CHIME National Patient ID Challenge

Instructions are at https://herox.com/PatientIDChallenge/guidelines

- Easily and quickly identify patients
- Achieve 100% accuracy in patient identification
- Protect patient privacy
- Protect patient identity
- Achieve adoption by the vast majority of patients, providers, insurers, and other stakeholders
- Scale to handle all patients in the U.S.

Submission Form

Title: Health Email ID

Short Description: Health Email ID identifies patients using the familiar email address format and brings the full power of the Web to our healthcare services.

Name: Adrian Gropper, MD

Affiliation: CTO of Patient Privacy Rights Foundation

Location: Watertown, MA, USA

Elevator Pitch: Explain what Your Solution does in a few words. (100 characters)

> A standard email address can be a patient ID. Forwarding makes it accessible to all ages and secure.

Metaphor: Fill in the blanks of the following sentence or make up your own. ___*Your Solution Name*___ is the _____ for _____.

Health Email ID makes health services come to you.

Executive Summary: Summarize each section of your proposal (4,000 characters)

Enrollment is as easy as getting your own domain name or buying one for a child. The process starts with a visit to a standard registrar (there are hundreds already), picking a name, checking for uniqueness, picking an email notification address and password, entering name, address, and payment information. This one-time process takes 5 minutes and costs about $10/year.

To support email patient ID, healthcare-enabled registrars would add two new features: a *hidden email and/or SMS forwarding address* to be pointed to a patient's current email service or the email/SMS service of their healthcare proxy. The second, would be a recovery feature in case the account password is forgotten or compromised. A healthcare registry would accept 5 email patient IDs of friends or family any three of which would be sufficient to respond as part of a recovery process. Neither email forwarding or 3 of 5 recovery add appreciably to a registrar's costs.

Identification is as simple as providing one's email address in-person or online. This could be enhanced with a sticker or a QR code on the home screen of one's cell phone. Once the email patient ID is entered at the point-of-care, two familiar processes would take place in parallel. One would send a coded notification via the hidden forwarding address associated with the patient ID to verify that the patient is actually in control of the identifier they present. The other process would display the patient's online health ID attributes, if they are public or accessible to the specific service provider. This health record "top page" might be as simple as a photo, insurance, and allergy information. In some cases, a link to an EHR could be provided. Both the email / SMS and attribute lookup would take only seconds could be put off in case of emergency.

Security is supported at many levels. The patient is always notified via their forwarding email / SMS address. Compromised domain registrations are rare and easily remedied by a recovery challenge to the five registered trustee emails associated with each registration. Replacement of an ID would be equivalent to re-enrollment at a particular service provider. The use of an email patientID is voluntary and it would be their choice to keep a separate email patient ID for health purposes or not. Security is supported at many levels by signed assertions accessible via the patient's "top page". An insurance

coverage claim, for example, could be digitally signed by the insurance carrier and independently verified by any provider.

Privacy and Anonymity are supported by the use of multiple email addresses. Patients may keep more than one email patient ID so their mental health encounters could be easily separated from other healthcare. True anonymity would require a trusted registrar to issue separate coded addresses on-demand as is typical for dating services. The Health Email ID solution goes beyond national and state standards by offering the User Managed Access (UMA) standard as an option. This enables patients to post the address of an UMA-standard authorization server hosting their detailed privacy settings.

Scalability is effectively guaranteed by building on top of the Internet's domain infrastructure. Email patient IDs and cell phones are accessible regardless of nationality and their commodity nature assures that they are affordable.

Adoptability for email patient ID is second to none. Service providers already use email one way or another and in many cases, email is the ID associated with a patient portal. WebFinger (RFC7033) is the standard for converting email to a web page with patient attributes and other features. Enrollment systems will need to be modified to use an email address as the primary key and provide access to a standard web page for verification. The use of Internet standards throughout ensures it will be easily accessible on all software platforms and to services not yet invented.

Why should your Solution be chosen for an award? (750 characters)

The Health Email ID patient ID solution is the most patient-centered and endorsed by two of the world's leading patient advocacy organizations: Patient Privacy Rights and the Society for Participatory Medicine.

An email ID is most likely to be adopted, to scale, and to support global health innovations because it is natively Internet-standard. There are no proprietary or license barriers and no US-specific assumptions.

Patient ID must work beyond regulated health care providers. The Precision Medicine Initiative, patient communities, wearable and home monitors, genomic and quantified

self labs, and decision support at the point-of-care are the new reality. Health Email ID as patient ID anchors the patient's real-world care team.

