May 10, 2010

Markle Connecting for Health Collaborative Statement on the Issuance of Proposed Regulations to Establish Certification Programs for Health Information Technology

This paper represents a collective view that was deeply informed by the many and diverse collaborators of Markle Connecting for Health.

We submit these comments in response to the Notice of Proposed Rule Making (NPRM) issued by the US Department of Health and Human Services (HHS) establishing a "permanent" program for the testing and certification of health information technology (health IT).[1]

I. Introduction

Certification is primarily a way of enforcing that products meet certain criteria or standards. It can exert a powerful influence on products and markets—an influence that is particularly potent when the certification program is run or sanctioned by government. It is therefore critical that any certification program with government imprimatur be structured carefully to support clear public policy goals and avoid unnecessary restraints on market innovation.

The American Recovery and Reinvestment Act of 2009 (ARRA) authorizes the National Coordinator for Health Information Technology to establish a voluntary certification program or programs for health IT.[2] Although the proposed HHS program for testing and certifying EHR technology is technically voluntary, it will play a pivotal role in triggering eligibility for approximately $34 billion in stimulus funding and consequently will have a high degree of influence over technology development and choice in a rapidly changing health IT market. For these reasons, HHS must structure the certification program carefully to focus only on those elements that are necessary to achieving its policy goals while avoiding unintended consequences.

Overall, the proposed program takes an appropriately measured approach to certification, as evidenced by its independence, limits in scope, emphasis on privacy and security, and flexibility for future innovations. The proposed rule aligns with many of the principles and recommendations this Collaborative has previously made.[3] In particular:

- It separates the parties responsible for developing the certification requirements from the parties that will perform the certification of products, and allows for a plurality of such certification services.

---

1 Proposed Establishment of Certification Programs for Health Information Technology; Proposed Rule. 75 Federal Register 46 (March 10, 2010), pp. 11,327-11,373.

2 Public Law 111-5, Section 3001(c)(5)(A) (enacted February 17, 2009).

3 See the following collaborative responses: "Comments on CMS's proposed rulemaking for the EHR Incentive Program" (PDF, 408K), available at http://www.markle.org/downloadable_assets/20100315_ehrincent_cms0033p.pdf; "Comments on the ONC's Interim Final Rule" (PDF, 196K), available at http://www.markle.org/downloadable_assets/20100315_ehrtechifrrule.pdf.

- It allows for innovation by maintaining the "minimum necessary" approach to standards and certification criteria to support Meaningful Use. [4]

- It establishes a transparent process through the National Institute of Standards and Technology (NIST) for developing the methods that will be used to test qualified health IT against the certification requirements.

Even amid these encouraging directions in the NPRM, the positioning and future scope of a government-run or government-sanctioned certification program for health IT must be thought through now. Certification can be a tool for achieving some public policy goals, but it is good for some objectives and not for others. The role of HHS-sanctioned testing and certification is an important but limited one. We discuss below why HHS should not rely too heavily on certification to achieve all of its public policy objectives for health IT.

The comments below, which were developed in collaboration with a wide array of organizations and individuals, recommend the following:

- **HHS should create clear, standard language about the purpose and goals of its certification program, and its limitations** in addressing important public policy questions raised by the adoption and use of health IT. HHS should establish "labeling" requirements for certified products that are consistent and clear to help providers and purchasers understand the scope of the testing and certification under the HHS program to implement ARRA financial incentives. In particular, the standard language should communicate the scope of certification, as well as its limitations both in terms of implementation experience and privacy and security.

- **HHS should clarify the rules by which EHR modules may be exempt** from testing against all privacy and security certification criteria.

- **Except for the specific circumstances in which such services are being used to help health care providers and hospitals qualify for Meaningful Use incentives under ARRA, HHS should limit the scope of extending the current certification program to other forms of health IT** such as electronic personal health records (PHRs) or health information exchanges (HIEs). In the eyes of the HHS-sanctioned testing and certification program, PHRs and HIEs should only be considered when packaged as EHR modules. In other words, when they are offered as components of a complete EHR or an EHR bundle, they may be tested and certified under the same rules as EHR modules, based on the limited scope of Meaningful Use. Otherwise, the public policy benefits are not clear for certifying PHRs or HIEs outside of the Meaningful Use context.

