Cerner™

2800 Rockcreek Parkway
Kansas City, MO 64117
816.201.1024 Tel
816.474.1742 Fax

April 3, 2015

Karen DeSalvo, MD
Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

RE: *Comments on Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap Draft Version 1.0*

<Submitted Electronically>

Dear Dr. DeSalvo,

On behalf of Cerner, I am writing to provide comment on "Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap Draft Version 1.0." We commend you and your team for the well-organized and comprehensive approach toward advancing widespread, nationwide interoperability of health information, and are appreciative of what will certainly require super-human efforts to receive and incorporate feedback from various stakeholders across the U.S. health industry.

You will no doubt receive responses from many great thought leaders. Cerner's unique perspective from our decades of experience in automating and transforming health care enables us to be innovative and visionary, yet grounded in the realities of today's world. Improving the health of individual and communities is our core business, and nothing is more crucial to this process than interoperability. We strongly believe that clinical data should always flow unimpeded to wherever it is needed for direct clinical care and treatment of the patient. Bold actions by both government and industry are needed to achieve the best possible outcome with the patient at the center.

We support President Obama's "precision medicine" initiative as well as CMS' recently announced goal of moving rapidly toward value-based payment schemes for doctors. We are pleased to see these two nationwide goals – which we believe will shift the paradigm in health care over the next decade – are linked with the roadmap.

Cerner understands the importance of collaboration across the healthcare industry in this complex undertaking. While we recognize 100% alignment on every point may not be achievable, several of our associates participated in efforts to voice detailed stakeholder comments in response to the Roadmap, including Electronic Health Records Association (EHRA), HL7, HIMSS, and eHealthInitiative. Further, you and your team worked closely with our associates who provided feedback on various aspects of the Roadmap through their activities with the Health IT Policy and Standards Committees and respective workgroups. Our brief individual response today focuses on several topics either worthy of particular emphasis or distinction from our colleagues. Please find attached our respectfully submitted comments for your consideration.

Cerner compliments the federal government's efforts and willingness to approach this critical topic thoughtfully and comprehensively. Please do not hesitate to contact me if we can be of further assistance.

Sincerely,

Meg Marshall

Meg Marshall
Director, Government Health Policy
Cerner Corporation
meg.marshall@cerner.com
816.201.3052

Cerner's individual comments on the Roadmap are focused on four areas: achieving the appropriate balance between government and private market action; recommended steps within the current certification program; privacy and security; and governance.

I. Government v. Private Market Action - Achieving the Appropriate Balance

Successful exchange of health information is occurring now across the industry. While technology itself was once reasonably considered the greatest barrier to widespread interoperability, leaders within the health IT industry responded and effectively advanced standards development and implementation. Now, technology, while not without its challenges, is arguably the easiest issue to overcome. We agree with the declaration "most providers should be able to send, receive, find and use a common set of electronic clinical information by the end of 2017."

Cerner has long been committed to true information liquidity across geographic and technical boundaries. As you know, in 2013, we co-founded CommonWell Health Alliance to facilitate the exchange of clinical data across EHR systems and providers. Last year, we joined with several industry partners to launch the Argonaut Project to accelerate the development and adoption of HL7's Fast Healthcare Interoperability Resources. We are making significant investments in voluntary, private market-led activities with the goal to solve technical challenges of interoperability. These efforts should inform and complement, not conflict with, efforts by the federal government to achieve the same goals. ONC acknowledgement, support and appropriately deference to private initiatives will go a long way in assuring stakeholders that their significant investments in health exchange will be recognized and rewarded.

Congressional Activities: Education, Collaboration and Advocacy

- Cerner is pleased to see Congressional interest in investigating ways to ensure taxpayer dollars spent on the EHR Incentive Program support certified EHRs that truly are interoperable.
- We encourage ONC to become active educators with members of Congress to ensure that the federal government focuses not just on the technical capabilities of EHRs and the certification processes by which EHRs are tested, but also on provider and vendor business practices that discourage interoperability efforts by making it too difficult or too expensive for providers to connect and exchange patient data with others in their community. Specifically, we recommend that ONC:
    - Clearly indicate necessary steps Congress must take to advance interoperability, such as appropriate jurisdictional clarification or appropriations funding.
    - Communicate where market and regulatory failures have occurred, if any, relative to health IT incentives and adoption, which may justify Congressional action.
    - Work with Congress to recognize a common definition of interoperability that can be leveraged by the entire spectrum of stakeholders, representing an industry-wide approach and achieving a definition of interoperability that includes all categories of health IT, such as medical devices, and consumer devices and apps.
- We strongly urge ONC to advocate for the removal of the current prohibition on expenditures related to the study and development of a National Patient Identifier. Accurate patient identification is crucial to ensuring the right health data is available to the right people (providers, organizations *and* consumers) at the right place, and at the right time. The ideal short-term outcome would be for Congress to authorize the Secretary

