No Act

P.E. 1/31/14

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

DIVISION OF
CORPORATION FINANCE

14005546



March 6, 2014

Act: 1934
Section:
Rule: 14a-8 (OPS)
Public
Availability: 3-6-14

Keir D. Gumbs
Covington & Burling LLP
kgumbs@cov.com

Re: UnitedHealth Group Incorporated

Dear Mr. Gumbs:

This is in regard to your letter dated March 5, 2014 concerning the shareholder proposal submitted by Arjuna Capital/Baldwin Brothers Inc. on behalf of Ann B. Alexander for inclusion in UnitedHealth's proxy materials for its upcoming annual meeting of security holders. Your letter indicates that the proponent has withdrawn the proposal and that UnitedHealth therefore withdraws its January 31, 2014 request for a no-action letter from the Division.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

COVINGTON & BURLING LLP

BEIJING BRUSSELS LONDON NEW YORK
SAN DIEGO SAN FRANCISCO SEOUL
SHANGHAI SILICON VALLEY WASHINGTON

KEIR D. GUMBS
1201 PENNSYLVANIA AVENUE, NW
WASHINGTON, DC 20004-2401
T 202.662.5500
kgumbs@cov.com

March 5, 2014

**BY ELECTRONIC MAIL TO SHAREHOLDERPROPOSALS@SEC.GOV**

Office of Chief Counsel
Division of Corporation Finance
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Re: UnitedHealth Group Incorporated – Withdrawal of No-Action Request Letter Regarding the Shareholder Proposal Submitted by Arjuna Capital on Behalf of Ann B. Alexander

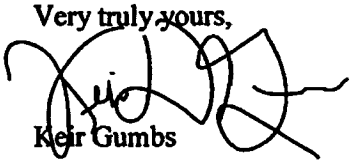
Ladies and Gentlemen:

By letter dated January 31, 2014, UnitedHealth Group Incorporated, a Minnesota corporation (the "Company"), submitted to the staff of the Division of Corporation Finance (the "Staff") a no-action request (the "No-Action Request Letter") relating to the Company's intention to exclude from its proxy materials for its 2014 Annual Meeting of Shareholders a shareholder proposal (the "Proposal") received by the Company on December 20, 2013 submitted by Arjuna Capital on behalf of Ann B. Alexander (the "Proponent").

Enclosed as Exhibit A is a letter from the Proponent, dated March 3, 2014, withdrawing the Proposal. In reliance on the letter from the Proponent and on behalf of the Company, we respectfully advise the Staff that we hereby withdraw the No-Action Request Letter.

If you have any questions or desire additional information, please contact the undersigned at (202) 662-5500 or Amy L. Schneider, Deputy General Counsel of the Company, at (952) 936-4986.

Very truly yours,



Keir Gumbs

Enclosure

cc: Ms. Amy L. Schneider
Ms. Natasha Lamb

**Exhibit A**

See attached

# Arjuna Capital

March 3, 2014

VIA E-MAIL TO amy.l.schneider@uhg.com

Amy L. Schneider
Deputy General Counsel
UnitedHealth Group Incorporated
9900 Bren Road East, MN008-T502
Minnetonka, MN 55343

Re: Shareholder Proposal for the 2014 Annual Meeting

This letter is being submitted by Arjuna Capital ("Arjuna Capital") on behalf of Ann B. Alexander (the "Proponent") with respect to a shareholder proposal (the "Proposal") submitted to UnitedHealth Group Incorporated (the "Company") by Arjuna Capital on behalf of the Proponent on December 20, 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 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,

Natasha Lamb
Director of Equity Research &
Shareholder Engagement

ARJUNA CAPITAL
ENLIGHTENED ENGAGEMENT IN THE CAPITAL MARKETS

December 20th, 2013

Dannette Smith
Secretary to the Board of Directors
UnitedHealth Group Center
9900 Bren Road East
Minnetonka, Minnesota 55343
952-936-1316
dannette.smith@UHG.com

Dear Ms. Smith:

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 UnitedHealth Group on behalf of our client Ann B. Alexander. 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, Ann B. Alexander holds more than $2,000 of UNH 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 Ann B. Alexander authorizing Arjuna Capital/Baldwin Brothers Inc. to undertake this filing on her 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 UnitedHealth Group 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: Stephen J. Hemsley, President 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 and patients report privacy concerns may delay necessary care.

According to the Office of the National Coordinator for Heath 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 EHR ("Poor Prognosis for Privacy") and hosted an expert panel highlighting privacy-protective behavior and data use concerns.

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

In 2013, Bloomberg reported UnitedHealth recalled software from hospital emergency departments in over 20 states, as an error caused patient prescriptions notes to disappear. Bloomberg highlighted six EHR software recalls since 2009 from Picis Inc., acquired by UnitedHealth 2010.

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.

A 2013 McKinsey report, "The big data revolution in healthcare," recommends "[p]romoting transparency as a cultural norm:"

> "Many executives believe that data transparency is just as likely to produce damaging consequences as new opportunities. But if leaders don't pursue transparency efforts, regulators or other external bodies may do so on their behalf – and not gently."

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

**Resolved,** shareholders request 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 the Proposal is not asking the Company to disclose risks, specific incidents, or legal compliance procedures, but rather, we believe investors need to understand how the Board is overseeing these concerns.

December 20th, 2013

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

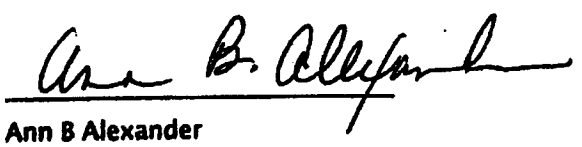
Dear Ms. Lamb,

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

I am the beneficial owner of more than $2,000 worth of common stock in UNH 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,



Ann B Alexander

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 20th, 2013

UnitedHealth Group Center
9900 Bren Road East
Minnetonka, Minnesota 55343
Attention: Secretary to the Board of Directors

To the Secretary to the the Board of Directors or WHOM IT MAY CONCERN:

Re: Ann B Alexander / Account 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 OMB Memorandum M-07-16 *** 50 shares of common stock in UnitedHealth Group Incorporated (UNH).*

As of December 20th, Ann B Alexander held, and has held continuously for at least one year, 50 shares of UNH stock.

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

Sincerely,

12/12/10: insert the date that the stock position was received by the custodian

COVINGTON & BURLING LLP

BEIJING BRUSSELS LONDON NEW YORK
SAN DIEGO SAN FRANCISCO SEOUL
SHANGHAI SILICON VALLEY WASHINGTON

KEIR D. GUMBS
1201 PENNSYLVANIA AVENUE, NW
WASHINGTON, DC 20004-2401
T 202.662.5500
kgumbs@cov.com

January 31, 2014

**BY ELECTRONIC MAIL TO SHAREHOLDERPROPOSALS@SEC.GOV**

Office of Chief Counsel
Division of Corporation Finance
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Re: UnitedHealth Group Incorporated – Shareholder Proposal Submitted by Arjuna Capital on Behalf of Ann B. Alexander

Ladies and Gentlemen:

This letter and the enclosed materials are submitted on behalf of UnitedHealth Group Incorporated, a Minnesota corporation (the "Company"), to request confirmation from the staff of the Division of Corporation Finance (the "Staff") that it will not recommend enforcement action to the U.S. Securities and Exchange Commission (the "Commission") if the Company excludes the shareholder proposal described herein (the "Proposal") submitted by Arjuna Capital on behalf of Ann B. Alexander (the "Proponent") from the proxy materials for its 2014 Annual Meeting of Shareholders. For the reasons set forth below, the Company intends to exclude the Proposal from its proxy materials in reliance on Rule 14a-8(i)(10) and Rule 14a-8(i)(7) under the Securities Exchange Act of 1934.

In accordance with Staff Legal Bulletin No. 14D (Nov. 7, 2008), we are emailing this letter to the Staff at shareholderproposals@sec.gov. In accordance with Rule 14a-8(j) we are simultaneously sending a copy of this letter and its attachments to the Proponent as notice of the Company's intent to omit the proposal from the 2014 proxy materials. Likewise, we take this opportunity to inform the Proponent that if the Proponent elects to submit any correspondence to the Commission or the Staff with respect to the Proposal, a copy of that correspondence should be provided concurrently to the undersigned on behalf of the Company.

