but as they have become embedded in nearly every aspect of our lives, they also carry substantial risk to our society as a whole, and to each of us that participates in the digital economy.

Privacy and data security have become the focus of national and international discussion and debate, addressed as top-level priorities by heads-of-government and legislatures around the world. They are also the focus of national and international lobbying campaigns, investigation by numerous non-governmental organizations, and an extraordinary amount of media attention.

The disclosures in 2013 of extensive surveillance programs by the U.S. National Security Agency and other government agencies have triggered unprecedented attention to the issues of privacy and data security. By one estimate, disclosures of spying abroad may cost U.S. companies as much as \$35 billion in lost revenue through 2016 because of doubts about the security of information on their systems.³

Target, one of America's largest retail chains, disclosed breaches that are believed to have exposed personal data of as many as 110 million customers, more than a third of the population of the United States. At a hearing on the incident, Senator Patrick Leahy, chair of the Senate Judiciary Committee, said if consumers cannot trust businesses to keep their data secure, "our economic recovery is going to falter."⁴

In February 2013, President Obama declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cybersecurity."⁵

The Securities and Exchange Commission Division of Corporation Finance recognized the importance and arrival of this issue in 2011 by issuing cybersecurity disclosure guidance. The guidance noted in its preamble:

In general, cyber incidents can result from deliberate attacks or unintentional events. We have observed an increased level of attention focused on cyber attacks that include, but are not limited to, gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption. Cyber attacks may also be carried out in a manner that does not require gaining unauthorized access, such as by causing denial-of-service attacks on websites. Cyber attacks may be carried out by third parties or insiders using techniques that range from highly sophisticated efforts to

³ <http://www.bloomberg.com/news/2013-11-26/nsa-spying-risks-35-billion-in-u-s-technology-sales.html>

⁴ <http://www.nytimes.com/2014/02/05/business/target-to-speed-adoption-of-european-anti-fraud-technology.html?hpw&ref=technology>

⁵ <http://www.whitehouse.gov/cybersecurity>

electronically circumvent network security or overwhelm websites to more traditional intelligence gathering and social engineering aimed at obtaining information necessary to gain access.

The objectives of cyber attacks vary widely and may include theft of financial assets, intellectual property, or other sensitive information belonging to registrants, their customers, or other business partners. Cyber attacks may also be directed at disrupting the operations of registrants or their business partners.⁶

The Debate in Washington

In February 2012, for example, the Obama Administration unveiled a “Consumer Privacy Bill of Rights”⁷ as part of a “comprehensive blueprint to protect individual privacy rights and give users more control over how their information is handled.” The administration said the initiative “seeks to protect all Americans from having their information misused by giving users new legal and technical tools to safeguard their privacy.”

President Obama said⁸:

In just the last decade, the Internet has enabled a renewal of direct political engagement by citizens around the globe and an explosion of commerce and innovation creating jobs of the future. Much of this innovation is enabled by novel uses of personal information. So, it is incumbent on us to do what we have done throughout history: apply our timeless privacy values to the new technologies and circumstances of our times.

Privacy and data security have attracted significant attention from leaders of the U.S. Congress. On January 2, 2014, House Majority Leader Eric Cantor, citing recent high profile data breaches at Target and other companies, specifically expressed concerns over security of health care data. Mr. Cantor noted that four separate House Committees (Science, Homeland Security, Energy & Commerce, and Oversight & Government Reform) have recently investigated the risks of data breaches in online exchanges.⁹

In January 2014, Sen. Patrick Leahy re-introduced a Senate bill to set one nationwide standard for data breach notification—presently, 46 states have their own data breach notification laws—and mandate that consumers be told when their personal information has been compromised.¹⁰

⁶ CF Disclosure Guidance: Topic No. 2, Cybersecurity, October 13, 2011.

⁷ <http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b>

⁸ <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>

⁹ <http://majorityleader.gov/blog/2014/01/memo-legislation-on-data-breaches-and-obamacare.html>

¹⁰ <http://blogs.wsi.com/riskandcompliance/2014/01/08/personal-data-privacy-bill-re-introduced-in-congress/>

A front page New York Times story (“As Hacking Against U.S. Rises, Experts Try to Pin Down Motive”¹¹) reported that “corporate America is caught between what it sees as two different nightmares – preventing a crippling attack that brings down America’s most critical systems, and preventing Congress from mandating that the private sector spend billions of dollars protecting against the risk.”

Privacy and Data Security in Healthcare – The Public Debate

Privacy and data security are critical to delivering good health care. According to the Office of the National Coordinator for Health Information Technology:

Ensuring privacy and security of health information, including information in electronic health records (EHR), is the key component to building the trust required to realize the potential benefits of electronic health information exchange. If individuals and other participants in a network lack trust in electronic exchange of information due to perceived or actual risks to electronic health information or the accuracy and completeness of such information, it may affect their willingness to disclose necessary health information and could have life-threatening consequences.¹²

Patient advocacy organizations emphasize that since their introduction, electronic health records have dramatically altered patient perspectives on privacy and data security. The Privacy Rights Clearinghouse, a nonprofit organization, explains:

Today you have more reason than ever to care about the privacy of your medical information. Intimate details you revealed in confidence to your doctor were once stored in locked file cabinets and on dusty shelves in the medical records department.

