February 6, 2015

Karen DeSalvo, MD, MPH, MSC
National Coordinator for Health Information Technology
Office of the Secretary, Department of Health and Human Services
200 Independence Ave., S.W., Room 7-729D
Washington, D.C. 20201

Re: Comments on Draft Federal Health IT Strategic Plan 2015-2020

Dear Dr. DeSalvo:

Thank you for the opportunity to provide comments on the Federal Health IT Strategic Plan for 2015-2020. Any health care strategic plan should have as its highest priorities (a) the safety of patients, (b) the protection of fundamental patient rights that are essential for quality health care and (c) the promotion of the ethical practice of medicine and psychiatry. Yet the Federal Health IT Goals on page 8 of the draft strategic plan are "collection, share and use" of health information and the top priority is "Expand Adoption of Health IT."

Both HHS and Congress have found that health information privacy is a "fundamental right" of all Americans.[1] HHS has further determined that the right to privacy of health information "is necessary to secure effective, high quality health care."[2] In fact, HHS has found that the entire health care delivery system is based on protection of the individual's right to privacy.[3] The Supreme Court has also found that the effectiveness of mental health services is "rooted in the imperative need for confidence and trust" and even "the mere possibility of

[1] HHS finding: "Privacy is a fundamental right. As such, it must be viewed differently than any ordinary economic good." 65 Fed. Reg. at 82,464 (Dec. 28, 2000). "Congress finds that. . . the right to privacy is a personal and fundamental right protected by the Constitution of the United States." The Privacy Act of 1974, section 2(a)(4).
[2] 65 Fed. Reg. at 82,467.
[3] HHS finding: "In short, the entire health care system is built upon the willingness of individuals to share the most intimate details of their lives with their health care providers." 65 Fed. Reg. at 82,467.

disclosure" may impede the development of the confidential relationship necessary for successful treatment.[4]

The President has also recently reaffirmed the importance of personal privacy in this Administration:

> One thing should be clear, even though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion that privacy is an outmoded value. It has been at the heart of our democracy from its inception, and we need it now more than ever. (Emphasis supplied.)[5]

Recognition and protection of the individual's fundamental right to privacy should be set forth as part of the Mission of ONC on page 3 and the number one guiding principle on page 7.

Goal 2 of the draft plan reads "Advance Secure and Interoperable Health Information," but HHS has long conceded "there is no such thing as a totally secure [electronic health information] system that carries no risk to security." 68 Fed. Reg. at 8346 (Feb. 20, 2003). So objectives such as enabling individuals, providers and public health entities "to securely send, receive, find and use electronic health information" and advancing standards "to support secure and interoperable health information" (Objectives A and B under Goal 2) are false promises and objectives that have never been achieved and will not likely be achieved in the five years covered by the plan, if ever.

ONC should eliminate statements in its strategic plan that give the public the false impression that electronic health information systems can be made secure and should expressly inform the public that "there is no such thing" as a secure electronic health information system. In addition, the strategic plan should state the reasons why these systems present a greater threat to patient privacy than paper records. The plan should inform the public that the nation's

[4] Jaffee v. Redmond, 116 S. Ct. 1923, 1928 (1996).
[5] Letter from President Barack Obama to the American People (Feb. 23, 2012).

most prominent experts in health IT have determined that health IT makes it possible, "for the first time in the history of medicine" to

> Improperly disclose identifiable health information of millions of individuals 'in a matter of seconds';
>
> Steal health information without having physical access to it and from locations that may be beyond the reach of U.S. laws; and
>
> Breach an individual's PHI in a manner that makes it impossible to restore." [footnotes omitted][6]

The fact that electronic health information systems make possible massive privacy breaches on an unprecedented scale has been illustrated most recently by the apparent sophisticated hack of millions of electronic health records at Anthem.[7]

Essential facts

The Strategic Plan should also set forth facts that are essential to establishing a strategy that is consistent with ONC's "vision" and "mission" (page 3 of the draft). For example, the draft states that "as of June 2014, 75 percent (403,000+) of the nation's eligible professionals and 92 percent (4,500+) of eligible hospitals received incentive payments from the EHR incentive program" (page 4 of the draft). However, the draft should also mention that during the same 5 years during which HHS was paying more than $30 billion in incentives to get practitioners and providers to become "meaningful users" of health IT, more than 41 million Americans had their health information privacy breached mostly in incidents involving electronic health IT systems.[8] This is more than the total number of people residing in Canada or in any state in the U.S. This number could