## THE PROPOSAL

The Proposal provides in pertinent part:

***Resolved**, shareholders request 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 the Proposal is not asking the Company to disclose risks, specific incidents, or legal compliance procedures, but rather, we believe investors need to understand how the Board is overseeing these concerns.*

## BASIS FOR EXCLUSION

The Company respectfully requests that the Staff concur in its view that the Proposal may be excluded from the Company's 2014 proxy materials pursuant to Rules 14a-8(i)(10) and 14a-8(i)(7), for the reasons discussed below.

## ANALYSIS

### I. The Proposal may be excluded under Rule 14a-8(i)(10) because the Company has substantially implemented the Proposal through its Form 10-K and Proxy Statement disclosures.

Rule 14a-8(i)(10) permits a company to exclude a shareholder proposal if the company has already substantially implemented the proposal. The Commission said that "substantial" implementation under the rule does not require implementation in full or exactly as presented by the proponent. *See* SEC Release No. 34-40018 (May 21, 1998, n. 30). The Staff has provided no-action relief under Rule 14a-8(i)(10) when a company has satisfied the "essential objective" of a proposal, even if the company did not take the exact action requested by the proponent, did not implement the proposal in every detail, or exercised discretion in determining how to implement the proposal.[1] The Staff has considered a proposal substantially implemented when

---

[1] *See, e.g., ConAgra Foods, Inc.* (Jul. 3, 2006) (permitting exclusion of a shareholder proposal requesting publication of a sustainability report when the company had posted online a report on the topic of sustainability); *Talbots, Inc.* (Apr. 5, 2002) (permitting exclusion of a shareholder proposal requesting that the company implement a corporate code of conduct based on the International Labor Organization (ILO) human rights standard where the company had already implemented a code of conduct addressing similar topics but not based on ILO standards); *Nordstrom, Inc.* (Feb. 8, 1995) (permitting exclusion on substantial implementation grounds of a shareholder proposal requesting a code of conduct for its overseas suppliers that was substantially covered by existing company guidelines); *Texaco, Inc.* (Mar. 28, 1991) (permitting exclusion on substantial implementation grounds of a proposal requesting that the company adopt the Valdez Principles where the company had already adopted policies, practices, and procedures regarding the environment.)

the company's practices are deemed consistent with the "intent of the proposal." *Aluminum Company of America* (Jan. 16, 1996).

The Staff has consistently taken the position that a proposal seeking disclosures or a report regarding a particular subject may be substantially implemented through the disclosures that a company makes in compliance with applicable laws and regulations, including through disclosure required by the federal securities laws. *See, e.g., JPMorgan Chase & Co.* (Mar. 15, 2012) (permitting exclusion of a shareholder proposal requesting that the company's independent directors assess how the company is responding to risks associated with executive compensation as substantially implemented because the company had provided such disclosures in response to Item 402(s) of Regulation S-K); *The Goldman Sachs Group, Inc.* (Mar. 15, 2012) (permitting exclusion of a shareholder proposal requesting that the company's directors assess how the company is responding to risks associated with executive compensation as substantially implemented because Goldman had provided such disclosures in response to Item 402(b) of Regulation S-K); *Verizon Communications Inc.* (Feb. 21, 2007) (permitting exclusion of a shareholder proposal requesting the company disclose relationships between each independent director and the company that the board considered when determining each such director's independence as substantially implemented because the company had provided such disclosures in response to Item 407 of Regulation S-K); *Eastman Kodak Co.* (Feb. 1, 1991) (permitting exclusion of a shareholder proposal requesting that the company disclose in its annual report all fines paid for violating environmental laws as substantially implemented because the company had provided similar disclosures in response to Item 103 of Regulation S-K).

Here, the Proposal calls for the Company's Board of Directors (the "Board") to publish a report, at reasonable expense and excluding confidential or proprietary information, explaining how the Board is overseeing privacy and data security risks. The Proposal does not provide any additional detail regarding what topics the requested report would include. As explained below, the Company believes it has substantially implanted the Proposal through its existing disclosures and thus, the Proposal is excludable under Rule 14a-8(i)(10).

### *A. The Company has disclosed privacy and data security as a significant risk factor to its business*

Item 503(c) of Regulation S-K requires disclosure of "the most significant factors" that make an investment in the Company's securities speculative or risky. Item 503(c) states that the risk factor discussion cannot "present risk that could apply to any issuer." In response to Item 503(c), the Company has identified risks relating to data security and privacy as "significant." Specifically, the Company provided a risk factor detailing the data security and privacy risks facing the Company under the following heading in the risk factor section of in its Form 10-K, filed with the Commission on February 6, 2013 (the "2013 10-K"):

> **If we fail to comply with applicable privacy and security laws, regulations and standards, including with respect to third-party service providers that**

**utilize sensitive personal information on our behalf, or if we fail to address emerging security threats or detect and prevent privacy and security incidents, our business, reputation, results of operations, financial position and cash flows could be materially and adversely affected.**

The collection, maintenance, protection, use, transmission, disclosure and disposal of sensitive personal information are regulated at the federal, state, international and industry levels and requirements are imposed on us by contracts with customers. These laws, rules and requirements are subject to change. Further, many of our businesses are subject to the Payment Card Industry Data Security Standards (PCI DSS), which is a multifaceted security standard that is designed to protect credit card account data as mandated by payment card industry entities. See Item 1, "Business - Government Regulation" for additional information. HIPAA also requires business associates as well as covered entities to comply with certain privacy and security requirements. Even though we provide for appropriate protections through our contracts with our third-party service providers and in certain cases assess their security controls, we still have limited oversight or control over their actions and practices.

Our facilities and systems and those of our third-party service providers may be vulnerable to privacy and security incidents; security attacks and breaches; acts of vandalism or theft; computer viruses; coordinated attacks by activist entities; emerging cybersecurity risks; misplaced or lost data; programming and/or human errors; or other similar events. Emerging and advanced security threats, including coordinated attacks, require additional layers of security which may disrupt or impact efficiency of operations.

Compliance with new privacy and security laws, regulations and requirements may result in increased operating costs, and may constrain our ability to manage our business model. For example, final HHS regulations released in January 2013 implementing the ARRA amendments to HIPAA may further restrict our ability to collect, disclose and use sensitive personal information and may impose additional compliance requirements on our business. In addition, HHS has announced that it will continue its audit program to assess HIPAA compliance efforts by covered entities. Although we are not aware of HHS plans to audit any of our covered entities, an audit resulting in findings or allegations of noncompliance could have a material adverse effect on our results of operations, financial position and cash flows.

Noncompliance or findings of noncompliance with applicable laws, regulations or requirements, or the occurrence of any privacy or security breach involving the misappropriation, loss or other unauthorized disclosure of sensitive personal information, whether by us or by one of our third-party service providers, could

> have a material adverse effect on our reputation and business, including mandatory disclosure to the media, significant increases in the cost of managing and remediating privacy or security incidents and material fines, penalties and litigation awards, among other consequences, any of which could have a material and adverse effect on our results of operations, financial position and cash flows.

A copy of excerpts from the 2013 10-K devoted to the Company's discussion of the privacy and data security risks that it faces is attached hereto as Exhibit A, with sections of note highlighted.

### *B. The Audit Committee is responsible for overseeing the Company's enterprise risk management, which includes privacy and data security risks*

The Audit Committee of the Board (the "Audit Committee") is tasked with assisting the Board in fulfilling, *inter alia*, its oversight responsibilities relating to "the Company's compliance with legal and regulatory requirements [and] the efficacy of the Company's enterprise risk management structure and key processes." The charter for the Audit Committee (the "Audit Committee Charter") is attached as hereto as Exhibit B and (as noted in the Company's proxy statement) available on the Company's website. The Audit Committee Charter makes clear that the Audit Committee shall undertake the following responsibilities and duties related to Enterprise Risk Management:

- Review with management, the Company's enterprise risk management framework, including the governance structure, the guidelines and policies for assessing, identifying, managing, monitoring and reporting of significant risks.

- Meet periodically with management to review the Company's significant risks and the steps management has taken to monitor, control or mitigate such risk.

Data security and privacy risks are among the risks that the Audit Committee reviews with management, which we believe is made clear by the fact that such risks are included in the Company's risk factor disclosures and the fact that the Company discloses the fact that the Audit Committee is responsible for overseeing the significant risks facing the Company. All of this information is available to Company shareholders on the Company's website, where the Audit Committee Charter is posted.