Now, sensitive information about your physical and mental health will almost certainly end up in data files. Your records may be seen by hundreds of strangers who work in health care, the insurance industry, and a host of businesses associated with medical organizations. What's worse, your private medical information is now a valuable commodity for marketers who want to sell you something.¹³

Contrary to the Company’s assertion that privacy and data security are ordinary business, academic research points to the complicated policy implications that have arisen since the introduction of EHRs in the last several years. A 2012 study of EHRs by researchers at the University of Nebraska concluded:

¹¹ <http://www.nytimes.com/2013/03/04/us/us-weighs-risks-and-motives-of-hacking-by-china-or-iran.html?hpw>

¹² <http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf>

¹³ <https://www.privacyrights.org/HIPAA-basics-medical-privacy-electronic-age>

While the implementation of electronic health records in the United States will take place primarily in private settings, the adoption of EHRs has implications for both public and private health administrators. That is, it will likely take considerable government involvement to ensure that technology systems are functional across providers and to help guarantee that information is shared across providers in a secure manner. **These realities, in conjunction with public opinion polls that show security is a primary concern of the public in the development of EHRs suggest that this responsibility may be a critical one for governments across the U.S. and around the world as EHRs become more prevalent.**¹⁴ [Proponent's emphasis.]

A July 2012 survey of healthcare consumers found demonstrable evidence that Americans are deeply concerned about the implementation of EHRs:

Worries about the security of personal information continue to blunt public acceptance of electronic health record (EHR) systems now used by more than half of the nation's office-based physicians, according to a survey conducted by Harris Interactive for Xerox.

Sixty-three percent of Americans fear that a computer hacker will steal their personal data, down just 1 percentage point from 2010...

Overall, the percentage of Americans with some kind of EHR anxiety rose from 83% to 85% over this time frame, according to the survey, which was published last month.¹⁵

This new digitization of the healthcare industry attracted the attention of *The Wall Street Journal*, which reported on looming problems in a May 2013 article under the headline, "Poor Prognosis for Privacy."

The sharing of Americans' health information is set to explode in coming years, with millions of patients' medical records converted to electronic form and analyzed by health-care providers, insurers, regulators and researchers.

That has prompted concerns over privacy—and now, new federal rules that aim to give patients more control over their information are posing technical and administrative problems for the doctors and hospitals that have to implement them. Information-technology experts say the challenges illustrate how difficult it may be to protect sensitive patient information as digitization of the health-care industry expands.¹⁶

¹⁴ <http://ppc.unl.edu/userfiles/file/Documents/staffpubs/Herian,%20Shank%20AbdelMonem-Trust%20and%20EHRs.pdf>

¹⁵ <http://www.medscape.com/viewarticle/769778>

¹⁶ <http://online.wsj.com/news/articles/SB10001424127887323798104578454793056230984>

BusinessWeek reported:

As hospitals shift to digital medical records, administrators promise patients better care and shorter waits. They often neglect to mention that they share files with state health agencies, which in turn sell the information to private data-mining companies. The records are stripped of names and addresses, and there's no evidence that data miners are doing the legwork to identify individual patients. Yet the records often contain patients' ages, Zip Codes, and treatment dates—enough metadata for an inquiring mind to match names to files or for aggressive companies to target ads or hike insurance premiums.¹⁷

These concerns have been amplified in the explosion of media coverage surrounding implementation of the Affordable Care Act. Commentators on all sides of the political debate have weighed in with concerns about privacy:

The privacy issues associated with the bungled Obamacare website roll out may bode ill for physicians and healthcare providers who participate in the expansion of the federal government's Electronic Medical Records (EMR) collection.

"Eventually the goal is to have all of these electronic systems connected. In that way, it's good because in theory, you could be anywhere and get someone's medical records," Dr. Jeffrey A. Singer, Arizona surgeon and adjunct scholar at Washington, D.C.'s Cato Institute, told Newsmax. "You could be traveling and somehow end up in an ER in a faraway place."

"But if all your information is kept up in a cloud, how safe is it?" Singer said.

Singer said he fears that personal data could be used politically, recalling breaches that have occurred with the Internal Revenue Service going after political opponents of the Obama administration.¹⁸

The Washington Post reported: "As more doctors and hospitals go digital with medical records, the size and frequency of data breaches are alarming privacy advocates and public health officials."¹⁹

Indeed, a February 2014 healthcare industry survey found that security breaches, data loss, and unplanned outages cost U.S. hospitals more than \$1.6 billion annually. Nearly one in five (19 percent) global healthcare organizations has experienced a security breach in the last 12 months at a cost of \$810,189 per incident, according to the survey.²⁰

¹⁷ <http://www.businessweek.com/articles/2013-08-08/your-medical-records-are-for-sale>

¹⁸ <http://www.newsmax.com/Newsfront/obamacare-medical-records-privacy/2013/11/08/id/535604>

¹⁹ http://www.washingtonpost.com/national/health-science/medical-data-breaches-raise-alarms/2012/06/02/gIQAVPWt9U_story.html

²⁰ <http://www.businesswire.com/news/home/20140203005353/en/82-Percent-Health-Executives-Report-Organizations-Prepared#.Uv0dRvidWSq>

The Ponemon Institute reports in its "Third Annual Patient Privacy & Data Security Study" released December 2012, that "healthcare organizations seem to face an uphill battle in their efforts to stop and reduce the loss or theft of protected health information (PHI) or patient information" and most health systems are likely to "experience a data breach of some kind." The study found that 94 percent of healthcare organizations experienced at least one breach in the past two years and 45 percent dealt with more than five in the same period. The study documents the "severe economic consequences," with the average cost of a data breach rising to \$2.4 million over the last two years. Other key findings acknowledge the risks to patients as study "respondents acknowledge the harms to patients if their records are lost or stolen." "Seventy percent of respondents say there is an increased risk that personal health facts will be disclosed if the records are stolen or lost. This is followed by the risk of financial identity theft and medical identity theft (61 percent and 59 percent, respectively)."²¹