[6] "The Financial Impact of Breached Protected Health Information," p. 15, American National Standards Institute (March 2012).
[7] "Millions of Anthem Customers Targeted in Cyberattack," New York Times (Feb. 5, 2015) http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html?_r=0.
[8] "Reporting HIPAA Breaches: A New Approach," Data Breach Today (Jan. 26, 2015) http://www.databreachtoday.com/reporting-hipaa-breaches-new-approach-a-7830/p-2.

be increased by 80 million depending on the details of the recent electronic hack involving Anthem.[9]

The rate of breaches and thefts in health IT systems is on the rise with other nations launching attacks on electronic health information systems in the U.S. and using the information to commit fraud and identity theft.[10] There were nearly 4 million more health records stolen in 2014 than in any previous year.[11]

The strategic plan should acknowledge that the public is losing confidence in the ability of health IT systems and privacy laws to protect the privacy of their health information.[12] This has resulted in patients withholding information from electronic health information systems.[13] ONC has found:

> If individuals and other participants in a network lack trust in electronic exchange of information due to perceived or actual risks to electronic health information or the accuracy and completeness of such information, it may affect their willingness to disclose necessary health information and could have life-threatening consequences. (emphasis supplied)[14]

Medical identity theft victims have experienced misdiagnoses, mistreatment, delay in treatment, and being prescribed the wrong drugs.[15] These

[9] "Hackers Breach Anthem, 80M Exposed," Modern Healthcare (Feb. 4, 2015) http://www.modernhealthcare.com/article/20150204/NEWS/302049928?utm_source=modernhealthcare&utm_medium=email&utm_content=20150204-NEWS-302049928&utm_campaign=mh-alert.
[10] "China Suspected in Major Hacking of Health Insurer", Washington Post (Feb. 5, 2015) http://www.washingtonpost.com/business/economy/investigators-suspect-china-may-be-responsible-for-hack-of-anthem/2015/02/05/25fbb36e-ad56-11e4-9c91-e9d2f9fde644_story.html
[11] "2015 Could Be the Year of the Hospital Hack", MIT Technology Review (Dec. 23, 2014) http://www.technologyreview.com/news/533631/2015-could-be-the-year-of-the-hospital-hack/
[12] "80% of Patients Worry About Health Data Security", Forbes (Dec. 4, 2014) http://www.forbes.com/sites/brucejapsen/2014/12/04/4-in-5-patients-remain-concerned-about-health-data-security/
[13] "Nearly Half of Patients Withheld Info in Their EHR", Health Data Management (Dec. 16, 2014) http://www.healthdatamanagement.com/news/Nearly-Half-of-Patients-Withheld-Info-in-Their-EHR-49450-1.html; "Provider Use of EHRs Could Deter Patient Disclosure, Study Finds", iHealth Beat (July 21, 2014) http://www.ihealthbeat.org/articles/2014/7/31/study-provider-use-of-ehrs-could-deter-patient-disclosure
[14] "Guide to Privacy and Security of Health Information", Office of the National Coordinator, pp. 5 and 28.
[15] "Medical Identity Theft Hits Growth Phase", Healthcare IT News (Sept. 12, 2013) http://www.healthcareitnews.com/news/medical-identity-theft-numbers-grow

are clearly issues that must be addressed in the five year strategic plan if health IT is to be successful.

Specific Recommendations

1. **The strategic plan should not expand the adoption of health IT until it is proven safe for patients and effective in reducing health care costs.**

The draft says that "evidence suggests" health IT improves patient safety, and the federal government is "positioned to improve health, health care, and reduce costs through the secure use of information and technology." Draft at pp. 4 and 11. Section 13424(e) of the HITECH Act required GAO to provide a report to Congress by March 2014 describing the impact of the act on "overall health care costs" and "reduction in medical errors." In its report to Congress in response to this statutory directive[16], GAO found it could not provide that information to Congress for the following reasons:

> However, although HHS, CMS, and ONC have established important performance measures for the goals related to adoption and meaningful use of EHRs, **they have not established measures linked to the second category of goals, which would help them to track program outcomes such as health care quality, efficiency, and patient safety**.
>
> Furthermore, ONC has acknowledged the need to develop performance measures to track patient safety, in part due to **concerns that EHRs could have some unintended consequences that cause patient harm**. However, ONC has not yet developed these potential measures. (footnote omitted which cites a program started in July 2013 to begin collecting data on medical errors in health IT. http://www.healthit.gov/sites/default/files/safety_plan_master.pdf)

[16] "Electronic Health Record Programs: Participation Has Increased But Action Needed to Achieve Goals, Including Improved Quality of Care," GAO-14-207, p. 3, n. 12 citing the requirements of section 13424(e).