of Health and Human Services to research effectiveness and feasibility of such an identifier and publish her findings in a report to Congress. At the March 10, 2015, Health IT Policy Committee Meeting, Jodi Daniel offered a briefing on the HIPAA National Patient Identifier prohibition and a written opinion as to how it should be applied within FACA discussions. We encourage Ms. Daniel to move forward with this activity.

- Cerner urges ONC to work with Congress and across federal agencies to pursue a strategy that supports the integration and exchange of *all* types of health information through a nationwide, privacy-focused legal framework that focuses on penalizing those who use data inappropriately or to discriminate rather than prohibiting the exchange of specific types of data across all venues of care. Inconsistencies in various state and federal privacy laws pertaining to sensitive health information such as that protected under 42 CFR Part 2, 38 CFR Part 1, emancipated minor-related data such as reproductive health, and other common sensitive data types and conditions, continue to be obstacles to widespread health information exchange. One possible mechanism could be for ONC to lead a cross-state effort focused on simplification and harmonization.
- Not all stakeholders critical to achieving nationwide EHR interoperability are eligible under the EHR Incentive Program, and not all health IT critical to achieving EHR interoperability is certified under the ONC's program for certified electronic health record technology (CEHRT). As such, ONC should work with Congress to identify appropriate mechanisms to close these gaps. Further, ONC, FDA and FTC should publish the final report to Congress regarding recommendations toward a risk-based health IT framework, as required under FDASIA.
- Cerner wholeheartedly agrees with designating the Inspector General of the Department of Human Services with authority to investigate claims in connection with the Medicare incentive programs, and specifically, investigation of claims of vendors in violation of an attestation; and health care providers with respect to the use of such records under a specified Medicare incentive program. We recognize that this may require Congressional action, however, and we suggest that ONC's report on data blocking to be informative as to the specific legislative language that defines the actions justifying penalties, and suggestions as to what the most effective penalties shall be. We also suggest that any resulting legislative text allows includes future programs as necessary to action delivery and payment systems reform efforts.
- Cerner strongly believes that the ongoing transition from the current fee-for-service payment model toward value- and outcomes-based payment models will improve care for all Americans. Interoperability is the key to the success of healthcare reform. Providers shifting from fee-for-service to value-based models will be successful only if they are able to leverage additional capabilities that increased connectivity at the community level enables to share real-time data and ultimately reduce costs, manage risk and improve quality. Further, the shift in payment incentives provides a business driver that encourages timely exchange of information and ultimately supports efforts toward nationwide interoperability. We were exceptionally pleased to see the recent announcements by Secretary Burwell toward delivery system reform, specifically to ensure 50% of Medicare payments are tied to quality or value through alternative payment models by the end of 2018 and 90% of all Medicare fee-for-service payments are tied to quality or value by the end of 2018. Cerner strongly urges ONC to work with Congress and other federal agencies to tie interoperability to its support for overall delivery system reform, specifically Secretary Burwell's goals for Medicare payment reform. In addition we believe that specific Medicare and Medicaid reimbursement programs should have strong and direct language that requires interoperability to participate in the programs.

Private and State Actors

We note that the phrase "call to action" is used 79 times in the 166-page document. Success of this roadmap relies heavily on ONC and the existing certification program as the hammer, which may not be a clear-cut, effective incentive. Commitment to action by private players will be relied upon heavily, however, it is unclear based on the roadmap how this commitment will be either incented or mandated. While this is the ONC Interoperability Roadmap, we look forward to agencies designated in the Federal Health IT Strategic Plan to provide details around their plans to operationalize and be accountable for activities assigned to them via this Plan.