A December 2013 report by Experian, the credit rating agency, noted that the number of data breaches both experienced and reported by all companies is expected to continue to rise, with "all signs pointing to 2014 being a critical year for companies to better prepare to respond to security incidents and data breaches." With regard to the health care industry, the Experian report stated:

***Healthcare Breaches: Opening the Floodgates* - With the addition of the Healthcare Insurance Exchanges, millions of individuals will be introduced into the healthcare system and in return increase the vulnerability of the already susceptible healthcare industry. When combined with new HIPAA data breach compliance rules taking shape, the healthcare industry is likely to make the most breach headlines in 2014. [Proponent's emphasis.]**

Non-governmental Organizations

Failure to provide patients with assurances of privacy and data security can have tragic impact, according to Dr. Deborah Peel, founder of the nonprofit organization Patient Privacy Rights. She told *The Wall Street Journal* "the effect that this has on patients, when there's no privacy, is (that) millions delay and avoid treatment for cancer, depression and sexually transmitted diseases because they know the information isn't private."²²

Indeed, The Center for Democracy and Technology concluded:

Patients who mistrust whether their information will be handled confidentially will not fully participate in their own health care. Without appropriate protections for privacy and security in the healthcare system, people will engage in "privacy-

²¹ <http://www.ponemon.org/library/third-annual-patient-privacy-data-security-study>

²² <http://blogs.wsj.com/experts/2013/11/18/video-do-electronic-medical-records-threaten-patient-privacy/?KEYWORDS=privacy>

protective" behaviors to avoid having their personal health information used inappropriately.

Threat of New Regulation

While there is enormous potential in EHRs, failure to provide assurances of privacy could result in the risk of new regulation. According to a 2011 report by the McKinsey Global Institute:

The sensitive nature of health information, and the potential for discrimination based on it, makes security and privacy rights protection critical. Many countries have regulations such as HIPAA and HITECH, the US laws designed to protect the security and privacy of health records. As using big data becomes more important to the industry, policy makers may have to reevaluate these laws or intervene to ensure that access to data is available in a safe and secure way that also enables health care outcomes to be optimized.²³ [Proponent's emphasis.]

Privacy and data security have attracted attention from state regulators, legislators and law enforcement. California Attorney General Kamala D. Harris recently issued best practice recommendations for providers -- and tips for patients -- to better safeguard health data from theft. "Medical identity theft has been called the privacy crime that can kill," she said. "As the Affordable Care Act encourages the move to electronic medical records, the healthcare industry has an opportunity to improve public health and combat medical identity theft with forward-looking policies and the strategic use of technology."²⁴

The Nexus to Cerner

As a leader in the field of electronic health records, Cerner is at the center of the extensive debate regarding privacy and data security in healthcare. There is a clear nexus between the issue and the Company specifically.

A particular concern is Cerner's ambitious efforts to use patient data in ways that could threaten patient privacy. According to a published report and internal company marketing material, Cerner is reportedly "leveraging" billions of patient records it has at its disposal as marketable information to pharmaceutical companies and researchers. In 2010 The Kansas City Business Journal reported:

Cerner Corp. is looking for big things from what is now a small corner of its business.

The North Kansas City-based health care information technology company, known mostly for the health-record software sold to hospitals and clinics, is leveraging the

²³http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation

²⁴ <http://www.healthcareitnews.com/news/locking-down-chrs-medical-id-theft>

billions of anonymous patient records it has at its disposal as marketable information to pharmaceutical companies and researchers.

Cerner said the data operation is a big reason revenue for its LifeSciences Group has increased by roughly 20 percent during each of the past five years.

Mark Hoffman, the company's life sciences solutions vice president, predicted that annual growth will be greater still in the future...

"This is just the beginning for us in the life sciences," he said.

Included in Cerner's data warehouse are 1.2 billion lab results. It also has smaller numbers of medication orders and other data...

Cerner President Trace Devanny said in a statement that although the LifeSciences Group is a "minor contributor to our bottom line," the company views it as a "key component of our long-term global growth strategy."²⁵

The *New York Times* reported in 2009 in "*When 2+2 Equals a Privacy Question:*"

Big players like the Cerner Corporation, which maintains electronic health systems for 8,000 clients, including large hospitals and retail clinics, and smaller players like Practice Fusion, which offers its Web-based health record systems free to health care providers, say they make use of patient data collected from their clients.