### *C. The Company has disclosed how its Audit Committee and the Board oversee risk, including privacy and data security risks*

In addition to the disclosure regarding the operation of the Audit Committee that is available on the Company's website in the form of the Audit Committee Charter, the Commission's rules require the Company to provide disclosure regarding the Board's role in overseeing the Company's risks. Specifically, Item 407(h) of Regulation S-K requires the

Company to disclose "the extent of the board's role in the risk oversight of the [Company], such as how the board administers its oversight function and the effect that this has on the board's leadership structure." Consistent with the requirements of Item 407(h), and in addition to the provisions of the Audit Committee Charter discussed above, the Company provides substantial disclosure regarding the Board's role in risk oversight. In particular, page 13 of the Company's most recent Proxy Statement on Schedule 14A, filed with the Commission on April 24, 2013 (the "2013 Proxy Statement") states:

> ***Enterprise-Wide Risk Oversight***
>
> Our Board of Directors oversees management's enterprise-wide risk management activities. Risk management activities include assessing and taking actions necessary to manage risk incurred in connection with the long-term strategic direction and operation of our business. Each director on our Board is required to have risk oversight ability for each skill and attribute the director possesses that is reflected in the collective skills section of our director skills matrix described in "Proposal 1 — Election of Directors — Director Nomination Process — Criteria for Nomination to the Board" above. Collectively, our Board of Directors uses its committees to assist in its risk oversight function as follows:
>
> - The Audit Committee oversees our controls and compliance activities. The Audit Committee also oversees management's processes to identify and quantify material risks facing the Company. The enterprise risk management function, which reports to the Chief Accounting Officer, assists the Company in identifying and assessing the Company's material risks. The Company's General Auditor, who reports to the Audit Committee, assists the Company in evaluating risk management controls and methodologies. The Chief Accounting Officer and General Auditor provide periodic reports to the Audit Committee. In connection with its risk oversight role, the Audit Committee regularly meets privately with representatives from the Company's independent registered public accounting firm and the Company's CFO, General Auditor and Chief Legal Officer; . . .
>
> - Our Board of Directors maintains overall responsibility for oversight of the work of its various committees by receiving regular reports from the Committee Chairs regarding their work. In addition, discussions about the Company's strategic plan, consolidated business results, capital structure, merger and acquisition related activities and other business discussed with the Board of Directors include a discussion of the risks associated with the particular item under consideration.

Similar to the circumstances in *JPMorgan Chase & Co.*, *The Goldman Sachs Group Inc.* and *Eastman Kodak*, the Company's disclosures in response to Regulation S-K fully implement the Proposal, which simply asks for disclosure regarding how the Company oversees data security and privacy risks. As discussed above, the Company's disclosure in the 2013 10-K makes clear that privacy and data security are material risks facing the Company. Therefore, the disclosures in the 2013 Proxy Statement regarding the extent and specific role of the Board and Audit Committee in the risk oversight of the Company extends to privacy and data security risks. The Company believes that the disclosures required by Items 407(h) and 503(c) have substantially implemented the essential objective of the Proposal — they provide disclosure regarding how the Board is overseeing privacy and data security risks and thus, the Proposal is excludable under Rule 14a-8(i)(10).

***D. The Company will add Proxy Statement disclosure to further describe how the Audit Committee and the Board oversee risk***

Although additional disclosure regarding the Board's oversight of the Company's privacy and data security risks is not required for the Company to exclude the Proposal pursuant to Rule 14a-8(i)(10), at its February 12, 2014 meeting, the Audit Committee will consider and is expected to recommend an amendment to the Audit Committee Charter specifying that privacy and data security matters are included in the Audit Committee's role to oversee the effectiveness of the Company's compliance program. We will supplement this no-action letter and provide the amended Audit Committee Charter after the February 12, 2014 meeting.

To further implement the Proposal, the Company represents that it will make the following modifications to its disclosure in its Proxy Statement on Schedule 14A regarding the Audit Committee's oversight of the Company's risks (additions are **underlined and in bold**):

> The Audit Committee oversees our controls and compliance activities. The Audit Committee also oversees management's processes to identify and quantify material risks facing the Company, **including risks disclosed in the Company's Annual Report on Form 10-K**. The enterprise risk management function, which reports to the Chief Accounting Officer, assists the Company in identifying and assessing the Company's material risks. The Company's General Auditor, who reports to the Audit Committee, assists the Company in evaluating risk management controls and methodologies. The Chief Accounting Officer and General Auditor provide periodic reports to the Audit Committee. In connection with its risk oversight role, the Audit Committee regularly meets privately with representatives from the Company's independent registered public accounting firm and the Company's CFO, General Auditor and Chief Legal Officer; . . .

The Company believes that these additional disclosures substantially implement the essential objective of the Proposal and thus, the Proposal is excludable under Rule 14a-8(i)(10).

## II. The Proposal may be excluded under Rule 14a-8(i)(7) because it deals with the Company's ordinary business operations and does not raise a significant policy issue.

We believe that the Company may also exclude the Proposal pursuant to Rule 14a-8(i)(7) because it deals with matters relating to the Company's ordinary business operations. The ordinary business exclusion rests on two central considerations: (1) the subject matter of a proposal (i.e., whether the subject matter involves a matter of ordinary business); and (2) the degree to which the proposal attempts to micromanage a 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." Exchange Act Release No. 40018 (May 21, 1998); Exchange Act Release No. 20091 (Aug. 16, 1983). In Exchange Act Release No. 40018, the Commission explained that the term "ordinary business" refers to matters that are not necessarily "ordinary" in the common meaning of the word, but that the term "is rooted in the corporate law concept [of] providing management with flexibility in directing certain core matters involving the company's business and operations." *Id.*

### *A. Subject Matter of the Requested Report is within the Ordinary Business of the Company*

The Proposal requests a report on "how the Board is overseeing privacy and data security risks." When reviewing shareholder proposals that request a risk assessment, the Staff bases its Rule 14a-8(i)(7) analysis on "whether the underlying subject matter of the risk evaluation involves a matter of ordinary business to the company." Staff Legal Bulletin No. 14E (Oct. 27, 2009) ("SLB 14E"). In numerous no-action letters, the Staff has reviewed the underlying subject matter of the risk(s) the board is asked to report on, and has permitted the exclusion of proposals when the underlying subject matter of the proposals involve a matter of ordinary business to the company. *See, e.g. Sempra Energy* (Jan. 12, 2012, *recon. denied* Jan. 23 , 2012) (permitting exclusion under Rule 14a-8(i)(7) of a shareholder proposal requesting that the board "conduct an independent oversight review of the [c]ompany's management of political, legal, and financial risks posed by Sempra operations in any country that may pose an elevated risk of corrupt practices," noting in its response letter that "although the proposal requests the board to conduct an independent oversight review of Sempra's management of particular risks, the underlying subject matter of these risks appears to involve ordinary business matters"); *The Western Union Co.* (Mar. 14, 2011) (permitting exclusion under Rule 14a-8(i)(7) of a shareholder proposal that requested that the company establish a risk committee on its board of directors and report on certain identified risk categories, including "risks to customer base, fee structure, community and customer good will, growing competition" which appears to have provided the basis for the Staff's grant of no-action relief).

The Staff has permitted exclusion of numerous shareholder proposals that, like the instant Proposal, focus on procedures for protecting customer data, information and privacy, on the basis that such proposals relate to ordinary business. In fact, in *Verizon Communications* and *Bank of*

*America*, discussed below, it has taken the position that shareholder proposals seeking a report regarding risks associated with data security and privacy involve ordinary business matters.

In *Verizon Communications, Inc.* (Feb. 27, 2007), the Staff permitted the exclusion under Rule 14a-8(i)(7) of a shareholder proposal requesting a report on the "technological, legal and ethical policy issues surrounding the disclosure of customer records and communications content to government agencies without a warrant and non-governmental entities (e.g., private investigators), and their effect on customer privacy rights" because the proposal related to "Verizon's ordinary business operations (i.e. procedures for protecting customer information)." This decision is highly relevant because, as is the case here, the issues addressed by the shareholder proposal in that letter arguably raised significant social policy issues regarding data privacy, and yet the Staff properly concluded that the proposal could be excluded under Rule 14a-8(i)(7).

Similarly, in *Bank of America Corp.* (Feb. 21, 2006), a shareholder proposal requested a report on Bank of America'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." The Staff allowed Bank of America to exclude the proposal under Rule 14a-8(i)(7) based on Bank of America's arguments that the proposal concerned a core management function and attempted to "usurp[] management's authority by allowing stockholders to govern the day-to-day business of managing the banking and financial relationships that [Bank of America] has with its customers and the privacy protection afforded to its customers." In permitting exclusion, the Staff took note that the proposal related to the company's "procedures for protecting customer information" — part of the company's ordinary business operations.