- **HHS should clarify the type and scope of modifications that would require a product to be recertified.**

Details of our recommendations are set forth below.

---

[4] "Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology; Interim Final Rule." 75 Federal Register 8 (13 January 2010), pp. 2,014–2,047.

II. General Comments: Certification Goals, Purpose, and Limitations

The proposed HHS-sanctioned testing and certification program aims to offer basic assurance that certified technology is capable of supporting providers' achievement of Meaningful Use goals. Although it may be tempting to believe that a stamp of certification will solve all potential problems faced in implementing health IT, it is vital to recognize the areas where certification can indeed be helpful in accelerating the Meaningful Use goals and where it has inherent limitations. The challenge for the Office of the National Coordinator for Health Information Technology (ONC) is not only in distinguishing between the two, but also in communicating to providers what HHS-sanctioned testing and certification will mean—and not mean—for them.

Role of Certification

HHS-sanctioned testing and certification should be used only where it is well matched to an objective and where it provides a compelling benefit to both purchasers and users. HHS-sanctioned testing and certification serve two primary roles:

- **Provide basic assurance that technology can meet the technology-dependent elements of Meaningful Use and key technology-dependent components of privacy and security.** In this respect, certification provides confidence that a product is not misstating its certified technical capabilities with regard to Meaningful Use criteria.

- **Test interoperability capabilities.** NIST is charged with developing the conformance test methods (test procedures, test data, and test tools) to assess compliance with the Meaningful Use technical requirements and standards. NIST is well suited to this task; it has performed similar roles for other aspects of IT. Appropriately, the test methods will be developed through an open and transparent process and will provide an objective tool for evaluating qualified health IT against adopted interoperability criteria.

Critically, HHS-sanctioned testing and certification cannot be the only mechanism for instilling confidence in providers and patients that EHR technology can be used safely and effectively. The acquisition of certified technology, by itself, does not guarantee that it will be implemented and used to support the goals of Meaningful Use, and to establish strong privacy and security protections.

Certification is not a proxy for strong privacy and security protections. Establishing trust requires a comprehensive framework of policies and practices.

Specifically, certification is not a proxy for the enforcement of a regulatory framework and it cannot substitute for the complete framework of privacy and security protections necessary for trust among users of qualified health IT. In other words, the existence of privacy and security capabilities in technology does not mean that privacy and security protections will be correctly implemented, or that a user's policies and practices will use and further support these capabilities.

As we have said in the past, establishing and maintaining trust in health IT—from the public and medical professionals alike—requires a complementary comprehensive framework of privacy and security protections. [5]

The trust framework is built on three pillars: implementation of core privacy principles based on fair information practices, adoption of sound network design characteristics where technology requirements fulfill and bolster the privacy and security objectives, and strong oversight and accountability mechanisms. HHS-sanctioned testing and certification is one way for the federal government to ensure that EHR technology include core technical functions that support policy goals. But such technical functions should follow policy, and not establish it.

In general, privacy practices are not primarily attributable to software. Rather, they depend on behavioral conformance to a broad set of policies. These policies must be carried out mostly not by those who develop the technology and get it certified, but rather by those who implement it and use it in a variety of heterogeneous implementations in the field.

HHS-sanctioned testing and certification can help providers know whether they are getting *some* of the capabilities they need to support Meaningful Use requirements, including certain privacy-protective capabilities. However, by itself, certification says little about which of these capabilities are actually used in the field, whether they are correctly implemented or supported, or whether they are enforced through an organization's policies and practices. For example, technical aspects of the privacy and security framework certification may test whether a technology is capable of keeping immutable audit logs or maintaining access controls. It does not, however, detect whether these features are correctly used by the organization, maintained or monitored, nor does it determine whether other elements of a trust framework are in place, such as policies for access to information, transparency, consent, authorization, authentication, enforcement mechanisms for failure to protect patient information, and mechanisms to address the circumstances when patient information is lost or misused. A critical task of health IT is to have the capabilities to enable and support these policies, but the existence of these capabilities is not the same as implementing or complying with the privacy and security practices in total.

Certification Provides Limited Assurances on the Integration and Implementation of EHR Technology

The proposed program evaluates products at "a point before implementation in the HIT lifecycle," noting that products will be tested and certified "independent of, and disassociated from, their potential operating environments."[6] This is an appropriate approach. ONC should resist the temptation to try to remedy the integration challenges for EHR modules by trying to certify every specific integration of modules.