A spokeswoman for Cerner, whose Web site promotes its "data mining of our vast warehouse of electronic health records," said the company shares de-identified patient data with researchers or drug companies looking for patients to participate in clinical trials. The patient records are "double scrubbed," she said, explaining that the company removes personal data like names and addresses before it runs a search using a numbered code for each patient.²⁶

While Cerner says these records are anonymized, there is substantial scientific question as to whether data can be adequately de-identified. After studying the issue in the context of healthcare records, the Center for Democracy and Technology concluded: "No record of personal information can be truly de-identified to the point where there is no risk of becoming identifiable."²⁷

These issues are especially troublesome as Cerner works to "ease barriers preventing doctors and doctors and hospitals from sharing data." Cerner is acting as a leader in an initiative by five electronic health records companies to form a nonprofit group aimed at

²⁵ <http://www.bizjournals.com/kansascity/stories/2009/06/01/story5.html?page=all>

²⁶ <http://www.nytimes.com/2009/10/18/business/18stream.html>

²⁷ <https://www.cdt.org/blogs/devan-mcgraw/2108better-policies-de-identified-health-data>

setting standards for exchanging data across their systems.²⁸ The Ponemon Institute reports that “concerns about the security of Health Information Exchanges (HIE) are keeping organizations from joining.” In their 2012 study they found “66 percent of respondents say they are only somewhat confident (30 percent) or not confident (36 percent) in the security and privacy of patient data on HIEs.” Ensuring privacy and data security is therefore of critical concern.²⁹

Privacy and data security present very real potential risks for Cerner. Yet, Proponent notes, the terms “privacy” and “data security” are not even mentioned in the charter of any of the company’s Board committees: the Audit Committee; Compensation Committee; Nominating, Governance and Policy Committee; or the Corporate Governance Committee.; resulting in opacity when investors seek to understand and ensure adequate oversight.

Further, Cerner has not appointed a Chief Privacy Officer, best practice among peers such as AthenaHealth, Inc. and WebMD Health Corp. The existence of a Chief Privacy Officer indicates executive level management of this critical issue.

Cerner has also engaged in strong lobbying efforts, indicating the issues at hand are not simply ordinary business, but a social policy issue.

The *New York Times* reports:

As doctors and hospitals struggle to make new digital health records systems work, the clear winners are big companies like Allscripts that lobbied for that legislation and pushed aside smaller competitors...

While proponent say new record-keeping technologies will one day reduce costs and improve care, profits and sales are soaring now across the records industry.... At Cerner Corp. of Kansas City, Mo., sales rose 60 percent during that period.

Cerner’s lobbying dollars doubled to nearly \$400,000 between 2006 and last year, according to the Center for Responsive Politics.

Current and former industry executives say that big digital records companies like Cerner, Allscripts and Epic Systems of Verona, Wis., have reaped enormous rewards because of the legislation they pushed for. “Nothing that these companies did in my eyes was spectacular,” said John Gomez, the former head of technology at Allscripts. “They grew as a result of government incentives.”³⁰

²⁸ <http://www.bloomberg.com/news/2013-03-04/cerner-mckesson-lead-alliance-to-let-doctors-share-data.html>

²⁹ <http://www.ponemon.org/library/third-annual-patient-privacy-data-security-study>

³⁰ <http://bits.blogs.nytimes.com/2013/02/20/daily-report-health-data-swells-profits-in-an-industry/?ref=cernercorporation>

The forgoing illustrates the strong nexus between the Company and the social policy debate.

II. The Proposal Does Not Seek To Micro-manage the Company

What's clear is that privacy and data security are, and will continue to be, critical and consistent issues of public policy debate for many years to come. This is particularly true of the healthcare industry. Investors have every reason to be concerned and involved regarding privacy and data security – not on a day-to-day operational level, but by seeking transparent board-level oversight to ensure privacy and data security risks to the Company and society are adequately addressed. Yet, it is unclear to investors how the Company's Board of Directors is overseeing the relevant risks and heading off a digital disaster that could affect the privacy, and perhaps the health, of millions of people. Thus, the current Proposal seeks to create transparency regarding that oversight process.

The Proposal seeks top-level information about how the Board is managing the issues of privacy and data security and their considerable risks to the Company. The current oversight of these issues at the Company is unclear and insufficiently transparent, in the opinion of the Proponent. As stated in the supporting statement: We emphasize that the Proposal is not asking the Company to disclose risks, specific incidents, or legal compliance procedures; rather, we believe, investors need to understand more fully how the Board oversees the concerns described above.

The SEC explained in the 1998 Release that proposals are not permitted to seek “to ‘micro-manage’ the company by probing too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment.” Such micro-management may occur where the proposal “seeks intricate detail, or seeks specific time-frames or methods for implementing complex policies.” However, “timing questions, for instance, could involve significant policy where large differences are at stake, and proposals may seek a reasonable level of detail without running afoul of these considerations.”

While the Company does not make a micro-management argument, we would like to take this opportunity to point out that the proposal is not seeking any intricate details, nor does it seek to implement complex policies. As demonstrated above, the issue has entered the mainstream media, such that it does not constitute a complex issue that is beyond the ability of shareholders to understand or make decisions about with respect to how to vote on the Proposal.

For all the reasons submitted above, we maintain that the Company has not met its burden of persuasion that the Proposal relates simply to the Company's Ordinary Business and does not raise a significant policy issue.

Conclusion

In conclusion, we respectfully request the Staff to inform the Company that Rule 14a-8 requires a denial of the Company's no-action request. As demonstrated above, the Proposal is not excludable under Rule 14a-8. In the event that the Staff should decide to concur with the Company and issue a no-action letter, we respectfully request the opportunity to speak with the Staff in advance.

Please contact me at (978) 578-4123 or natasha@arjuna-capital.com with any questions in connection with this matter, or if the Staff wishes any further information.

Sincerely,



Natasha Lamb
Director of Equity Research & Shareholder Engagement
Arjuna Capital

cc: Craig Evans via email at craig.evans@stinsonleonard.com
Office of Chief Counsel
Stinson Leonard Street

Randy Sims via e-mail at rsims@cerner.com
Chief Legal Officer and Secretary
Cerner Corporation

Attachment A

Patient Privacy and Data Security

Whereas, Patient trust is critical for an effective and efficient healthcare system, Electronic Health Record (EHR) security breaches are accelerating, patient records are sold, and patients report privacy concerns may delay necessary care.