The positions reflected in *Verizon* and *Bank of America* are consistent with other letters involving shareholder proposals seeking to influence ordinary business decisions regarding data security and privacy. For example, in *Huntington Bancshares Inc.* (Jan. 10, 2011), a shareholder proposal requested that the company adopt a minimum time period for its records retention policy on all electronic loan files, and adopt necessary internal controls to safeguard these assets from unauthorized access and accidental loss or deletion. The Staff permitted exclusion of the proposal under Rule 14a-8(i)(7), noting that the proposal "relates to the policies and procedures for the retention of records regarding the products and services [the company] offers." The Staff has taken similar positions with respect to proposals concerning internet privacy, customer privacy, and the security of customer information. *See Comcast Corp.* (Mar. 4 , 2009)(proposal requesting 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," excludable because the proposal relates to the ordinary business matter of "procedures for protecting user information."); *Consolidated Edison, Inc.* (Mar. 10, 2003) (proposal requesting that employees of Con Edison who enter a customer's premises not concern themselves with or report on the lifestyles of the occupants of the premises, excludable because the proposal related to the ordinary business matter of "management of employees and

customer relations"); *Zions Bancorporation* (Feb. 11, 2008, *recon. denied* Feb. 29, 2008) (proposal that requested that the board implement a mandatory adjudication process prior to termination of certain customer accounts, excludable because the proposal related to the ordinary business matter of "procedures for handling customers' accounts".) These letters demonstrate that the Staff has historically permitted the exclusion of shareholder proposals relating to the protection of the company's customers' data, information and privacy, on the basis that such matters concern a company's ordinary business matters. The same principle should apply to the Proposal.

A key component of the Company's ordinary business is the protection of data and the privacy of its customers and members and ensuring that all data stored by the Company or by Company products, including private health information, is secure. The Company is routinely assessing and improving its methods and processes to protect its data and its customers' privacy as part of its compliance and privacy programs. These matters are generally overseen by the Audit Committee, as disclosed in the Company's proxy statement. Further, as disclosed in the Company's 2013 10-K and as detailed in the Proposal, a material breach of the Company's data security could materially affect the Company's operations and result in litigation, both from customers and various state and federal government entities. Ensuring that the Company's data is secure and customer privacy is maintained requires the efforts of Company employees with specialized knowledge of the Company's privacy and data security protocols. Because of the importance of data security to the Company and the industry in which it operates, privacy and data security issues are so fundamental to management's ability to run the Company that they could not, as a practical matter, be subject to shareholder oversight.

***B. The Proposal does not address a significant social policy issue, but instead relates entirely to ordinary business matters***

In Staff Legal Bulletin No. 14C (Jun. 28, 2005) citing Release No. 34-40018, the Staff explained that, where a proposal focuses on a "sufficiently significant" social policy issue, the proposal may not be excluded because, in the view of the Commission, the proposal would "transcend day-to-day business matters." If the underlying subject matter of the proposal "transcends the day-to-day business matters of the company and raises policy issues so significant that it would be appropriate for a shareholder vote," the Staff will not concur that there is a basis to exclude the proposal so long as "a sufficient nexus exists between the nature of the proposal and the company." Staff Legal Bulletin No. 14E (Oct. 27, 2009).

Notwithstanding the fact that the Proponent likely views the Proposal as raising significant social policy considerations, the no-action positions described in the preceding section make clear that the core issue that the Proposal seeks to address, data security and privacy, constitute ordinary business matters. As explained above, the Staff has consistently permitted the exclusion of proposals requesting reports on the protection of customer data on the internet and customer privacy. Moreover, those letters demonstrate that any social policy considerations raised by such proposals do not transcend the ordinary business matters to which

the proposals relate. Maintaining data security and privacy are essential to the successful operation of companies in the modern business world. Such issues, however, are technical and commercial issues rather than significant policy issues.

While we recognize that the resolved clause of the Proposal (and the paragraph immediately preceding the resolved clause) refer to the Board's oversight of data security and privacy risks, the rest of the supporting statement makes clear that the focus and thrust of the Proposal is really the risk posed to the Company by such risks and not the Board's oversight of such risks. For example, the supporting statement includes the following statements concerning data security and privacy risks, all of which are focused on the risks to the Company and to patients posed by data security and privacy concerns:

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

- "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 (COT) 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 ..."

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

- "In 2013, Bloomberg reported UnitedHealth recalled software from hospital emergency departments in over 20 states, as an error caused patient prescriptions notes to disappear. Bloomberg highlighted six EHR software recalls since 2009 from Picis Inc., acquired by UnitedHealth 2010."

- "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."

As we believe is made clear by these statements, the focus of the Proposal is data security and privacy risks faced by the Company and consumers, which makes the Proposal similar to

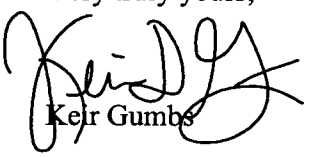
numerous other proposals that have been excluded under Rule 14a-8(i)(7), even where the risks focused on by such proposals raise social policy considerations. *See e.g., FirstEnergy Corp.* (Mar. 8, 2013) (proposal requesting a report on actions that FirstEnergy is taking or could take to reduce risk throughout its energy portfolio, excludable where the Staff noted "Proposals that concern a company's choice of technologies for use in its operations are generally excludable under rule 14a-8(i)(7)"); FirstEnergy Corp. (Mar. 7, 2013)(proposal requesting that the company adopt strategies and quantitative goals to reduce the company's impacts on, and risks to, water quantity and quality, excludable where the Staff noted "we note that the proposal addresses the company's impact on water quantity and does not, in our view, focus on a significant policy issue"); *Exxon Mobil Corporation* (Mar. 6, 2012)(request that the board prepare a report discussing possible short and long term risks to the company's finances and operations posed by the environmental, social, and economic challenges associated with the oil sands, where the Staff noted "we note that the proposal addresses the 'economic challenges' associated with the oil sands and does not, in our view, focus on a significant policy issue."). Like the proposals in each of these letters, the Proposal focuses on risks that are ordinary business matters. Consequently, based on the precedent established by such letters and the other no-action letters cited throughout this no-action request, we believe that the Company should be able to exclude the Proposal from its proxy materials in reliance on Rule 14a-8(i)(7).

## CONCLUSION

For the reasons set forth above, we respectfully request that the Staff confirm that it will not recommend enforcement action to the Commission if the Company excludes the Proposal and the supporting statement from the proxy materials for its 2014 Annual Meeting of Shareholders in reliance on Rule 14a-8(i)(10) and Rule 14a-8(i)(7). Please note that the Company expects to submit its proxy materials for printing no later than April 21, 2014; consequently the Company would appreciate it if the Staff could respond to this request by then.

If you have any questions regarding this request or desire additional information, please contact the undersigned at (202) 662-5500 or Amy L. Schneider, Deputy General Counsel of the Company, at (952) 936-4986.

Very truly yours,



Keir Gumbs

Enclosure

cc: Ms. Amy L. Schneider
Ms. Natasha Lamb

**Exhibit A**

Excerpts of 2013 10-K Discussing Privacy and Data Security Risks

Excerpts from Item 1 – Business

See attached

Legislation remains difficult to predict and is not yet fully known. See also Item 1A, "Risk Factors" for a discussion of the risks related to the Health Reform Legislation and related matters.

**Other Federal Laws and Regulation**

We are subject to various levels of U.S. federal regulation. For example, when we contract with the federal government, we are subject to federal laws and regulations relating to the award, administration and performance of U.S. government contracts. CMS regulates our UnitedHealthcare businesses, and certain aspects of our Optum businesses. Our UnitedHealthcare Medicare & Retirement, UnitedHealthcare Community & State and OptumHealth businesses submit information relating to the health status of enrollees to CMS (or state agencies) for purposes of determining the amount of certain payments to us. CMS also has the right to audit performance to determine compliance with CMS contracts and regulations and the quality of care given to Medicare beneficiaries. Beginning in 2014, our commercial business may be subject to audit related to the risk adjustment and reinsurance data. See Note 12 of Notes to the Consolidated Financial Statements included in Item 8, "Financial Statements" and Item 1A, "Risk Factors" for a discussion of audits by CMS.