- Cerner encourages ONC to incent private payers to implement policies that reward providers who strive to exchange and appropriately integrate health information from external data sources.
- We encourage ONC to facilitate discussions regarding state-level tort reform and other legislative activities focused on providing appropriate protections and safeguards that encourage data exchange between providers.

II. Recommended Steps Within the Current Certification Program

Cerner associates John Travis and Catherine Britton participate in ongoing Kaizen sessions for the ONC certification process. We are grateful for these opportunities and believe these meetings are a much more effective place for public comment; however, we offer a few summary key points specific to Table 9, item 12.

- We recognize the need to decouple EHR certification from the EHR Meaningful Use Program. We agree with JASON Task Force recommendations that provide for a narrowed approach for CEHRT that providers will implement for MU3 and will be providing comment to the recently released NPRMs.
- Certification requirements must always have a clear program purpose and linkage – a regulatory underpinning if you will - if there is to be federal sponsorship and oversight of it.
- Certification should focus on what is of high value for the public good and less so on the internal workings of the provider setting. Programs that require certification should not entail many prescriptive low level "functional measures" that are questionable as to their merit and their ability to be derived as a byproduct of clinical care. Instead, certification should focus on what is of merit to support core components: interoperability requirements needed for high value clinical information exchange, security and privacy, quality measure reporting in support of value based programs, patient safety, consumer engagement and public health reporting.
- Certification of interoperability related requirements need to provide for much more support to modularity of clinical information exchange suited to and supportive to the clinical need at hand, and not be solely based on prescriptive document-based exchange without a significant value basis, or that which over-presumes what is of common interest to all care venues. A significant complaint as to meaningful use has been of the useless nature of the current Transition of Care document and many providers continue to rely on other manners of exchanging what they believe really is of value. What is of value is not going to be uniform between acute care, long term care, home health, and so on.
- ONC should provide for a deeming recognition of certifications and accreditations that are widely recognized and of proven value to the industry where certification requirements overlap with those other recognized credentials. For example, electronic prescribing and SureScripts certification. Certifying eRX within the EHR Meaningful Use Program adds no value to what the industry already practically requires. Certifying any capabilities related to controlled substance prescribing also would be useless to incorporate into anything other than what the DEA already recognizes. Doing anything in the future that would supplant CAQH CORE recognition would create similar redundancy.
- The cycle time of the introduction of new criteria editions and their impacts on vendor and client timeframes for development and deployment need to adequately account for all of the following activities

beyond the obvious activities of gap assessment, design, software coding, testing and rollout for upgrade/update.

  - Vendors need the opportunity to evaluate clinical workflow impact of not only requirements but of making both functional and clinical quality measures by products of care that fit seamlessly not only within the one exemplar workflow that may be used for testing but also for all workflows that similarly support the same activity as alternative workflows.
  - Vendors need to evaluate for usability. We recognize that a steady criticism has been of certified systems being technically able to meet testing requirements but not being very usable. Part of that stems from a compression of time to get the requirement met which makes it difficult to do a full job of human factors review, and accounting for usability design - measurement requirements can be challenging to fold in without an adequate cycle of that kind of review.
  - Client adoption includes time needed for reasonable upgrade/update rollout and adoption timely to first year need of anything new – inclusive of
    - Training, testing, workflow redesign, policy/procedure development, queuing of resource demand on vendor capacity, potential new licensing/contracting needs, engaging with external entities (state agency onboarding or registry onboarding), identifying trading partners locally
    - Balancing with many other regulatory demands contemporary to the timeframes of new criteria adoption and use (e.g. ICD 10, value based initiatives, etc)
- Test method development needs far greater attention to assure
  - Quality and stability of testing tools
  - Validity and accuracy of test procedures and data sets
  - Transparency of development of the above
  - Transparency of interpretive guidance provided from ONC to the entities involved in testing and certification

Cerner recommends ONC takes steps to ensure transparency of critical interoperability data, and addresses data blocking practices.