According to the Office of the National Coordinator for Health Information Technology:

“Ensuring privacy and security of health information...is the key component to building the trust required to realize the potential benefits of electronic health information exchange.”

Perceived or actual privacy risks “may affect [patient] willingness to disclose necessary health information and could have life-threatening consequences.”

According to the Center for Democracy and Technology (CDT) a recent survey found 80 percent of respondents expressed concerns about identity theft or fraud; and 56 and 55 percent about employer and insurer access, respectively:

“Patients who mistrust whether their information will be handled confidentially will not fully participate in their own health care. Without appropriate protections for privacy and security in the healthcare system, people will engage in ‘privacy-protective’ behaviors to avoid having their personal health information used inappropriately.”

Privacy-protective behaviors include delaying care and asking providers to omit information from records. A 2011 New London Consulting study found 27.1 percent of respondents may withhold information and 27.6 percent may postpone care.

In 2013, The Wall Street Journal reported on the difficulty of protecting patient privacy in EHR (“Poor Prognosis for Privacy”) and hosted an expert panel on EHR and privacy highlighting privacy-protective behavior and data use concerns.

Breaches of privacy and data security are growing. A 2012 HIMSS Analytics and Kroll Advisory Solutions survey of healthcare organizations found 27 percent experienced a security breach in 2011, versus 19 percent in 2010, and 13 percent in 2008.

Collection, disclosure, or misuse of personal information can cause great harm to individuals and society - including discrimination, identity theft, financial loss, loss of business or employment opportunities, humiliation, reputational damage, or physical harm including delayed care.

Further, the CDT reports 77 percent of Americans are concerned about their medical information being used for marketing purposes.

Published reports indicate Cerner is “leveraging” billions of patient records as marketable information. Data sales have led to substantial revenue growth, according to Company vice president Mark Hoffman who stated, “This is just the beginning for us in the life sciences.” There is substantial scientific question as to whether data can be adequately de-identified.

We believe Cerner's Board has a fiduciary and social duty to protect company assets, including the personal information of customers. Risks include privacy breaches, litigation, and a loss in brand value and revenue opportunities.

Resolved, shareholders request that the Board of Directors publish a report, at reasonable expense and excluding confidential or proprietary information, explaining how the Board is overseeing privacy and data security risks.

Supporting Statement: It should be emphasized that the Proposal is not asking the Company to disclose risks, specific incidents, or legal compliance procedures, but rather, we believe investors need to understand more fully how the Board is overseeing these concerns.



Craig L. Evans
816.691.3186 **DIRECT**
816.412.1129 **DIRECT FAX**
craig.evans@stinsonleonard.com

January 17, 2014

Via electronic mail (shareholderproposals@sec.gov)

U.S. Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
100 F Street, N.E.
Washington, D.C. 20549

Re: Cerner Corporation
Shareholder Proposal of Steven Schewel
Exchange Act of 1934 – Rule 14a-8

Ladies and Gentlemen:

Pursuant to Rule 14a-8(j) under the Securities Exchange Act of 1934, as amended, we are writing on behalf of our client, Cerner Corporation, a Delaware corporation (the "Company"), to request that the Staff of the Division of Corporation Finance (the "Staff") of the Securities and Exchange Commission (the "Commission") concur with the Company's view that, for the reasons stated below, it may exclude the shareholder proposal and supporting statement (the "Shareholder Proposal") submitted by Steven Schewel ("Mr. Schewel", and together with his designated proxy Natasha Lamb of Arjuna Capital/Baldwin Brothers Inc. referred to herein as the "Proponent"), on December 13, 2013 for inclusion in the proxy materials that the Company intends to distribute in connection with its 2014 Annual Meeting of Shareholders (the "2014 Proxy Materials").

Pursuant to Rule 14a-8(j), this letter is being filed with the Commission no later than 80 days prior to the date on which the Company intends to file its definitive 2014 Proxy Materials. In accordance with *Staff Legal Bulletin No. 14D* (Nov. 7, 2008), we are submitting this letter via electronic mail to the Staff in lieu of mailing paper copies. Also pursuant to Rule 14a-8(j), a copy of this submission is being sent simultaneously to the Proponent as notice of the Company's intention to exclude the Shareholder Proposal from its 2014 Proxy Materials.

THE SHAREHOLDER PROPOSAL

The Shareholder Proposal states in relevant part:

Resolved, shareholders request that the Board of Directors publish a report, at reasonable expense and excluding confidential or proprietary information, explaining how the Board is overseeing privacy and data security risks.

A copy of the Shareholder Proposal and all related correspondence with the Proponent is attached to this letter as Exhibit A.

BASIS FOR EXCLUSION

As discussed more fully below, we have advised the Company that the Shareholder Proposal may be properly omitted from the 2014 Proxy Materials pursuant to Rule 14a-8(i)(7), which permits a company to exclude proposals relating to the Company's "ordinary business operations."

ANALYSIS

The Proposal May Be Excluded Under Rule 14a-8(i)(7) Because The Proposal Relates To Matters Of The Company's Ordinary Business Operations And Does Not Raise A Significant Policy Issue.