The 20-page proposal starts below as page 5:

Health Email ID Proposal for the CHIME Patient ID Challenge

April, 2016

1. Contents

2. Enrollment

Enrollment is as easy as getting your own domain name or buying one for a child. The process starts with a visit to a standard registrar (there are hundreds already), picking a name, checking for uniqueness, picking an email notification address and password,

entering name, address, and payment information. This one-time process takes 5 minutes and costs about $10/year.

To support email patient ID, healthcare-enabled registrars would add two new features: a *hidden email and/or SMS forwarding address* to be pointed to a patient's current email service or the email/SMS service of their healthcare proxy. The second, would be a recovery feature in case the account password is forgotten or compromised. A healthcare registry would accept 5 email patient IDs of friends or family any three of which would be sufficient to respond as part of a recovery process. Neither email forwarding or 3 of 5 recovery add appreciably to a registrar's costs.

3. Identification

Identification is as simple as providing one's email address in-person or online. This could be enhanced with a sticker or a QR code on the home screen of one's cell phone. Once the email patient ID is entered at the point-of-care, two familiar processes would take place in parallel. One would send a coded notification via the hidden forwarding address associated with the patient ID to verify that the patient is actually in control of the identifier they present. The other process would display the patient's online health ID attributes, if they are public or accessible to the specific service provider. This health record "top page" might be as simple as a photo, insurance, and allergy information. In some cases, a link to an EHR could be provided. Both the email / SMS and attribute lookup would take only seconds could be put off in case of emergency.

4. Security

Security is supported at many levels. The patient is always notified via their forwarding email / SMS address. Compromised domain registrations are rare and easily remedied by a recovery challenge to the five registered trustee emails associated with each registration. Replacement of an ID would be equivalent to re-enrollment at a particular service provider. The use of an email patientID is voluntary and it would be their choice to keep a separate email patient ID for health purposes or not. Security is supported at many levels by signed assertions accessible via the patient's "top page". An insurance coverage claim, for example, could be digitally signed by the insurance carrier and independently verified by any provider.

5. Privacy and Anonymity

Privacy and Anonymity are supported by the use of multiple email addresses. Patients may keep more than one email patient ID so their mental health encounters could be easily separated from other healthcare. True anonymity would require a trusted registrar to issue separate coded addresses on-demand as is typical for dating services. The Health Email ID solution goes beyond national and state standards by offering the User Managed Access (UMA) standard as an option. This enables patients to post the address of an UMA-standard authorization server hosting their detailed privacy settings.

6. Scalability

Scalability is effectively guaranteed by building on top of the Internet's domain infrastructure. Email patient IDs and cell phones are accessible regardless of nationality and their commodity nature assures that they are affordable.

7. Adoptability

Adoptability is for email patient ID is second to none. Service providers already use email one way or another and in many cases, email is the ID associated with a patient portal. WebFinger (RFC7033) is the standard for converting email to a web page with patient attributes and other features. Enrollment systems will need to be modified to use an email address as the primary key and provide access to a standard web page for verification. The use of Internet standards throughout ensures it will be easily accessible on all software platforms and to services not yet invented.

8. Implementation

Implementation will proceed by first developing a reference implementation of the healthcare-enhance service in collaboration with a current domain registrar. The reference implementation would be documented and offered to all other registrars for a reasonable fee to defray the startup cost. This initial phase should take about 6 months since registrars already have processes in place for customer registration and service

and adding email and SMS notification and forwarding is mostly back-end work. The account recovery features are not technically challenging and are not cost-sensitive. Billing and spam control features could be added in later phases as uptake proceeds.

The second phase of implementation, initial launch, would be in partnership with a health information exchange. They have the management structure and relationships to make this practical and they are under pressure to solve consent and patient engagement problems that are linked to identity management. It could be said that the capabilities of typical HIEs are complementary to typical domain registrars. Launch planning can proceed in parallel with the Phase 1 reference implementation and clinical use within one year from project inception is achievable.

A full US implementation is equivalent to giving every person a personal domain account. At current pricing, without family and volume discounts, this would be some $3 B. This represents less than 0.1% of the projected $4.4 T annual healthcare costs. The program would be designed in such a way as to distribute these costs a widely as possible, primarily via health plans, with alternatives for self-pay and public sector supported registrations.

9. FAQ and other valuable features

What is the essence of the Health Email ID proposal?

The patient identifier is globally unique on the Internet, as in an email address, issued as a personal domain name by any Internet domain registrar willing to offer a limited set of enhancements including forwarding notifications, account recovery features, and spam control.