Our UnitedHealthcare reportable segment, through UnitedHealthcare Community & State, also has Medicaid and CHIP contracts that are subject to federal regulations regarding services to be provided to Medicaid enrollees, payment for those services and other aspects of these programs. There are many regulations surrounding Medicare and Medicaid compliance, and the regulatory environment with respect to these programs has become and will continue to become increasingly complex as a result of the Health Reform Legislation. In addition, our UnitedHealthcare Military & Veterans business and certain of Optum's businesses hold contracts with federal agencies including the DoD and we are subject to federal law and regulations relating to the administration of these contracts.

Certain of UnitedHealthcare's and Optum's businesses, such as UnitedHealthcare's eyeglass manufacturing activities and Optum's high acuity clinical workflow software, hearing aid products, and clinical research activities, are subject to regulation by the U.S. Food and Drug Administration (FDA), and the clinical research activities are also subject to laws and regulations outside of the United States that regulate clinical trials. Laws and regulations relating to consumer protection, anti-fraud and abuse, anti-kickbacks, false claims, prohibited referrals, inappropriately reducing or limiting health care services, anti-money laundering, securities and antitrust also affect us.

***HIPAA, GLBA and Other Privacy and Security Regulation.*** The administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA), apply to both the group and individual health insurance markets, including self-funded employee benefit plans. HIPAA requires guaranteed health care coverage for small employers and certain eligible individuals. It also requires guaranteed renewability for employers and individuals and limits exclusions based on pre-existing conditions. Federal regulations related to HIPAA include minimum standards for electronic transactions and code sets, and for the privacy and security of protected health information. The HIPAA privacy regulations do not preempt more stringent state laws and regulations that may also apply to us.

Federal privacy and security requirements change frequently because of legislation, regulations and judicial or administrative interpretation. For example, the U.S. Congress enacted the American Recovery and Reinvestment Act of 2009 (ARRA), which significantly amends, and adds new privacy and security provisions to HIPAA and imposes additional requirements on uses and disclosures of health information. ARRA includes new contracting requirements for HIPAA business associate agreements; extends parts of HIPAA privacy and security provisions to business associates; adds new federal data breach notification requirements for covered entities and business associates and new reporting requirements to HHS and the Federal Trade Commission (FTC) and, in some cases, to the local media; strengthens enforcement and imposes higher financial penalties for HIPAA violations and, in certain cases, imposes criminal penalties for individuals, including employees. In January 2013, HHS issued its final regulations implementing the ARRA amendments to HIPAA and updating the HIPAA privacy, security and

enforcement rules. In the conduct of our business, we may act, depending on the circumstances, as either a covered entity or a business associate. Federal consumer protection laws may also apply in some instances to privacy and security practices related to personally identifiable information. The use and disclosure of individually identifiable health data by our businesses is also regulated in some instances by other federal laws, including the Gramm-Leach-Bliley Act (GLBA) or state statutes implementing GLBA, which generally require insurers to provide customers with notice regarding how their non-public personal health and financial information is used and the opportunity to "opt out" of certain disclosures before the insurer shares such information with a third party, and which generally require safeguards for the protection of personal information. See Item 1A, "Risk Factors" for a discussion of the risks related to compliance with HIPAA, GLBA and other privacy-related regulations.

***ERISA.*** The Employee Retirement Income Security Act of 1974, as amended (ERISA), regulates how goods and services are provided to or through certain types of employer-sponsored health benefit plans. ERISA is a set of laws and regulations that is subject to periodic interpretation by the DOL as well as the federal courts. ERISA places controls on how our business units may do business with employers who sponsor employee benefit health plans, particularly those that maintain self-funded plans. Regulations established by the DOL provide additional rules for claims payment and member appeals under health care plans governed by ERISA. Additionally, some states require licensure or registration of companies providing third-party claims administration services for health care plans.

**State Laws and Regulation**

***Health Care Regulation.*** Our insurance and HMO subsidiaries must be licensed by the jurisdictions in which they conduct business. All of the states in which our subsidiaries offer insurance and HMO products regulate those products and operations. These states require periodic financial reports and establish minimum capital or restricted cash reserve requirements. The National Association of Insurance Commissioners (NAIC) has adopted model regulations that, when implemented by states would require certain governance practices substantially similar to the Sarbanes-Oxley Act of 2002 and expand insurance company and HMO risk and solvency assessment reporting. We expect that states will adopt these or similar measures over the next few years, expanding the scope of regulations relating to corporate governance and internal control activities of HMOs and insurance companies. Certain states have also adopted their own regulations for minimum medical loss ratios with which health plans must comply. In addition, a number of state legislatures have enacted or are contemplating significant reforms of their health insurance markets, either independent of or to comply with or be eligible for grants or other incentives in connection with the Health Reform Legislation. We expect the states to continue to introduce and pass similar laws in 2013, and this will affect our operations and our financial results.

Health plans and insurance companies are also regulated under state insurance holding company regulations. Such regulations generally require registration with applicable state departments of insurance and the filing of reports that describe capital structure, ownership, financial condition, certain intercompany transactions and general business operations. Some state insurance holding company laws and regulations require prior regulatory approval of acquisitions and material intercompany transfers of assets, as well as transactions between the regulated companies and their parent holding companies or affiliates. These laws may restrict the ability of our regulated subsidiaries to pay dividends to our holding companies.

In addition, some of our business and related activities may be subject to other health care-related regulations and requirements, including PPO, managed care organization (MCO), utilization review (UR) or TPA-related regulations and licensure requirements. These regulations differ from state to state, and may contain network, contracting, product and rate, and financial and reporting requirements. There are laws and regulations that set specific standards for delivery of services, appeals, grievances and payment of claims, adequacy of health care professional networks, fraud prevention, protection of consumer health information, pricing and underwriting practice and covered benefits and services. State health care anti-fraud and abuse prohibitions encompass a wide

range of activities, including kickbacks for referral of members, billing unnecessary medical services and improper marketing. Certain of our businesses are subject to state general agent, broker, and sales distributions laws and regulations. Our UnitedHealthcare Community & State, UnitedHealthcare Medicare & Retirement and certain Optum businesses are subject to regulation by state Medicaid agencies that oversee the provision of benefits to our Medicaid and CHIP beneficiaries and to our dually eligible beneficiaries. We also contract with state governmental entities and are subject to state laws and regulations relating to the award, administration and performance of state government contracts.

***Guaranty Fund Assessments.*** Under state guaranty fund laws, certain insurance companies (and HMOs in some states), including those issuing health, long-term care, life and accident insurance policies, doing business in those states can be assessed (up to prescribed limits) for certain obligations to the policyholders and claimants of insolvent insurance companies that write the same line or lines of business. Assessments generally are based on a formula relating to premiums in the state compared to the premiums of other insurers and could be spread out over a period of years. Some states permit member insurers to recover assessments paid through full or partial premium tax offsets.

***Pharmacy Regulation.*** OptumRx's mail order pharmacies must be licensed to do business as pharmacies in the states in which they are located. Our mail order pharmacies must also register with the U.S. Drug Enforcement Administration and individual state controlled substance authorities to dispense controlled substances. In many of the states where our mail order pharmacies deliver pharmaceuticals there are laws and regulations that require out-of-state mail order pharmacies to register with that state's board of pharmacy or similar regulatory body. These states generally permit the pharmacy to follow the laws of the state in which the mail order pharmacy is located, although some states require that we also comply with certain laws in that state. Our mail order pharmacies maintain certain Medicare and state Medicaid provider numbers as pharmacies providing services under these programs. Participation in these programs requires the pharmacies to comply with the applicable Medicare and Medicaid provider rules and regulations. Other laws and regulations affecting our mail order pharmacies include federal and state statutes and regulations governing the labeling, packaging, advertising and adulteration of prescription drugs and dispensing of controlled substances. See Item 1A, "Risk Factors" for a discussion of the risks related to our PBM businesses.

***Privacy and Security Laws.*** States have adopted regulations to implement provisions of the GLBA. Like HIPAA, GLBA allows states to adopt more stringent requirements governing privacy protection. A number of states have also adopted other laws and regulations that may affect our privacy and security practices, for example, state laws that govern the use, disclosure and protection of social security numbers and sensitive health information or that are designed to protect credit card account data. State and local authorities increasingly focus on the importance of protecting individuals from identity theft, with a significant number of states enacting laws requiring businesses to notify individuals of security breaches involving personal information. State consumer protection laws may also apply to privacy and security practices related to personally identifiable information, including information related to consumers and care providers. Additionally, different approaches to state privacy and insurance regulation and varying enforcement philosophies in the different states may materially and adversely affect our ability to standardize our products and services across state lines. See Item 1A, "Risk Factors" for a discussion of the risks related to compliance with state privacy and security-related regulations.