The Company may exclude the Shareholder Proposal under Rule 14a-8(i)(7) because the Shareholder Proposal resembles other customer information and privacy proposals that the Staff has previously found excludable; the Shareholder Proposal's treatment of health information relates to the Company's product development; and the subject matter of the Shareholder Proposal does not raise significant policy issues. Rule 14a-8(i)(7) allows a company to omit shareholder proposals that deal "with a matter relating to the company's ordinary business operations." According to Exchange Act Release No. 40018 (May 21, 1998) (the "1998 Release"), the policy behind the ordinary business exclusion is consistent with the corporate law concept of managerial flexibility and seeks "to confine the resolution of ordinary business problems to management and the board of directors, since it is impracticable for shareholders to decide how to solve such problems at an annual shareholders meeting."

The 1998 Release identifies two central considerations under the ordinary business exclusion. The relevant consideration here relates to the proposal's subject matter, where "[c]ertain tasks are so fundamental to management's ability to run a company on a day-to-day basis that they could not, as a practical matter, be subject to direct shareholder oversight." *Id.* Shareholder proposals related to such tasks are excludable absent a focus on social policy issues that are "so significant" as to "transcend the day-to-day business matters" of the company. *Id.* Where the shareholder proposal involves the preparation of a report or

a proposal related to a company's risks, the Staff has stated it will look to whether the report's underlying subject matter concerns an ordinary business issue of the company. *Staff Legal Bulletin No. 14E* (Oct 27, 2009) ("Bulletin No. 14E"). If the ordinary business exclusion is met and is not transcended by a significant policy issue, then the proposal will be excludable under Rule 14a-8(i)(7).

The Staff has consistently agreed that privacy and customer information proposals can be omitted from a company's proxy statements under the ordinary business exclusion. For example, a series of recent No-Action Letters have allowed technology companies to exclude shareholder proposals dealing with privacy and customer information. In *Comcast Corp.* (avail. Mar. 4, 2009), the company sought to exclude a shareholder proposal that requested a report on "the effects of the company's Internet network management practices in the context of the significant public policy concerns regarding the public's expectations of privacy...on the Internet." Comcast argued that the shareholder proposal should be omitted under the ordinary business exclusion because proper oversight of management practices required an intimate knowledge of the company's management tools and techniques as well as a detailed understanding of "network architectures, business practices, and available network technology," neither of which shareholders of a public company were reasonably expected to possess. The Staff agreed with Comcast and found that shareholder proposals relating to "procedures for protecting user information" could be omitted as an ordinary business matter. Using the same rationale, the Staff in *Qwest Communication International Inc.* (Feb. 17, 2009); *Verizon Communications Inc.* (avail. Feb. 13, 2009); and *AT&T Inc.* (avail. Jan. 26, 2009, recon. denied Feb. 27, 2009) found that it was appropriate to exclude similar shareholder proposals concerning digital privacy. Again, in *Bank of America Corp.* (avail. Feb. 21, 2006), the Staff concurred in excluding a proposal that requested a report on the company's "policies and procedures for ensuring that all personal and private information pertaining to all Bank of America customers will remain confidential in all business operations" on the basis that "the procedures for protecting customer information" constituted ordinary business operations.

Here, Mr. Schewel's Shareholder Proposal regarding "privacy and data security risks" relates directly to "the procedures for protecting customer information." The Company is in the business of providing health care information technology solutions—including electronic health record systems—to health care organizations ranging from small individual clinics to large multi-hospital systems. Clients use the Company's products and systems to collect, store and access patient medical information at the appropriate point of care. From a technical perspective, clients generally store patient records in one of two ways. One method is by licensing the Company's software and storing medical information on the client's own systems. In those instances, the Company will work closely with the client to deploy appropriate safeguards in order to secure client information. The second method is for the Company to provide a hosting service where client information is stored in the Company's data centers. The procedures the Company uses to secure hosted client information are highly technical and include safeguards such as a multi-layered security architecture designed to prevent unauthorized access, the deployment of advanced security software and controls for ensuring compliance, and specialized training programs

that help employees maintain an expertise in information security. Considering the Company's business is predicated upon its ability to secure both client-stored and hosted client information, any report on customer privacy and data security is inextricably linked to the Company's procedures for protecting customer information and ought to be excluded under Rule 14a-8(i)(7).

Furthermore, Board oversight of privacy and data security is a fundamental aspect of the Company's day-to-day operations because data privacy lies at the heart of health care information technology. For the reasons mentioned above, the Company's business inherently involves protecting and hosting patient medical information for Company clients. Ensuring the integrity, privacy and security of this information is a central part of the day-to-day management and oversight of the Company's business. Proper oversight requires regular and ongoing interaction between the Board, management and skilled company employees who are experts in Company privacy controls and data security systems. Appropriate oversight also requires Company directors, officers and managers who are able to respond promptly and knowledgeably in the event of an emerging security concern. Given the specialized nature of privacy and data security, the dynamic nature of electronic security, and the importance of data security to the Company's overall business, oversight of such operations, as a practical matter, is fundamental to the Company's daily operations and cannot be effectively regulated by shareholder oversight.

Additionally, the Staff has allowed companies to exclude proposals relating to a company's product development. For example, in *DENTSPLY Int'l. Inc.* (avail. Mar. 21, 2013), a shareholder proposed that the company issue a report summarizing how the company plans to reduce environmental impacts by phasing out mercury from the company's products. The company argued the proposal related to its product research, development and content, which was nothing more than the company's ordinary business operations. The Staff agreed, finding that "[p]roposals concerning product development are generally excludable under rule 14a-8(i)(7)." Again, in *Applied Digital Solutions, Inc.* (avail. Apr 25, 2006) the Staff agreed that a shareholder proposal that asked the company's independent directors to issue a report "on the harm the continued sale and use of RFID chips could have on the public's privacy, personal safety and financial security" could be excluded because the sale and use of RFID chips amounted to product development, which is an ordinary business operation.