What is the primary business model?

It is expected that thousands of domain registrars around the world would be able to add the forwarding and account recovery features for nominal cost while being able to generate increased revenue and compete on the basis of spam control charges and one-time charges for account recovery activities. To avoid a digital divide, registrar services could be offered by libraries, local, and state government in support of privacy-preserving public health efforts.

Is there a risk of an email address being re-assigned to a different person?

No. Personal domains are controlled by the individual person. The cost of managing a personal domain is about 0.1% of the average cost of healthcare in the US. Whether privately, publicly, linked to 911, or community-funded, this cost of about $10 / year is likely the most inexpensive way to manage a unique patient identity system.

Can someone use a regular email as a healthcare patient ID?

Yes, but a “black box warning” would be displayed if a regular email address is registered as a patient ID. The patient identity verification feature will work with any email address as it does with other websites already but regular emails are more likely to change and to have spam problems. The dedicated healthcare email address benefits from the forwarding feature and can control spam much more effectively.

Are new technical standards or laws required?

No. All of the elements of the Health Email ID global unique patient identifier are already standard and operating at Internet scale. Email is already the dominant globally unique person identifier and well understood. Email or other personal Internet domains are clearly “personal identifying information” under current regulations. New regulations on the use and sharing of globally unique person identifiers will help protect privacy and limit the impact of spam but these are not strictly required for success.

How does the personal domain as identifier work with children and elders?

The email address associated with an identifier is not used directly. It is always forwarded to another, hidden, email address or mobile phone capable of standard text messaging. This enables a parent or other healthcare proxy to be the responsible party

and to transfer control to the patient subject at the age of maturity or when a different healthcare proxy takes over.

How will spam be controlled?

A unique patient identifier with an integral notification mechanism could be abused for non-health related and marketing purposes. Registrars will compete on the basis of spam reduction features. Traditional spam filtering approaches based on sender reputation could be used by registrars. These could be supplemented by small charges for the forwarding of notifications as part of patient registration and admission processes. Given the high value of health-related services, such spam control charges related to identity management will be easily tolerated and will encourage a more patient-centered and diverse health information ecosystem. These charges might also distribute the cost of the patient ID system to the actual service providers.

What are the 4 typical use case examples?

Use Case 1: arrival at primary care provider for routine care with photo ID.

The photo ID can include a personal domain identifier, typically an email address.

Use Case 2: arrival at primary care provider for routine care without any identification.

The patient states their email address from memory. It is entered into a computer that results in sending a message to the registered notification addresses

(including emails and SMS text messages) accessible for verification from the patient's mobile device.

Use Case 3: presenting at emergency room unconscious with photo ID and family member available.

The photo ID can include a personal domain identifier, typically an email address. As part of the registration process, the family member's unique identifying information can be collected as the Grantor for treatment authorization.

Use Case 4: presenting at ER with family member but no photo ID.

The family member can provide the patient's personal domain identifier. To enable identity verification and access to payment and critical medical information, the patient may have set up a personal web page with their photograph, and links to other personal resources such as a standard Health Email ID Authorization Server. Note that the existence and content of such a public verification and / or policy management service is entirely voluntary for every individual and can be separate from the personal domain registrar that is at the core of the globally unique identity for the proposed solution.

What are the principal standards for the Health Email ID solution?

Required

- All of the Domain Name System (DNS) standards

- RFC 5321 and RFC 5322 are the basic e-mail standards
- RFC 7033 WebFInger for lookup of attributes of a personal domain beyond DNS

Optional

- RFC 6749 The OAuth2 authorization framework
- OpenID Connect for patient and user attribute management and single-sign-on
- User-Managed Access (UMA) Profile of OAuth 2.0 for access authorization
- RFC 5724 SMS text message service for verification and notification

Note that all of these standards are international, open, and free - leading to increased patient safety, lower costs, and easier medical research.

Are photographs and facial recognition used in the solution?

The use of photographs and other biometrics is voluntary and optional but recommended. A Photograph can be used on an ID card with the email address identifier but the ID card is not strictly required as long as the patient or a family member remembers their medical email address or carries it with them without a photograph. A photograph can also be posted voluntarily on a web-page associated with the email address via the WebFinger standard. This is recommended as a way to avoid errors in cases where the correct email address cannot be verified directly via a mobile device. Facial recognition at the point of care can be used to speed registration in certain situations but the photograph of the patient and their medical email identifiers are to be secured as PHI and not shared without authorization.

Can the email universal patient identifier be used beyond healthcare?