- We wholeheartedly support ongoing public listing of EHR vendors and providers in compliance with interoperability certification requirements. We suggest ONC should require through CEHRT requirements vendor transparency regarding all one-time and recurring fees associated with the interoperability capabilities of the certified EHR product. This public reporting mandate must occur as soon as possible.
- We support and agree with efforts to identify and penalize EHR vendors not in compliance with interoperability certification criteria, with methods including de-certification, and support public reporting thereof.
- We agree with leveraging an attestation process by which vendors and providers state they are not knowingly and intentionally block data in an unfair, unreasonable or discriminatory manner. We suggest that this attestation begins as soon as possible.
- The 2014 Omnibus Appropriations bill requested ONC to provide to Congress a detailed report regarding the extent of information blocking, including an estimated number of vendors and eligible hospitals/eligible providers who block information, as well as a comprehensive strategy on how to address information blocking. This report was due several weeks ago. We encourage ONC to make the report publically available. We also suggest that ONC draw from the findings of this report to inform future regulations in this area, including that which prevents unfair, deceptive or discriminatory fee structures for interoperability technology.

We are encouraged to see the Stage 3 Meaningful Use Program NPRM propose the addition of discrete data APIs to the list of certifiable technologies. We strongly believe that the “public API” (as proposed by the JASON Task Force) will be a major step forward in interoperability.

III. Privacy and Security

Verifiable Identity and Authentication of all Participants (Table 6, p. 61)

Identity Proofing

- Policies and best practices do not necessarily suffice for identity proofing as far as organizational trust is concerned. Many organizations will be concerned about any risks they may assume if there is a lack of formal agreement or legal framework. For example, due to potential legal ramifications, many organizations are leery of adopting a transitive trust model (organization A trusts organization B and organization B trusts organization C, therefore organization A should trust organization C). Rather than trying to implement this model, the federal government should determine the minimum conditions necessary for trust to be established between organizations.
- Standards are needed so that a 'general-purpose' credential, such as one developed under National Strategy for Trusted Identities in Cyberspace (NSTIC) can be used to verify providers without requiring them to directly integrate with specific service providers' offerings. The result of such proofing should be some form of high-assurance digital credential that an individual can use to prove/authenticate their identity to an organization.

Authentication

- While mobile phones, email, and one-time-password generators are useful tokens or factors for authentication, there must also be processes, procedures or associated policies that account for situations in which such devices fail, are lost, or are otherwise temporarily incapable of being utilized. There also needs to be an exception process that allows a risk/compliance officer to make any necessary day-to-day decisions regarding authentication processes to ensure care is delivered in a timely manner.
- Multi-factor authentication for provider access to health information, while feasible, also has the potential to reduce the quality of care by adding time and complexity to the authentication process. Therefore, Cerner recommends that multi-factor authentication only be mandated in scenarios that justify additional risk mitigation, such as:
  - Providers needing remote access to PHI
  - Electronic ordering of prescriptions and procedures
  - Accessing mental health history
  - Accessing financial information that could be used for identity theft
- E-Prescribing of controlled substances: It is important to note that the Drug Enforcement Agency (DEA)'s regulations pre-date the era of smart-phones, meaning the current wording prevents the use of a smartphone in a multi-factor authentication solution if the e-Prescribing application is running on the same phone (or "computer"). Cerner believes the e- multi-factor authentication requirements for e-Prescribing need to be modernized to recognize that there are secure ways for a phone to serve as a computing device. This supports the roadmap's stated goal to "leverage *existing mobile technologies and smart phones* to provide efficient, effective paths for patient or provider identity authentication."
- Another important consideration regarding multi-factor authentication from a patient perspective is that it could make it too difficult for patients to reset their patient portal account to ensure continued access to

their provider's services. While re-authentication is necessary when an account is reset, the process should not be overly cumbersome from a usability standpoint.

- Accessing dependents' health information (i.e. children) needs to be addressed in terms of authentication processes as well.
- While standardization for how organizations issue or accept multi-factor credentials are needed, policies should not restrict an organization from developing innovative authentication methods that sufficiently address risks while also enhancing provider experience. An example of such innovation would be using RFID badges that allow providers to 'roam' across workstations once authenticated. These badges also can provide a second-factor authentication that doesn't penalize the provider's time to login.
- The roadmap's statement "SDOs will work with health IT developers to conduct Pilots using RESTful approaches for authentication," is a laudable goal, because there is not yet a widely-accepted standard definition for "RESTful authentication." We urge ONC to specify a specific protocol to champion, such as Open ID Connect (OIDC) and a specific objective to achieve (i.e. pilot interoperable authentication using an open standard that can function in a web browser) and then encourage market-based experiments, leading to refinements to the standard, based on real-world use.
- OAuth2 has become the 'gold standard' for proxied authorization, now in use by most big Internet companies, so Cerner encourages its adoption in the health care industry as well. The SMART Platform team has proposed an OAuth2 profile for third-party authorization of SMART apps, which is the same profile that the Argonaut Project is validating. We strongly encourage the ONC to specifically call out the need to adopt OAuth2 for appropriate use-cases.