In the present case, the Company's ability to develop innovative products is fundamental to the Company's ordinary business operations. As a health care information technology company, the Company's product development initiatives reasonably include research into new methods of securing client information and new systems capable of analyzing public health trends using blinded patient information. Mr. Schewel's claim that the Company "is 'leveraging' billions of patient records as marketable information," even if it were accurate, relates directly to the Company's efforts to develop innovative products. Since the Staff has previously agreed that proposals related to product development can be omitted under the ordinary business exclusion, Mr. Schewel's Shareholder Proposal concerning such products should similarly be excluded.

Finally, the Shareholder Proposal does not raise a significant policy issue that would transcend the Company's day-to-day business matters. Even when considering matters of company risk and customer privacy, the Staff has consistently agreed that such issues do not rise to the level of a significant policy issue. In *Sempra Energy* (avail. Jan. 12, 2012, recon. denied Jan. 23, 2012), the Staff agreed that a shareholder proposal urging the board to conduct a review and publish an annual report on the company's "management of political, legal, and financial risks posed by Sempra operations in 'any country that may pose an elevated risk of corrupt practices'" could be omitted because "the underlying subject matter of these risks appears to involve ordinary business matters." The result was similar in *The Western Union Co.* (avail. Mar. 14, 2011), where the Staff concurred that a shareholder proposal asking the board to establish a risk committee to monitor and report on the company's potential risk exposures could be omitted because "the underlying subject matters of these risks appear to involve ordinary business matters." Additionally, as mentioned above, proposals addressing customer information and privacy have widely been found to not transcend a company's day-to-day operations.

The Proponent's Shareholder Proposal does not transcend the Company's daily business operations because the Shareholder Proposal deals only with the mechanical aspects of company risks and customer privacy. The question of "how the Board is overseeing privacy and data security risks," though important, is a technical issue rather than policy-based question. The Board's involvement in data and privacy matters is focused on the electronic systems responsible for maintaining data integrity and the employees tasked with managing and improving such systems, both of which may be difficult for shareholders to comprehend and regulate appropriately. The Commission appears to share this perspective. In the Division of Corporation Finance's Disclosure Guidance: Topic No. 2 (Cybersecurity) (Oct. 13, 2011) ("Disclosure"), the Commission tackles the security risks of digital technologies and advises companies to monitor and disclose such risks in the same way as "other operational and financial risks...." The similar treatment of digital, financial, and operational risks suggests that these challenges ought to be viewed comparably. Since operational and financial risks have traditionally been considered a part of a company's day-to-day business operations, the same treatment should be extended to electronic risks. Given the technical nature of the Board's involvement with privacy and security issues, and the Disclosure's similar treatment of digital, financial, and operational risks, Mr. Schewel's Shareholder Proposal addressing privacy and data security should be excludable under Rule 14a-8(i)(7).

CONCLUSION

Based upon the foregoing analysis, we respectfully request that the Staff concur that it will take no action if the Company excludes the Shareholder Proposal from its 2014 Proxy Materials. Should the Staff disagree with the conclusions set forth in this letter, or should any additional information be desired in support of the Company's position, we would appreciate the opportunity to confer with the Staff concerning these matters prior to the issuance of the Staff's response. Please do not hesitate to contact the undersigned attorney at (816) 691-3186.

U.S. Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
January 17, 2014
Page 6

Sincerely,

Stinson Leonard Street LLP

A handwritten signature in black ink that reads "Craig L. Evans". The signature is written in a cursive style with a large initial "C".

Craig L. Evans

CLE:WC

cc: Natasha Lamb, Director of Equity Research & Shareholder Engagement —
Arjuna Capital/Baldwin Brothers Inc. (as proxy for Steven Schewel)
Randy Sims, Senior Vice President, Chief Legal Officer and Secretary —
Cerner Corporation

Exhibit A

(see attached)

ARJUNA CAPITAL
ENLIGHTENED ENGAGEMENT IN THE CAPITAL MARKETS

December 11th, 2013

Corporate Secretary
Cerner Corporation
2800 Rockcreek Parkway
North Kansas City, Missouri 64117
(816) 221-1024

Dear Corporate Secretary:

Arjuna Capital is the sustainable wealth management platform of Baldwin Brothers, Inc., an investment firm based in Marion, MA.

I am hereby authorized to notify you of our intention to lead file the enclosed shareholder resolution with Cerner Corporation on behalf of our client Steven Matthew Schewel. Arjuna Capital/Baldwin Brothers Inc. submits this shareholder proposal for inclusion in the 2014 proxy statement, in accordance with Rule 14a-8 of the General Rules and Regulations of the Securities and Exchange Act of 1934 (17 C.F.R. § 240.14a-8). Per Rule 14a-8, Steven Matthew Schewel holds more than \$2,000 of CERN common stock, acquired more than one year prior to today's date and held continuously for that time. Our client will remain invested in this position continuously through the date of the 2014 annual meeting. Enclosed please find verification of the position and a letter from Steven Matthew Schewel authorizing Arjuna Capital/Baldwin Brothers Inc. to undertake this filing on his behalf. We will send a representative to the stockholders' meeting to move the shareholder proposal as required by the SEC rules.