***Corporate Practice of Medicine and Fee-Splitting Laws.*** Certain of our businesses function as direct service providers to care delivery systems and, as such, are subject to additional laws and regulations. Some states have corporate practice of medicine laws that prohibit certain entities from practicing medicine or employing physicians to practice medicine. Additionally, some states prohibit certain entities from sharing in the fees or revenues of a professional practice (fee-splitting). These prohibitions may be statutory or regulatory, or may be a matter of judicial or regulatory interpretation. These laws, regulations and interpretations have, in certain states, been subject to limited judicial and regulatory interpretation and are subject to change.

***Consumer Protection Laws.*** Certain businesses participate in direct-to-consumer activities and are subject to emerging regulations applicable to on-line communications and other general consumer protection laws and regulations.

**Banking Regulation**

Optum Bank is subject to regulation by federal banking regulators, including the Federal Deposit Insurance Corporation (FDIC), which performs annual examinations to ensure that the bank is operating in accordance with federal safety and soundness requirements, and the Consumer Financial Protection Bureau, which may perform periodic examinations to ensure that the bank is in compliance with applicable consumer protection statutes, regulations and agency guidelines. Optum Bank is also subject to supervision and regulation by the Utah State Department of Financial Institutions, which carries out annual examinations to ensure that the bank is operating in accordance with state safety and soundness requirements and performs periodic examinations of the bank's compliance with applicable state banking statutes, regulations and agency guidelines. In the event of unfavorable examination results from any of these agencies, the bank could be subjected to increased operational expenses and capital requirements, enhanced governmental oversight and monetary penalties.

**International Regulation**

Certain of our businesses and operations are international in nature and are subject to regulation in the jurisdictions in which they are organized or conduct business. These regulatory regimes encompass tax, licensing, tariffs, intellectual property, investment, management control, labor, anti-fraud, anti-corruption and privacy and data protection regulations (including requirements for cross-border data transfers) that vary from jurisdiction to jurisdiction, among other matters. We have recently acquired and may in the future acquire or commence additional businesses based outside of the United States, increasing our exposure to non-U.S. regulatory regimes. For example, our acquisition of Amil subjects us to Brazilian laws and regulations affecting the managed care and insurance industries and regulation by Brazilian regulators including the national regulatory agency for private health insurance and plans, the Agência Nacional de Saúde Suplementar (ANS), whose approach to the interpretation, implementation and enforcement of industry regulations could differ from the approach taken by U.S. regulators. For more information about the Amil acquisition, see Note 6 of Notes to the Consolidated Financial Statement included in Item 8, "Financial Statements." In addition, our non-U.S. businesses and operations are also subject to U.S. laws that regulate the conduct and activities of U.S.-based businesses operating abroad, such as the Foreign Corrupt Practices Act.

**Audits and Investigations**

We have been and may in the future become involved in various governmental investigations, audits and reviews. These include routine, regular and special investigations, audits and reviews by CMS, state insurance and health and welfare departments, state attorneys general, the Office of the Inspector General (OIG), the Office of Personnel Management, the Office of Civil Rights, the FTC, U.S. Congressional committees, the U.S. Department of Justice (DOJ), U.S. Attorneys, the Securities and Exchange Commission (SEC), the Brazilian securities regulator, the Comissão de Valores Mobiliários (CVM), the Internal Revenue Service (IRS), the Brazilian federal revenue service — the Secretaria da Receita Federal (SRF), the DOL, the FDIC and other governmental authorities. Certain of our businesses have been reviewed or are currently under review, including for, among other things, compliance with coding and other requirements under the Medicare risk-adjustment model. Such government investigations, audits and reviews can result in assessment of damages, civil or criminal fines or penalties, or other sanctions, including loss of licensure or exclusion from participation in government programs. In addition, disclosure of any adverse investigation, audit results or sanctions could adversely affect our reputation in various markets and make it more difficult for us to sell our products and services while retaining our current business.

***COMPETITION***

As a diversified health and well-being services company, we operate in highly competitive markets. Our competitors include managed health care companies, insurance companies, HMOs, TPAs and business services outsourcing companies, health care professionals that have formed networks to directly contract with employers or with CMS, specialty benefit providers, government entities, disease management companies, and various

Excerpts from Item 1A – Risk Factors

See attached

CMS uses various payment mechanisms to allocate funding for Medicare programs, including adjusting monthly capitation payments to Medicare Advantage plans and Medicare Part D plans according to the predicted health status of each beneficiary as supported by data from health care providers as well as, for Medicare Part D plans, risk-sharing provisions based on a comparison of costs predicted in our annual bids to actual prescription drug costs. Some state Medicaid programs utilize a similar process. For example, our UnitedHealthcare Medicare & Retirement and UnitedHealthcare Community & State businesses submit information relating to the health status of enrollees to CMS or state agencies for purposes of determining the amount of certain payments to us. CMS and the Office of Inspector General for HHS periodically perform risk adjustment data validation (RADV) audits of selected Medicare health plans to validate the coding practices of and supporting documentation maintained by health care providers, and certain of our local plans have been audited. Such audits have in the past resulted and could in the future result in retrospective adjustments to payments made to our health plans, fines, corrective action plans or other adverse action by CMS. In February 2012, CMS published a final RADV audit and payment adjustment methodology. The methodology contains provisions allowing retroactive contract level payment adjustments for the year audited, beginning with 2011 payments, using an extrapolation of the "error rate" identified in audit samples and, for Medicare Advantage plans, after considering a fee-for-service (FFS) "error rate" adjuster that will be used in determining the payment adjustment. Depending on the plans selected for audit, if any, and the error rate found in those audits, if any, potential payment adjustments could have a material adverse effect on our results of operations, financial position and cash flows.

We have been and may in the future become involved in various governmental investigations, audits, reviews and assessments. These include routine, regular and special investigations, audits and reviews by CMS, state insurance and health and welfare departments, state attorneys general, the OIG, the Office of Personnel Management, the Office of Civil Rights, the FTC, U.S. Congressional committees, the DOJ, U.S. Attorneys, the SEC, the CVM, the IRS, the SRF, the DOL, the FDIC and other governmental authorities. Certain of our businesses have been reviewed or are currently under review, including for, among other things, compliance with coding and other requirements under the Medicare risk-adjustment model. Such investigations, audits or reviews sometimes arise out of or prompt claims by private litigants or whistleblowers that, among other things, we failed to disclose certain business practices or, as a government contractor, submitted false claims to the government. Governmental investigations, audits, reviews and assessments could expand to subjects beyond those targeted by the original investigation, audit, review, assessment or private action and could lead to government actions, which could result in the assessment of damages, civil or criminal fines or penalties, or other sanctions, including restrictions or changes in the way we conduct business, loss of licensure or exclusion from participation in government programs, any of which could have a material adverse effect on our business, results of operations, financial position and cash flows. See Note 12 of Notes to the Consolidated Financial Statements included in Item 8, "Financial Statements" for a discussion of certain of these matters.

**If we fail to comply with applicable privacy and security laws, regulations and standards, including with respect to third-party service providers that utilize sensitive personal information on our behalf, or if we fail to address emerging security threats or detect and prevent privacy and security incidents, our business, reputation, results of operations, financial position and cash flows could be materially and adversely affected.**

The collection, maintenance, protection, use, transmission, disclosure and disposal of sensitive personal information are regulated at the federal, state, international and industry levels and requirements are imposed on us by contracts with customers. These laws, rules and requirements are subject to change. Further, many of our businesses are subject to the Payment Card Industry Data Security Standards (PCI DSS), which is a multifaceted security standard that is designed to protect credit card account data as mandated by payment card industry entities. See Item 1, "Business — Government Regulation" for additional information. HIPAA also requires business associates as well as covered entities to comply with certain privacy and security requirements. Even though we provide for appropriate protections through our contracts with our third-party service providers and in certain cases assess their security controls, we still have limited oversight or control over their actions and practices.

Our facilities and systems and those of our third-party service providers may be vulnerable to privacy and security incidents; security attacks and breaches; acts of vandalism or theft; computer viruses; coordinated attacks by activist entities; emerging cybersecurity risks; misplaced or lost data; programming and/or human errors; or other similar events. Emerging and advanced security threats, including coordinated attacks, require additional layers of security which may disrupt or impact efficiency of operations.