Consistent Representation of Permission to Collect, Share and Use Identifiable Information (Table 7, p. 68-69)

- We concur with ONC that fear of violating the HIPAA Privacy Rule is inappropriately used as a reason by some organizations and providers to withhold certain health information about a patient. Rather than using HIPAA as a scapegoat, however, we support ONC's proposed action to clarify policy around the protections provided for organizations that share information, or 'interoperate' for TPO purposes while adhering to HIPAA. Today some organizations err on the side of withholding vs. disclosing information due to misinterpretation of the HIPAA statute and/or risk aversion, and we agree this trend must be reversed in order to facilitate effective interoperability. This could be done by shifting from the current 'thou may' approach to data liquidity enforced under HIPAA to a more stern 'thou shall' approach of the law.
- Cerner recommends that data-sharing standards be consistent with those required by HIPAA vs. more strict laws at the state level. Furthermore, we feel it is more effective to enforce stricter penalties for misuse of patient data vs. creating excessive and potentially burdensome policy around when and how to disclose certain data elements to certain providers.

Consent

- Technology that can appropriately facilitate patient consent depending on the situation is needed, but flexibility in developing this technology also is key as complex requirements could stifle innovation.
- We agree with the HITPC's Privacy and Security Workgroup that the Roadmap's definition of "basic consent" is confusing and should be clarified. For example, the Roadmap suggests that institutions can self-elect to offer "basic consent" to their patients. What is left unclear is what should happen if a patient exercises "basic consent" and decides to prohibit HIPAA-granted TPO exemptions. Does the patient's preference override the HIPAA exemptions? A definition of 'basic consent' needs to be addressed and broadly applied for exchange purposes, vs. providers requiring specific consent permission for certain documents, as this is often redundant. ONC should work to harmonize how consent is handled within state and local exchanges (such as in state immunization registries, for example), as this varies greatly and becomes burdensome to both patients and providers when consent must be granted multiple times for multiple specific purposes.

Defining “sensitive” information

- While creating policies around the proper management of sensitive and re-disclosure-restricted information is difficult, Cerner strongly encourages ONC to start any analysis from the perspective of patient safety. For example, many psychotropic medications have profound safety concerns if administered in conjunction with other drugs. We urge that requirements placed on vendors of HIT systems avoid restrictions on the flow and visibility of information that could inadvertently lead to these kinds of harms.
- Defining what is considered ‘sensitive’ for purposes of exchanging (disclosing and re-disclosing) health information is certainly a challenge. Per our suggestions to SAMHSA regarding revisions to 42 CFR Part Regulations, Cerner believes that if regulations are changed such that services or treatment rendered by any *provider* participating in federal health programs are covered by 42 CFR Part 2 (as opposed to anything rendered by a treatment *facility*), a more thorough definition of what those services are is needed so they are clearly understood by providers involved in health information exchange. This would allow both parties to know to what data privacy protections and consent permissions apply to the information being exchanged so the provider on the receiving end knows what is subject to limitations on re-disclosure beyond their own treatment-related use of the information. This includes identifying the conditions, medications, procedures, interventions and related clinical information for behavioral health treatment-related services so that any information pertaining to those services can be accurately identified as having ‘restricted re-disclosure’ in exchange.
- In sum, Cerner supports ONC’s proposal for the federal government, state governments and all entities exchanging health information to harmonize policies and regulations for obtaining consent at a more granular level when absolutely necessary (i.e. re-disclosure-restricted information is involved), but cautions that this change could also make the definition of ‘sensitive’ information more granular in nature too, which will cause confusion among providers if examples are not provided. If the regulations change so that sensitive information covered under 42 CFR Part 2 is defined based on the *type of treatment services provided* vs. *type of treatment facility*, SAMHSA will need to provide clear guidance as to exactly which treatment records are covered under the regulations and which are not. Lack of clarity in this regard would cause confusion and frustration among providers who treat comorbidities involving substance abuse but are not exclusively substance abuse/behavioral health providers. Providers who both send and receive substance abuse information for their patients need to understand the applicability of any revisions made to 42 CFR Part 2 to them specifically.