Providers will benefit from the flexibility to use multiple modules to achieve Meaningful Use. This will allow them to find a host of products and services that meet the needs of their patients. However, certification cannot anticipate all of the future demands that will be made on technology once implemented, including how products will work together. Trying to certify that all EHR modules work

---

[5] See *Connecting Professionals: A Common Framework for Private and Secure Information Exchange* by Markle Connecting for Health. Available at http://www.connectingforhealth.org/commonframework/index.html.

[6] Proposed Establishment of Certification Programs for Health Information Technology; Proposed Rule. 75 Federal Register 46 (March 10, 2010), page 11342.

together across different implementation settings is a combinatorial impossibility; trying to do so would dramatically increase the cost and complexity of the certification process, delay the release of new technology, and offer very little general value to users.

To satisfy the need by purchasers to have confidence in health IT, it is important to look to other mechanisms beyond certification to assess how products are performing in the field. If a vibrant health IT market emerges, we expect that services will emerge to monitor developments, track implementation experience and provide expert and user reviews and commentary. This has occurred for technology in many other domains (e.g., Consumer Reports, cnet.com, ZDnet, and others).

Technology marches forward rapidly, so it is also critical that certification requirements do not lock in today's capabilities. Generally speaking, when it comes to features or specific functions, it is most important to emphasize *what* technology must achieve, rather than specify exactly *how* the technology will necessarily operate to achieve it. This lesson became clear to the Environmental Protection Agency (EPA) after they specified a particular type of technology for emission incentives instead of specifying a target emission rate against which market forces would innovate. In the Clean Air Act of 1970, these emission standards ultimately stifled innovation and created perverse incentives to keep old plants in operation and new cleaner plants idle. The standard mandated the use of a specific technology to reduce emissions (i.e., using scrubbers) in newly built plants. However, even when the same emission rate could be achieved by a more cost effective technology (e.g., low-sulfur coal), the old plants kept running scrubbers in full force. By imposing a product standard the Clean Air Act locked in the use of older products and facilities.[7]

Long-Term Success Requires a Clear Articulation and Focus on Public Policy Objectives

ONC's current certification and testing program is carefully designed to be limited in scope and is targeted to accomplish the public policy goal of ensuring that federal funds are spent only on EHR Technology that is capable of achieving meaningful use. The evolution and maintenance of the program over time raises additional considerations. In this respect, much can be learned from other programs in other sectors.

For example the Energy Star program was introduced by the EPA in 1992 under the authority of the Clean Air Act as a voluntary program designed to promote energy-efficient computers. The program has been expanded over the years, in partnership with the Department of Energy (DOE), and now covers 60 product categories.[8] Technically, the program is voluntary; however, the federal government is required to purchase Energy Star products, and consumers and businesses may qualify for a number of tax credits by purchasing or using Energy Star-certified products.[9]

Although the Energy Star program has helped to raise the energy efficiency of appliances and electronics, it has more recently been criticized for overly lax certification standards, out-of-date testing procedures,

---

7 United States Environmental Protection Agency, Office of Air and Radiation. "The Benefits and Costs of the Clean Air Act: 1970 to 1990." October, 1997.

8 "Energy Star Program: Covert Testing Shows the Energy Star Program Certification Process is Vulnerable to Fraud and Abuse," US Government Accountability Office (GAO-10-470), March 2010, p. 3 (hereinafter GAO Report).

9 See GAO Report, pages 5-6.

and little independent verification of standards compliance.[10] The Government Accountability Office (GAO) issued a report in March 2010 that concluded that the program was vulnerable to fraud and abuse.[11] On April 14, 2010, the EPA and the DOE announced they would accelerate efforts to bolster the verification, testing, and enforcement aspects of the program.[12]

The Energy Star program can be instructive to the domain of health IT. Voluntary certification is not without significant limitations. Prior to extending the program significantly into the future, it is important to carefully consider the certification experience with respect to other policy initiatives—for example, improving reliability of financial audits,[13] improving the quality of goods produced overseas,[14] and achieving a more sustainable environment[15]— before moving forward. At every step, a certification should be designed to address a clear public policy goal—with demonstrable results—and be limited to what is necessary to achieve that goal.[16]

III. Modifications and Clarifications

Recommendation 1: Give providers and purchasers clear guidance on the scope and limitations of the testing and certification program, and require consistent representations or "labeling" for certified products.