Compliance with new privacy and security laws, regulations and requirements may result in increased operating costs, and may constrain our ability to manage our business model. For example, final HHS regulations released in January 2013 implementing the ARRA amendments to HIPAA may further restrict our ability to collect, disclose and use sensitive personal information and may impose additional compliance requirements on our business. In addition, HHS has announced that it will continue its audit program to assess HIPAA compliance efforts by covered entities. Although we are not aware of HHS plans to audit any of our covered entities, an audit resulting in findings or allegations of noncompliance could have a material adverse effect on our results of operations, financial position and cash flows.

Noncompliance or findings of noncompliance with applicable laws, regulations or requirements, or the occurrence of any privacy or security breach involving the misappropriation, loss or other unauthorized disclosure of sensitive personal information, whether by us or by one of our third-party service providers, could have a material adverse effect on our reputation and business, including mandatory disclosure to the media, significant increases in the cost of managing and remediating privacy or security incidents and material fines, penalties and litigation awards, among other consequences, any of which could have a material and adverse effect on our results of operations, financial position and cash flows.

**Our businesses providing PBM services face regulatory and other risks and uncertainties associated with the PBM industry that may differ from the risks of our business of providing managed care and health insurance products.**

We provide PBM services through our OptumRx and UnitedHealthcare businesses. Each business is subject to federal and state anti-kickback and other laws that govern their relationships with pharmaceutical manufacturers, physicians, pharmacies, customers and consumers. OptumRx also conducts business as a mail order pharmacy and specialty pharmacy, which subjects it to extensive federal, state and local laws and regulations. In addition, federal and state legislatures regularly consider new regulations for the industry that could materially and adversely affect current industry practices, including the receipt or disclosure of rebates from pharmaceutical companies, the development and use of formularies, and the use of average wholesale prices. See Item 1, "Business — Government Regulation" for a discussion of various federal and state laws and regulations governing our PBM businesses.

Our PBM businesses would also be materially and adversely affected by an inability to contract on favorable terms with pharmaceutical manufacturers and other suppliers, and could face potential claims in connection with purported errors by our mail order or specialty pharmacies, including in connection with the risks inherent in the packaging and distribution of pharmaceuticals and other health care products. Disruptions at any of our mail order or specialty pharmacies due to an accident or an event that is beyond our control could affect our ability to timely process and dispense prescriptions and could materially and adversely affect our results of operations, financial position and cash flows.

In addition, our PBM businesses provide services to sponsors of health benefit plans that are subject to ERISA. The DOL, which is the agency that enforces ERISA, could assert that the fiduciary obligations imposed by the statute apply to some or all of the services provided by our PBM businesses even where our PBM businesses are not contractually obligated to assume fiduciary obligations. In the event a court were to determine that fiduciary obligations apply to our PBM businesses in connection with services for which our PBM businesses are not contractually obligated to assume fiduciary obligations, we could be subject to claims for breaches of fiduciary obligations or entering into certain prohibited transactions.

**Exhibit B**

Audit Committee Charter

See attached

# UNITEDHEALTH GROUP
# BOARD OF DIRECTORS
# AUDIT COMMITTEE CHARTER
# (October 29, 2012)

## INTRODUCTION AND PURPOSE

UnitedHealth Group Incorporated (the "Company") is a publicly-held company and operates in a complex, dynamic, highly competitive, and regulated environment. In order to assure the kind of informed decision making beneficial to the Company, much of the Board of Director's oversight occurs through its standing committees, such as the Audit Committee (the "Committee"). The primary purpose of the Committee is (a) to assist the Board of Directors (the "Board") in fulfilling its oversight responsibilities relating to (i) the conduct and integrity of the Company's financial reporting to any governmental or regulatory body, the public or other users thereof, (ii) the Company's compliance with legal and regulatory requirements, (iii) the efficacy of the Company's enterprise risk management structure and key processes, (iv) the qualifications, engagement, compensation, independence and performance of the Company's independent outside auditor, and (v) the performance of the Company's General Auditor and internal audit function, and (b) to prepare the report of the Committee required by the Securities and Exchange Commission ("SEC") to be included in the Company's annual proxy statement.

The Committee's job is one of oversight. The Company's management is responsible for preparing the Company's financial statements and the independent outside auditor is responsible for auditing the annual financial statements and reviewing the quarterly financial statements. The Committee recognizes that financial management (including the General Auditor and internal auditing function), as well as the independent outside auditor, have more direct knowledge and detailed information about the Company than do Committee members. Consequently, in carrying out its oversight responsibilities, the Committee is not providing any expert or special assurance as to the Company's financial statements or any professional certification as to the independent outside auditor's work.

## COMPOSITION

The Committee shall be comprised of three or more directors as determined by the Board, each of whom the Board has determined (a) meets the independence requirements of the New York Stock Exchange ("NYSE") and the SEC, (b) meets the independence requirements under the Company's Standards for Director Independence; (c) is financially literate, and (d) qualifies as an "audit committee financial expert" as defined by SEC rules. Committee members may enhance their familiarity with finance and accounting by participating in educational programs conducted by the Company or an outside consultant.

No director may serve as a member of the Committee if such director serves on the audit committees of more than two other public companies unless the Board determines that such simultaneous service would not impair the ability of such director to serve effectively on the Committee, and discloses this determination in the Company's annual proxy statement. No member of the Committee may receive, directly or indirectly, any

compensation from the Company other than (i) director's fees, which may be received in cash, common stock, equity-based awards or other in-kind consideration ordinarily available to directors; (ii) a pension or other deferred compensation for prior service that is not contingent on continued service; and (iii) any other regular benefits that other directors receive.

The members of the Committee are appointed by the Board and serve until their successors are duly appointed or until their retirement, resignation, death or removal by the Board. Unless a Chair is elected by the full Board, the members of the Committee may designate a Chair by majority vote of the full Committee membership.

**MEETINGS**

The Committee shall meet at least four times per year, or more frequently as circumstances dictate. To the extent practicable, each of the Committee members shall attend each of the regularly scheduled meetings in person. A majority of the Committee members currently holding office constitutes a quorum for the transaction of business. The Committee shall take action by the affirmative vote of a majority of the Committee members present at a duly held meeting or by written action signed in the manner and by the number of Committee members required under the Company's Articles of Incorporation and Bylaws and applicable law. The Chair shall convene and chair meetings of the Committee, set agendas for meetings, and determine the Committee's information needs. In the absence of the Chair at a duly convened meeting, the Committee shall select a temporary substitute from among its members. As part of its job to foster open communication, time shall be periodically set aside at meetings for the Committee to meet with management (including the Company's Chief Executive Officer and Chief Financial Officer), the independent outside auditor and the General Auditor function in separate sessions to discuss any matters that the Committee or each of these groups believe should be discussed privately. The Committee will meet in regularly scheduled executive sessions without any members of management. The Committee may ask members of management or others to attend the meetings and provide pertinent information, as necessary. All other Board members have a standing invitation to attend meetings of the Committee.

**RESPONSIBILITIES AND DUTIES**

The Committee shall be subject to the following principles and shall undertake the following responsibilities and duties.

**Documents/Reports Review**

- Meet to review and discuss with management and the independent outside auditor the Company's annual and quarterly financial statements, including reviewing the Company's specific disclosures under Management's Discussion and Analysis of Financial Condition and Results of Operations. Based on its discussions with management and the independent outside auditor, the Committee shall recommend to the Board of Directors whether the Company's annual financial statements should be included in the Company's Annual Report on Form 10-K (or the Annual Report to Shareholders).

- Review the Annual Report on Form 10-K prior to filing.

- Discuss with management earnings press releases, as well as financial information and earnings guidance provided to analysts and rating agencies. Discussion of earnings releases as well as financial information and earnings guidance may be done in a general manner (i.e., discussions of the types of information to be disclosed and the type of presentation to be made).

- Discuss significant findings and recommendations of the Company's independent outside auditor and the General Auditor and internal auditors, together with management's responses to those findings and recommendations.

- Review and discuss with the Company's Chief Executive Officer and Chief Financial Officer the procedures undertaken in connection with the Chief Executive Officer and Chief Financial Officer certifications for Forms 10-K and Forms 10-Q, including their evaluation of the Company's disclosure controls and procedures and internal controls.

- Prepare the report required by SEC rules to be included in the Company's annual proxy statement.