> Another area that merits attention relates to HHS's ability to ensure that the EHR programs are on track to meet their goals. **While the EHR programs are ultimately intended to improve outcomes such as health care quality, efficiency, and patient safety, the agencies have not established performance measures for monitoring progress toward achieving these improvements.** Although HHS expects that EHRs can help achieve improved outcomes as well as support various other health care reform efforts that are also intended to improve care, **that result is not yet assured**.
>
> CMS and ONC officials have indicated that they do not expect to observe progress toward achieving the intended outcomes of improved health care quality, efficiency, and patient safety until at least Stage 3 of the EHR programs, **which is not expected until 2017.** [17]

So ONC has prevented GAO from making the statutorily required report to Congress by failing to establish measures and goals for safety and cost reduction in the five years since the HITECH Act was enacted.

In fact, numerous studies have shown that health IT is adding medical errors and health care costs.[18] HHS has acknowledged that complying with the regulations that implement the HITECH Act and HIPAA will take *32 million hours annually*. See 78 Fed. Reg. 54467 (Sept. 4, 2013). Using HHS' suggested hourly rate, that will add $2 billion annually to health care costs and $20 billion over the budget horizon used by the Congressional Budget Office. This estimate is likely to be low in view of the fact that most health privacy breaches go unreported, and the cost of class action lawsuits for breaches was not included. See 78 Fed. Reg. at 5669/2, 56671/2. Of course, to this cost must be added the more than $30

---

[17] Id. at pp. 40-43.

[18] "Debate Heats Up Over Safety of Electronic Health Records," USA Today (Feb. 3, 2015) http://www.usatoday.com/story/news/nation/2015/02/03/patient-safety-electronic-health-records-hhs/22765699/; "Feds Move Into Digital Medicine, Face4 Doctor Backlash", USA Today (Feb. 1, 2015) http://www.usatoday.com/story/news/nation/2015/02/01/backlash-against-electronic-medical-records/21693669/; "Promise of EMR Systems Yet to Be Fulfilled for Many; Main Gripes: Divided Attention, More Work, Costs", General Surgery News (Dec. 2014) http://www.generalsurgerynews.com/ViewArticle.aspx?d=In%2Bthe%2BNews&d_id=69&i=December+2014&i_id=1134&a_id=29071.

billion in "incentives" paid under the HITECH Act, the costs of defending audits and investigations by OCR, the fines imposed for HIPAA violations, the costs of defending class action law suits for breaches involving thousands of patients and the costs of lost reputation and business when electronic breaches occur.[19]

ONC should provide the information to Congress required by the HITECH Act with respect to whether health IT has actually reduced health care costs and medical errors over the past five years and should establish benchmarks to make that assessment beginning with the initial "meaningful use" incentives.

2. **The strategic plans should require *informed* patient choice in the disclosure of health information consistent with patients' rights under statutes, privileges and standards of ethics.**

The draft states that the federal government is committed to encouraging the development and use of policy and technology "to advance patients' rights to access, amend and make choices for the disclosure of their electronic health information. (emphasis supplied). Draft at p. 16. The draft also states that the federal government supports policy and technology "to facilitate patients' ability to control the disclosure of specific information that is considered to be sensitive in nature (such as information related to substance abuse treatment, reproductive health, mental health, or HIV) in an electronic environment." (Emphasis supplied.)

We strongly support protection of the patients' right to control the use and disclosure of sensitive health information and believe patients should have the right to make an *informed* choice about whether specific sensitive health information should be included in an electronic health record. This means, of course, that patients must be informed that such systems cannot be made secure and that if their health information is stolen electronically, their health information privacy can never be restored.[20]

[19] See "The Financial Impact of Breached Protected Health Information," supra at p. 44.