ISSUE: HHS-sanctioned testing and certification can be one mechanism to give providers confidence that qualified health IT has the capabilities for meeting some of the Meaningful Use requirements but providers must also be aware of the limitations.

RECOMMENDATION: Establish standard language or "labeling" requirements to help purchasers understand the value and the limitations of the HHS-sanctioned testing and certification program, and the specific criteria included in a product's certification. The labels should address the following:

- *Scope of certification:* Clarify that certification determines whether a product meets the necessary technical requirements for Meaningful Use, but does not reflect an assessment of user experience or implementation experience.

---

[10] Testimony of Mark Connelly, Consumer's Union, before the US Senate Committee on Energy and Natural Resources, March 19, 2009, http://energy.senate.gov/public/index.cfm?FuseAction=Hearings.Testimony&Hearing_ID=fca7d6fc-faee-5647-a738-1a423a317b30&Witness_ID=8f004236-17f4-4dd3-b275-6182019a8514.

[11] See generally GAO Report.

[12] "U.S. EPA, DOE Announce Changes to Bolster ENERGY STAR Program." April 14, 2010. Available at http://www.energy.gov/news/8847.htm .

[13] Jamal, Karim and Sunder, Shyam, "Regulation, Competition and Independence in a Certification Society: Financial Reports vs. Baseball Cards," June 11, 2007. Available at http://ssrn.com/abstract=912703.

[14] Chen, Ying-Ju and Deng, Mingcherng, "Mandatory vs. Voluntary Certification: Investment, Quality, and Information Asymmetry," July 25, 2008. Available at http://ssrn.com/abstract=1177023.

[15] "Certifiably Sustainable?: The Role of Third-Party Certification Systems." Report of a Workshop, National Research Council, Committee on Certification of Sustainable Products and Services, ISBN: 0-309-14712-3 (2010). Available at http://www.nap.edu/catalog/12805.html.

[16] Ibid, chapters 2 and 6.

- *Privacy and Security Considerations:* Clarify that certification alone is not a proxy for implementing the necessary policies and practices for privacy and security protection and cannot ensure compliance with them. Certification means only that some of the privacy and security capabilities exist in the technology, but that alone does not establish adequate privacy and security protections.

- *Applicable Certification Criteria:* Specify the criteria tested and met by the product.

- *Testing Conditions:* Specify the testing date, the version or release tested, and when applicable, which other EHR modules the product was tested with as a "bundle."

- *Applicable Privacy and Security Criteria in the case of Modules:* Specify the privacy and security criteria a product meets under HHS-sanctioned certification, and the privacy and security criteria it is exempt from meeting under the exceptions for modules.[17]

- *Limitations of Modular Integration:* Clarify that certification of EHR modules does not provide assurance that certified modules will work together seamlessly in their specific implementation.

There need to be effective mechanisms to monitor and enforce consistent representations or "labeling" for certified products.

RATIONALE: Implementing EHR technology can be challenging, and providers will need guidance before making a purchasing decision. HHS-sanctioned testing and certification could be confusing in the health IT marketplace because the term "certification" has been used differently for EHR technology over time. If certified products are required to make consistent representations and use common labeling language, it will provide a mechanism for conveying the general uses and limitations of certification and the specific criteria a product meets under the program.

For example, the NPRM's permissiveness on certification of "EHR modules" is important to encourage flexibility and innovation in the market. However, providers and purchasers must be aware that when EHR modules are independently certified under the program, it does not indicate that modules will integrate seamlessly or work together. It should be clearly articulated that modular certification is not the right tool for addressing seamless integration of various EHR modules.

Standard language or labels are one of many possible mechanisms that can be used to offer guidance in these areas and should be pursued in tandem with other complementary efforts. Specifically, ONC should also explore mechanisms to offer robust purchasing support through the Regional Extension Centers (RECs). Specifically, they should help providers evaluate products and their usability through workshops, and educational resources. HHS should also offer guidance and assistance to help providers of all sizes implement strong privacy and security policies and practices.