We would welcome discussion with Cerner about the contents of our proposal.

Please direct any written communications to me at the address below or to natasha@arjuna-capital.com. Please also confirm receipt of this letter via email.

Sincerely,



Natasha Lamb
Director of Equity Research & Shareholder Engagement
Arjuna Capital/Baldwin Brothers Inc.
204 Spring Street Marion, MA 02738

Cc: Neal Patterson, Chair and Chief Executive Officer

Enclosures

Patient Privacy and Data Security

Whereas, Patient trust is critical for an effective and efficient healthcare system, Electronic Health Record (EHR) security breaches are accelerating, patient records are sold, and patients report privacy concerns may delay necessary care.

According to the Office of the National Coordinator for Health Information Technology:

“Ensuring privacy and security of health information...is the key component to building the trust required to realize the potential benefits of electronic health information exchange.”

Perceived or actual privacy risks “may affect [patient] willingness to disclose necessary health information and could have life-threatening consequences.”

According to the Center for Democracy and Technology (CDT) a recent survey found 80 percent of respondents expressed concerns about identity theft or fraud; and 56 and 55 percent about employer and insurer access, respectively:

“Patients who mistrust whether their information will be handled confidentially will not fully participate in their own health care. Without appropriate protections for privacy and security in the healthcare system, people will engage in ‘privacy-protective’ behaviors to avoid having their personal health information used inappropriately.”

Privacy-protective behaviors include delaying care and asking providers to omit information from records. A 2011 New London Consulting study found 27.1 percent of respondents may withhold information and 27.6 percent may postpone care.

In 2013, The Wall Street Journal reported on the difficulty of protecting patient privacy in EHR (“Poor Prognosis for Privacy”) and hosted an expert panel on EHR and privacy highlighting privacy-protective behavior and data use concerns.

Breaches of privacy and data security are growing. A 2012 HIMSS Analytics and Kroll Advisory Solutions survey of healthcare organizations found 27 percent experienced a security breach in 2011, versus 19 percent in 2010, and 13 percent in 2008.

Collection, disclosure, or misuse of personal information can cause great harm to individuals and society - including discrimination, identity theft, financial loss, loss of business or employment opportunities, humiliation, reputational damage, or physical harm including delayed care.

Further, the CDT reports 77 percent of Americans are concerned about their medical information being used for marketing purposes.

Published reports indicate Cerner is “leveraging” billions of patient records as marketable information. Data sales have led to substantial revenue growth, according to Company vice president Mark Hoffman who stated, “This is just the beginning for us in the life sciences.” There is substantial scientific question as to whether data can be adequately de-identified.

We believe Cerner's Board has a fiduciary and social duty to protect company assets, including the personal information of customers. Risks include privacy breaches, litigation, and a loss in brand value and revenue opportunities.

Resolved, shareholders request that the Board of Directors publish a report, at reasonable expense and excluding confidential or proprietary information, explaining how the Board is overseeing privacy and data security risks.

Supporting Statement: It should be emphasized that the Proposal is not asking the Company to disclose risks, specific incidents, or legal compliance procedures, but rather, we believe investors need to understand more fully how the Board is overseeing these concerns.

December 5th, 2013

Natasha Lamb
Director of Equity Research & Shareholder Engagement
Arjuna Capital/Baldwin Brothers Inc.
353 West Main Street
Durham, NC 27701

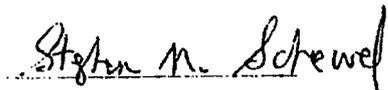
Dear Ms. Lamb,

I hereby authorize Arjuna Capital/Baldwin Brothers Inc. to file a shareholder proposal on my behalf at Cerner Corporation (CERN) regarding a Report on Privacy and Data Security.

I am the beneficial owner of more than \$2,000 worth of common stock in CERN that I have held continuously for more than one year. I intend to hold the aforementioned shares of stock through the date of the Company's annual meeting in 2014.

I specifically give Arjuna Capital/Baldwin Brothers Inc. full authority to deal, on my behalf, with any and all aspects of the aforementioned shareholder proposal. I understand that my name may appear on the Corporation's proxy statement as the filer of the aforementioned proposal.

Sincerely,

A handwritten signature in black ink that reads "Steve M. Schewel". The signature is written in a cursive style with a horizontal line underneath the name.

Steve Schewel

c/o Arjuna Capital/Baldwin Brothers Inc.
353 West Main Street
Durham, NC 27701

charles SCHWAB
ADVISOR SERVICES

1958 Summit Park Dr, Orlando, FL 32810

December 11th, 2013

Corporate Secretary
Cerner Corporation
2800 Rockcreek Parkway
North Kansas City, Missouri 64117

To WHOM IT MAY CONCERN:

Re: Stephen Matthew Schewel OMB Memorandum M-07-16***

This letter is to confirm that Charles Schwab & Co is the record holder for the beneficial owners of the account of above, which Arjuna Capital, the sustainable wealth management platform of Baldwin Brothers Inc. manages and which holds in the account ~~100 shares~~ 100 shares of common stock in Cerner Corporation (CERN).*

As of December 11th, Steve Schewel held, and has held continuously for at least one year, 100 shares of CERN stock.

This letter serves as confirmation that the account holder listed above is the beneficial owner of the above referenced stock.

Sincerely,



* 5/18/12: insert the date that the stock position was received by the custodian