[20] See statement by security expert: "If someone gets your credit card number, you cancel it. If you have HIV, and that gets out, there's no getting that back." "China Suspected in Major Hacking of Health Insurer," Washington Post (Feb. 5, 2015) http://www.washingtonpost.com/business/economy/investigators-suspect-china-may-be-responsible-for-hack-of-anthem/2015/02/05/25fbb36e-ad56-11e4-9c91-e9d2f9fde644_story.html.

Section 13405(a) of the HITECH Act affords individuals the right to obtain restrictions on the disclosure of their health information to a health plan for payment or health care operations purposes if they pay out of pocket for the health care item or service. Section 3002(b)(2)(B)(i) requires the consideration of technologies that protect the privacy of sensitive health information with the goal of minimizing the reluctance of patients to seek care because of privacy concerns. HHS has determined that more than 2 million Americans each year fail to seek mental health treatment because of privacy concerns at a cost of nearly $1 billion.[21] Section 13421(c) of the HITECH Act provides that nothing in the act or HIPAA shall be construed to waive any "privilege" otherwise applicable to health information. The Supreme Court has expressly recognized a "psychotherapist-patient privilege" that prevents the disclosure of communications between a psychotherapist and a patient without the patient's consent.[22]

HHS requires the "minimum necessary" provisions of the HIPAA privacy rule to be applied in a manner that is "consistent with, and [does] not override professional judgment and standards" for the ethical practice of medicine and psychiatry.[23] Standards of ethics of professions that handle especially sensitive health information, such as mental health information, have strong privacy standards. See, for example, the standards of the American Psychoanalytic Association:

> **IV. Confidentiality.** Confidentiality of the patient's communications is a basic patient's right and an essential condition for effective psychoanalytic treatment and research. A psychoanalyst must take all measures necessary to not reveal present or former patient confidences without permission, nor discuss the particularities observed or inferred about patients outside consultative, educational or scientific contexts.[24]

See similarly the ethics standards for the National Association of Social Workers:

[21] 65 Fed. Reg. at 82,777-779.
[22] Jaffee v. Redmond, 116 S. Ct. 1923 (1996).
[23] 67 Fed. Reg. at 53,197 (Aug. 14, 2002); 65 Fed. Reg. at 82,544 (Dec. 28, 2000).
[24] "Principles and Standards of Ethics for Psychoanalysts," American Psychoanalytical Association (June 2008).

> Social workers may disclose confidential information when appropriate with valid consent from a client or a person legally authorized to consent on behalf of a client.[25]

Accordingly, the strategic plan should clearly state that the strategy will protect the patient's statutory right to pay privately to prevent the disclosure of sensitive health information, that the strategy will provide for the segregation of highly sensitive health information such as "psychotherapy notes", that it will support, and not be inconsistent with, standards of professional ethics and that it will respect and preserve all privileges.

3. **<u>The strategic plan should include specific objectives, milestones and metrics for the protection of the patients' right to health information privacy.</u>**

Section 3001(c)(3) of the HITECH Act requires the ONC strategic plan "to include specific objectives, milestones, and metrics with respect to . . . the incorporation of privacy and security protections for the electronic exchange of an individual's individually identifiable health information." The plan contains no specific objectives, milestones or metrics with respect to protecting health information privacy.

The plan describes a strategy of using standard terminology and vocabulary with respect to health information privacy (draft at pp. 13-14). However, there is no objective designed expressly to protect the patient's right to health information privacy, nor is there any standard, or reference to a standard, that defines the term "privacy". It is difficult to see how a strategic health IT plan can protect the patient's right to privacy if the right is not mentioned and "privacy" is not defined.

Given that one of the federal "health IT principles" mentioned in the plan is to "respect individual preferences" and provide "person-centered care" that honors the individuals' "privacy needs, values, and choices regarding their

[25] "Code of Ethics, National Association of Social Workers," section 1.07(b) (2008).

information, health, and care"(draft p. 4), the plan should clearly state that an objective will be to protect the individual's right to health information privacy and that this right encompasses the right of the individual to decide who sees what health information and whether that any particular health information should be excluded from an electronic health record.

We appreciate the opportunity to provide comments on the draft strategic plan and are prepared to support any plan that recognizes and protects the patients' right to health information privacy and choice with respect to the information that goes into an electronic health system.

Sincerely,

James C. Pyles
Counsel