The NPRM gives ONC-Authorized Certifying Bodies (ONC-ACBs) the authority to make "qualitative factors" such as policies and conditions a requirement of certification.[18] We believe labels fall under the

---

[17] Proposed Establishment of Certification Programs for Health Information Technology; Proposed Rule. 75 Federal Register 46 (March 10, 2010), pp. 11,327-11,373, §170.450.

[18] Proposed Establishment of Certification Programs for Health Information Technology; Proposed Rule. 75 Federal Register 46 (March 10, 2010), Page 11,335.

scope of these qualitative factors, and would be allowable under the NPRM. ONC should create standardized language for all certified products.

Recommendation 2: Clarify the exceptions for certifying modules against privacy and security criteria.

ISSUE: The NPRM states that an EHR module must be tested against all privacy and security requirements, with three important exceptions.[19] An EHR module does not need to be tested independently against all privacy and security criteria if any of the following hold true:

- The module is tested as part of a "bundle" of modules that together comprise a "complete EHR." That is, if the bundle of modules together perform all of the functions necessary to comply with the certification criteria for a complete EHR, then each module within the cluster does not need to be tested independently for the privacy and security requirements.
- The module's vendor can demonstrate that it would be "technically infeasible" to perform specific privacy and security functions.
- The module performs only a subset of the privacy and security requirements. For example, if an EHR module performs only the encryption task of security requirements, it would not need to be assessed for tasks it does not perform.

The first exception requiring that bundles of EHR modules comprise a complete EHR is overly restrictive. Regarding the second exception, the phrase "demonstrate technical infeasibility" is vague and as written could lead to misunderstanding.

RECOMMENDATION:

- ONC should broaden the first exception so that bundles of EHR modules do not necessarily need to comprise a complete EHR in order to be tested as a bundle against the privacy and security requirements.
- Regarding the second exception, ONC should offer a simple, consistent set of conditions by which vendors may demonstrate that it would be technically infeasible for an EHR module to be certified against all privacy and security criteria.

RATIONALE: Allowing a certification process for bundles of EHR modules provides flexibility for rapid development, innovation, and response to market needs. However, requiring bundles to comprise a complete EHR is an unnecessarily rigid way to certify privacy and security related functions. For example, if a bundle of an e-prescribing module and a quality reporting module can produce a unified audit trail, it is clear that both those modules meet the audit trail requirement independently.

Little is gained by limiting the exception only to bundles that make up a complete EHR. It can be a deterrent to innovators who aspire to create modules for a specific aspect of Meaningful Use, but not the comprehensive set of solutions that make up a complete offering. As the NPRM is written, these vendors would not be able to test multiple modules as a bundle. However, to reiterate the previous

[19] Proposed Establishment of Certification Programs for Health Information Technology; Proposed Rule. 75 Federal Register 46 (March 10, 2010), pp. 11,328–11,373, §170.450.

recommendation, when modules are tested in bundles they should be labeled clearly and appropriately, including the particulars of what has been certified and the limitations.

Regarding the second recommendation, without more clarity, there is the risk that vendors and certifiers could have different expectations for the requirement to demonstrate technical infeasibility. It would be useful for ONC to issue guidance in the form of a common set of examples of both acceptable and unacceptable demonstrations of technical infeasibility. ONC should also offer an established list of conditions that would qualify modules for this exemption. This list should identify the most common conditions for exemption, while leaving the door open for vendors to demonstrate this exemption through other means. For example, the list could include exceptions for modules that do not use or have the ability to access identifiable information in their operation and modules intended to operate in the application context of a host where they do not control the environment.

Recommendation 3: Limit the HHS-sanctioned testing and certification program to the minimum needed to support Meaningful Use, interoperability, and existing privacy and security capabilities of qualified health IT.

ISSUE: ONC is authorized under ARRA to establish a voluntary certification program for health IT, including but not limited to EHR technology. As ONC considers the future of certification, it should evaluate expansion carefully against the stated objectives. ONC also asks for comments specifically on whether it should pursue a certification program for electronic personal health records (PHRs) or for networks designed for electronic health information exchange (HIEs).

RECOMMENDATION:

- Limit the scope of the HHS-sanctioned testing and certification program to the minimum needed to support Meaningful Use, interoperability, and the necessary privacy and security capabilities.
- Do not extend the program to require the general testing or certification of PHRs or HIEs except to the extent necessary to support meaningful use, interoperability, and existing privacy and security capabilities. Specifically, HHS should allow PHRs or HIEs that wish to be qualified as EHR modules for purposes of helping providers and hospitals achieve Meaningful Use.