Consistent Representation of Authorization to Access Health Information (Table 8, p. 73)

New Models of Care Delivery and Payment

- Cerner agrees with ONC that clarification is needed regarding how the HIPAA Privacy and Security rules apply to new models of care delivery and payment and population health management. For example, in order to support the value-based purchasing requirements for Accountable Care Organizations, data must be able to be disclosed. Important considerations regarding authorization to access and information within ACO include:
    - Are the participating organizations bound by an Organized Health Care Arrangement (OHCA)?
    - Do the participating organizations have common policies, procedures, notices and consent in regard to:

        - Their mutual operation
        - Exchange of information among them for purposes of TPO under HIPAA
        - Their notices of privacy practices and consent forms given to patients
        - How their notices as a collaborative entity relate to their notices as individual organizations
        - How patient rights are handled (regarding accounting of disclosures, for example) as a collaborative entity vs. an individual organization
- Cerner also feels it is important to have a clear classification of the activities involved in public reporting of data required for value-based purchasing, especially when individually identifiable ePHI is involved.
    - For example, the question of whether the disclosure of quality measures data used in a value-based purchasing program is considered disclosure for "payment" purposes under HIPAA, but would not fall under the Accounting of Disclosures requirement unless it is published via a CMS public access site for public reporting, needs to be answered.

IV. Governance

Cerner agrees to a great extent with the Governance Principles set forth in the Roadmap; primarily that there should be no policy, business, operational or technical barriers that prevent health information to flow where necessary to support patient care and treatment.

Cerner strongly urges ONC to recognize the JASON Task Force recommendation that a single national exchange network is neither feasible nor desirable. Instead, we recognize the need for multiple data sharing networks (DSNs) to exist, and that as need demands, network bridging should be used to connect any potentially isolated islands of health care data. To this extent, we agree there may be potential value in the creation of a new public-private governance coalition – "The Governance Entity" - but only if some very specific constraints are met. The Governance Entity must:

- Be completely independent from any incumbent data sharing network, with membership open to all DSNs.
- Be predicated on the JASON Task Force recommendation that multiple data sharing networks, some of which might be in competition with each other, will be necessary to meet the rapidly evolving needs of nationwide exchange.
- Be charged (and constrained) to specify only the minimum necessary governance to ensure that the "Principles" are likely to be met.
- Be committed to leveraging market forces so as to ensure that exchange is based on realistic and sustainable business models.
- Aggressively seek to avoid impeding innovation and experimentation in the marketplace.
- Focus on the floor, but not the ceiling, when defining expectations for national exchange, recognizing that some DSNs may offer advanced functions that should not be constrained, even if those functions are not available in every DSN.

We believe the proper focus of the Governance Entity should be on defining the minimum conditions necessary for DSNs and appropriate bridging services to exist. Suggested areas that would be **in scope** for the Governance Entity:

- National clarity around minimum necessary rules for provider identity and provider authentication. All networks would meet this floor. (Level of assurance)
- National clarity around minimum necessary rules for patient identity and authentication (for future states when patients can access the network to get their own data.) (Proofing minimums, etc.)
- National clarity around minimum policies for "default choice" and "basic choice" for patient privacy preferences

- National clarity around technical means to capture and share the patient's expressed wishes for the "choice" options defined above (how to prove that you have proper consent to request data)
- National clarity of the **Core Use Cases** that compromise the minimum extent of Nationwide Health Information Exchange
- Agreement on Transparency Metrics that all DSN should report.
- Agreement on approach to cross-DSN network fees
- Standards necessary to facilitate DSN Bridging, such as:
    - Bridging API standards (i.e., a common way for networks to talk to each other.)
    - Bridging Authentication/authorization
    - Minimum standards for patient identity matching (when crossing DSNs)
    - Content minimums that bridges must support
    - Trust fabric for cross-DSN trust (technical and policy)
    - Bridging directory standards, if necessary (for example, locating the address of an entity not inside my DSN)

But just as important, we think there should be areas that are **out of scope** for the Governance Entity. These include defining for the DSN:

- Internal functional scope (some DSNs will be more capable than others, etc.)
- Internal business and sustainability models
- Architecture and network topology
- Internal technical standards
- Internal content standards
- Internal fee structure