**Independent Outside Auditor**

- Make all decisions relating to the selection, evaluation, retention, oversight and replacement of the Company's independent outside auditor, and approve all fees and other terms of the Company's independent outside auditor. On an annual basis, the Committee shall receive from the independent outside auditor and review a report describing: the auditor's internal quality-control procedures; any material issues raised by the most recent internal quality-control review, or peer review, of the auditor, or by any inquiry or investigation by governmental or professional authorities, within the preceding five years, respecting one or more independent audits carried out by the auditor, and any steps taken to deal with any such issues; and, to assess the auditor's independence, all relationships between the auditor and the Company consistent with Independence Standards Board Standard No. 1 (as modified or supplemented). The Committee is responsible for actively engaging in a dialogue with the independent outside auditor with respect to any disclosed relationship or services that may impact the objectivity and independence of the independent outside auditor and take appropriate action in response to the independent outside auditor's report to satisfy itself of the auditor's independence. The independent outside auditor shall report directly to the Committee.

- Pre-approve, or adopt appropriate procedures to pre-approve, all audit and non-audit services and fees to be provided by the independent outside auditor, and consider whether the auditor's provision of non-audit services to the Company is compatible with maintaining the independence of the independent outside auditor.

- Review and evaluate the performance, qualifications and independence of the Company's independent outside auditor, taking into account the opinions of management, the General Auditor and the internal auditors.

- Review and evaluate the qualifications, performance and independence of the lead partner of the independent auditor, oversee proper rotation of the lead partner and other audit partners serving the account as required under SEC independence rules, and periodically evaluate whether there should be a rotation of the audit firm itself.

- Periodically consult with the Company's independent outside auditor, outside of the presence of management, about the auditor's judgments about the quality, and not just the acceptability, of the Company's accounting principles as applied to its financial reporting, and the Company's internal controls and the fullness and accuracy of the Company's financial statements.

- Obtain from the independent outside auditor in connection with any audit a report relating to the Company's annual audited financial statements describing all critical accounting policies and practices to be used, all alternative treatments of financial information within generally accepted accounting principles that have been discussed with management, ramifications of the use of such alternative disclosures and treatments, and the treatment preferred by the independent outside auditor, and any material written communications between the independent outside auditor and management, such as any "management" letter or schedule of unadjusted differences.

- Obtain from the independent outside auditor assurance that the audit was conducted in a manner consistent with Section 10A of the Securities Exchange Act of 1934, as amended, which sets forth certain procedures to be followed in any audit of financial statements required under the Exchange Act.

- Discuss the scope of the annual audit plans for the independent outside auditor.

- Establish policies governing the hiring by the Company of any current or former employee of the Company's independent outside auditor.

**Internal Audit**

- Review and approve the annual audit plans for the internal audit function and all material changes to such plans.

- Review and concur in the appointment and termination of the General Auditor.

- Periodically review and approve changes (if any) to the internal audit charter.

- Review significant internal audit results, including any problems or difficulties, together with management's action plans.

- Discuss regularly with the Company's General Auditor, the budget and staffing of the internal audit function, including responsibilities, organizational structure, auditor qualifications, and quality assurance reviews.

- Review the qualifications, performance and objectivity of the internal audit function.

**Enterprise Risk Management**

- Review with management, the Company's enterprise risk management framework, including the governance structure, the guidelines and policies for assessing, identifying, managing, monitoring and reporting of significant risks.
- Meet periodically with management to review the Company's significant risks and the steps management has taken to monitor, control or mitigate such risk.

**Financial Reporting Processes**

- In consultation with the Company's independent outside auditor, the General Auditor, and the internal auditors, consider the integrity of the Company's financial reporting processes, both internal and external.

- Discuss with management, the independent outside auditor, the General Auditor and the internal auditors, as appropriate: (a) any major issues regarding accounting principles and financial statement presentations, including any significant changes in the Company's selection or application of accounting principles, and major issues as to the adequacy of the Company's internal controls and any special audit steps adopted in light of material control deficiencies; (b) analyses prepared by management and/or the independent outside auditor setting forth significant financial reporting issues and judgments made in connection with the preparation of the financial statements, including analyses of the effects of alternative GAAP methods on the financial statements; (c) the effect of regulatory and accounting initiatives, as well as off-balance sheet structures, on the financial statements of the Company; and (d) the type and presentation of information to be included in earnings press releases (paying particular attention to any use of "pro forma" or "adjusted" non-GAAP information).

**Process Analysis and Review**

- Establish regular and separate systems of reporting to the Committee by each of management, the General Auditor, and the independent outside auditor regarding any significant judgments, changes or improvements that have been made in management's preparation of the financial statements and the view of each as to appropriateness of such judgments.

- Discuss with the independent outside auditor, at least annually, any audit problems or difficulties and management's responses, any difficulties the auditor encountered during the course of the audit work, including any restrictions on the scope of the auditor's activities or on access to requested information, and any significant disagreements with management. The discussions with the independent outside auditor should address, to the extent applicable, any accounting adjustments that were noted or proposed by the independent outside auditor but were "passed" (as immaterial or otherwise), any communications between the audit team and its national office with respect to auditing or accounting issues presented by the engagement; and any "management" or "internal control" letter issued, or proposed to be issued, by the independent outside auditor to the Company.

- Discuss, at least annually, with the independent outside auditor the matters required to be discussed under Statement on Auditing Standards 61, as amended by AU Section 380, as adopted by the PCAOB, as it may be modified or supplemented.

- Discuss any significant disagreement between management and the independent outside auditor in connection with the preparation of the financial statements, and resolve any disagreements between management and the independent outside auditor regarding financial reporting.

- Inquire of the Company's Chief Executive Officer and Chief Financial Officer as to the existence of any significant deficiencies in the design or operation of internal controls that could adversely affect the Company's ability to record, process, summarize and report financial data, any material weaknesses in internal controls, and any fraud, whether or not material, that involves management or other employees who have a significant role in the Company's internal controls.

**Other Activities**

- Consider any tax issues, legal and regulatory matters or employee complaints or similar matters brought to the attention of the Committee that may have a material impact on the Company's financial statements or accounting policies.

- Review with management the system the Company has in place to ensure that the Company's financial statements, reports, and other financial information disseminated to governmental organizations and the public satisfy legal requirements.

- Discuss and evaluate with management the Company's investment policy.

- Establish procedures for the receipt, retention and treatment of complaints received by the Company regarding accounting, internal accounting controls or auditing matters, and for the confidential, anonymous submission by Company employees of concerns regarding questionable accounting or auditing matters.

- Review and approve related-person transactions, consistent with the Company's Related-Person Transactions Approval Policy.

- Report regularly to the Board on Committee actions and any significant issues considered by the Committee.

- Perform such other functions as assigned by law, the Company's Articles of Incorporation or Bylaws, or the Board.

- Review with the Chief Compliance and Ethics Officer at least annually the effectiveness of the Company's Compliance and Ethics program.

- Review reports from the Chief Compliance and Ethics Officer regarding compliance with its Code of Business Conduct and Ethics and Principles of Ethics and Integrity.

- Receive and review periodic reports regarding matters relating to the Company's compliance with legal and regulatory requirements from the Chief Compliance and Ethics Officer, who has express authority to communicate directly with the Audit Committee as necessary.

**DELEGATION**

The Committee may, in its discretion, form and delegate authority to subcommittees when appropriate and to the extent permitted by the listing standards of the NYSE. The Committee may, in its discretion, delegate to one or more of its members the authority to pre-approve any audit or non-audit services to be performed by the independent outside auditor, provided that any such approvals are presented to the Committee at its next scheduled meeting. Any member of the Audit Committee is authorized to meet (in person or by telephone) with the Company's independent outside auditor in connection with the independent outside auditor's required communications with the Audit Committee prior to issuance of its consent to the Company's filings with the SEC; provided, however, that such Committee member provides an update of such meeting with the independent outside auditor to the full Audit Committee at its next regularly scheduled meeting.

**PERFORMANCE EVALUATION**

The Committee shall conduct an annual performance evaluation of the Committee, which evaluation shall compare the performance of the Committee with the requirements of this charter. The performance evaluation shall also include a review of the adequacy of this charter and shall recommend to the Board any revisions to this charter deemed necessary or desirable, although the Board shall have the sole authority to amend this charter. The performance evaluation shall be conducted in such manner as the Committee deems appropriate.

**RESOURCES AND AUTHORITY OF THE COMMITTEE**

In discharging its role, the Committee is empowered to inquire into any matter it considers appropriate to carry out its responsibilities, with access to all books, records, facilities and personnel at the Company. The Committee shall have the resources (including funding) and authority necessary or appropriate to discharge its duties and responsibilities, including conducting investigations into any matters within the Committee's scope of responsibilities, the selection, retention, termination and approval of fees and other retention terms of special counsel, accountants, or other experts or consultants, as it deems necessary or appropriate, and funding for ordinary administrative expenses of the Committee, without seeking approval of the Board or management.