RATIONALE: Regardless of the technology in question, the approach to certification should be limited to the minimum needed to enable providers to meet the Meaningful Use objectives, interoperability and existing privacy and security requirements. The cost of expanding the certification program should be carefully weighed against the benefits. However, HHS should allow PHRs or HIEs that wish to be qualified as EHR modules for purposes of helping providers and hospitals achieve Meaningful Use. We consider PHRs and HIEs separately below.

Personal health records: HHS should allow certification of PHRs that wish to be qualified as EHR modules for purposes of helping providers and hospitals achieve Meaningful Use. However we do not recommend general certification beyond this capability. Meaningful Use subsidies do not directly support PHRs. It is not known whether government certification will or can affect the decision of consumers to use PHRs. It is a rapidly innovating area, still in its early stages of

determining the features and functions that consumers will want. Extending the HHS-sanctioned testing and certification program beyond Meaningful Use requirements could unintentionally limit innovation by setting requirements that ossify today's technology capabilities without the implementation experience to know whether they will meet consumers' needs.

Secondly, certification of PHRs alone cannot serve as a proxy for whether a service is in compliance with a complete set of privacy and security practices or for an enforceable regulatory framework. Building consumer trust in PHRs requires a consistent, reliable, and enforceable policy framework. Congress, through ARRA, laid the groundwork for developing appropriate privacy and security protections for PHRs. Specifically, ARRA tasked HHS to work with the FTC to develop privacy and security recommendations for PHRs not already covered by the Health Insurance Portability and Accountability Act (HIPAA), and a report to Congress is due in 2010. We hope that this report will lead promptly to the promulgation of privacy and security policies that apply more comprehensively and consistently to those who offer personal health information services in the marketplace. A certification effort that would test for the presence of technical capabilities for implementing some of those policies could be revisited once a clear framework is in place that includes additional considerations for oversight, accountability, and enforcement.

Health Information Exchanges: Prioritizing the general certification of networks for the electronic exchange of health information is of unclear value. **HHS should allow certification of HIEs that wish to be qualified as EHR modules for purposes of helping providers and hospitals achieve Meaningful Use interoperability requirements. However, we do not recommend general certification beyond this capability.**

The technical standards for interoperability have already been set through the adopted certification criteria for EHR technology. Market pressure will encourage networks to properly support these standards because they will have an incentive to comply with the information sharing aspects of Meaningful Use.

In addition, it is not feasible to certify the majority of the privacy and security requirements at the network level, assuming that networks are truly networks and not simply large repositories of personally identifiable information.

Through its Nationwide Health Information Network (NHIN) work and other grant-making, ONC should make clear what the basic network requirements are for health information sharing, including those technical elements that implement the privacy and security aspects of a comprehensive framework.

Some propose certification of networks to prohibit the sale of data, and to enforce access and authorization controls. However, we view this very important objective to fall more appropriately to the systems at the edges holding and controlling the consumer's information. As we discussed for EHRs, such privacy and security protections are enforced through behaviors, policies and limitations that can be managed more effectively through other mechanisms where the data is held and where the majority of the risks lie.

Recommendation 4: Clarify the type and scope of modifications that would require a product to be recertified.

ISSUE: The NPRM describes certification as a snapshot in time. When a specific Complete EHR or EHR module version is certified, it will be labeled "certified" forever.[20] However, without a precise definition it is not clear how much a product can change and adapt to growing needs over time without losing its certification status. In addition, the term "version" is not defined.

RECOMMENDATION: Offer guidance on the extent to which a specific Complete EHR or EHR module can change while still maintaining its HHS-sanctioned certification status. This guidance should allow for a broad range of technology solutions.

RATIONALE: The NRPM should offer further guidance on the extent to which certified technology can change while still maintaining its certification status. While it says that a specific *version* will be labeled as certified forever, the term "version" is not defined and therefore open to interpretation. This ambiguity could lead to inconsistent or inappropriate practices across the certification program. If defined too narrowly, products could be required to undergo certification for minor updates and fixes. This would dramatically increase the costs of updating technology and unintentionally create a disincentive for growth and improvement. On the other hand, if the term "version" is overly broad, providers may lack the assurance that products that have undergone significant changes since the initial certification still comply with certification requirements. In addition, the current ambiguity of the term "version" could unfairly disadvantage Software as a Service (SaaS) vendors since they do not deploy traditional versions in the market and instead launch new releases on a regular basis to all users. SaaS vendors would face prohibitive certification costs if they were required to certify each new release.

ONC could remedy these issues by offering a simple set of conditions for determining when certification should be reassessed, so long as those conditions acknowledge and allow for a broad range of technology solutions. As a starting place, ONC can use the definition offered by ISO Guide 65, which specifies that certification should be re-evaluated "in the event of changes significantly affecting the product's design or specification."[21]

As one approach, ONC could specify the following:

- Certification status will be maintained unless a product's design or specification is altered such that it no longer fulfills the HHS-sanctioned certification criteria it was tested and certified to meet.

- As clarification, certification status will be maintained when a product is upgraded to comply with the new version of an adopted minimum standard.

---

[20] Proposed Establishment of Certification Programs for Health Information Technology; Proposed Rule. 75 Federal Register 46 (March 10, 2010), page 11,346.

[21] ISO/IEC GUIDE 65:1996(E).

Markle Connecting for Health Collaborative

This paper represents a collective view that was deeply informed by the many and diverse collaborators of Markle Connecting for Health.

The following individuals support the collaborative statement reflected in this document.

Christine Bechtel
National Partnership for Women & Families

Hunt Blair*
Office of Vermont Health Access

William Braithwaite, MD, PhD
Anakam Inc.

Mark Chassin, MD, MPP, MPH
The Joint Commission

Rex Cowdry, MD*
Maryland Health Care Commission

Mike Cummins
VHA, Inc.

Brian DeVore
Intel Corporation

Paul Egerman
Businessman/Entrepreneur

Steven Findlay
Consumers Union

Mark Frisse, MD, MBA, MSc
Vanderbilt Center for Better Health

Daniel Garrett
PricewaterhouseCoopers, LLP

Mark Gorman
National Coalition for Cancer Survivorship

Adrian Gropper, MD
MedCommons

Margalit Gur-Arie
Gross Technologies, Inc.

John Haughton MD, MS
DocSite, LLC

Douglas Henley, MD, FAAFP
American Academy of Family Physicians

Joseph Heyman, MD
American Medical Association

Gerry Hinkley, JD
Pillsbury Winthrop Shaw Pittman, LLP

Kevin Hutchinson
Prematics, Inc.

William Jessee, MD
Medical Group Management Association

Michael Kappel
McKesson Technology Solutions

Allan Korn, MD
Blue Cross and Blue Shield Association

Vince Kuraitis
Better Health Technologies, LLC

Joseph Kvedar, MD
Center for Connected Health, Partners HealthCare System, Inc.

Jack Lewin, MD
American College of Cardiology

Robert Marotta
WebMD Health Corp.

David McCallie, Jr., MD
Cerner Corporation

Deven McGraw, JD, MPH
Center for Democracy and Technology

Howard Messing
Meditech

John Moore
Chilmark Research

Peter Neupert
Microsoft Corporation

Marcus Osborne
Wal-Mart Stores, Inc.

Herbert Pardes, MD
NewYork-Presbyterian Hospital and NewYork-Presbyterian Healthcare System

Amanda Heron Parsons, MD, MBA*
New York City Department of Health & Mental Hygiene

Carol Raphael, MPH
Visiting Nurse Service of New York

Stephanie Reel
Johns Hopkins Medicine, Johns Hopkins University

** Federal, state and city employees collaborate but make no endorsement*

Peter Schad, PhD
RTI International

Scott Schumacher
Initiate, an IBM Company

Raymond Scott
Axolotl

Alfred Spector
Google

Thomas Sullivan, MD
DrFirst

Peter Tippett, MD, PhD
Verizon

Robin Thomashauer
Council for Affordable Quality Healthcare

Paul Uhrig, JD
Surescripts

Robert Wah, MD
Computer Sciences Corporation

Jeb Weisman, PhD
Children's Health Fund

Markle Foundation:

Zoë Baird
President

Carol Diamond
Managing Director
Chair, Markle Connecting for Health