Yes, but it should be discouraged in practice. The personal email identifier is voluntary and standards-based so there is nothing to prevent use beyond healthcare. It will be up to the patient or their custodian to decide if they want to use it payment or fitness or or other relationships but, in order to reduce the risk of spam, such use should be discouraged.

How will we deal with duplicate personal identifiers?

In some cases, a person may be issued a duplicate personal email address. This can happen inadvertently if the person forgets they already have a medical unique identifier or does not remember it in a situation where there is no ID card and an identifier is absolutely required. (These inadvertent duplicate IDs are very different from intentional multiple IDs designed to protect mental health records and similarly sensitive health information.) A duplicate unique medical identifier can be eliminated by the patient at any time by simply replacing it with the service provider. In the rare cases where that replacement is difficult, the forwarding address for the duplicate identifier can be set by the person to be the same as their principal medical identifier and the forwarding process will effectively merge the multiple identifiers.

Does the voluntary approach to unique person identifiers control fraud?

Yes. Identifiers control fraud according to the processes under which they are used. Coerced credentials such as a national identity card that is typically trusted without checking on the network invites fraud through forgery. A personal Internet domain identifier is much more difficult to forge because it is checked against the registrar that forwards the verification notification. This network-based verification can easily be integrated with eligibility checking with a health plan. In cases where a verified identity is required, such as for controlled substance prescription, the process can include checking for a coerced credential such as a driver's license or passport.

Wouldn't a government mandated identifier still have some advantages?

Many countries use government-mandated patient identifiers. Typically, these are linked to payment but they don't have to be. It's not clear what advantages a government-issued identifier has over the proposed voluntary and standards-based Health Email ID solution. These government-mandated systems evolved prior to the widespread adoption of Internet standards and ubiquitous networking. Today, if the US or another country wanted to create laws governing the issuance and use of a unique patient identifier, they certainly can do it but it would still make sense to build on well-understood Internet standards and practices.

Would the personal domain identifier be on a patient's wrist-band?

Yes. In addition to being easy to remember (almost as easy as one's birthday in use today), the Health Email ID personal domain identifier is a valid Internet address and can fit as a standard computer-readable Q-R Code right on the wrist-band. This means that networked technology for imaging, laboratory specimens, or infusion pumps could automatically display a patient's photo as part of the clinical procedure, thereby speeding workflow and enhancing patient safety.

Does the Health Email ID identifier support unified electronic health records?

Yes. This Internet-native and standards-based approach encourages a unified health record for every patient that wants one. Modern standards such as HL7-FHIR and OAuth2 make it possible for every patient to be their own health information exchange (HIE) and direct their caregivers to the health record custodian of their choice. Health Email ID is a stepping stone toward an HIE of one for each of us.

Does the Health Email ID identifier support traditional health information exchange?

Yes. Any globally unique identifier, including a personal email domain, supports health information exchange (HIE). An identifier that supports notification such as we propose also helps the HIE manage privacy, security, and control errors. The HIE, for example,

can use the identifier directly to enable a patient portal - a feature that is currently quite rare in state, regional, and vendor-driven HIEs.

Can mobile phones speed adoption and use of the Health Email ID identifier?

Yes. A mobile phone can automate patient registration by connecting to nearby terminals in the same way that modern “pay-by-phone” systems do. In addition, a phone can display a standard Q-R code that can be read by a clinician’s technology. A phone can also read a Q-R code displayed on a provider’s screen and automatically perform an identity verification and single-sign-on process. All of the standards for doing this are open, free, international, and in widespread use.

Does the Health Email ID solution promote patient engagement?

Yes. The Internet standards underlying Health Email ID are also used for single-sign-on and for managing sharing of information among both regulated (HIPAA-covered) and unregulated personal health records and health services providers. Standards such as User-Managed Access (UMA) even make it possible for patients to choose a single patient portal to manage information across the many separate portals we have today.

Has anyone endorsed this personal domain email identifier proposal?

This proposal has been endorsed by two of the country's leading patient advocacy organizations: the Patient Privacy Rights Foundation and the Society for Participatory Medicine. It is notable that two international groups with diverse perspectives can reach agreement on our approach. Most of the questions in this FAQ were raised as concerns in the SPM list and helped make this a stronger proposal.

Is this proposal consistent with the NSTIC Principles?

Yes. The NSTIC (National Strategy for Trusted Identities in Cyberspace) has four Guiding Principles of their strategy:

" - Identity solutions will be privacy-enhancing and voluntary

- Identity solutions will be secure and resilient

- Identity solutions will be interoperable

- Identity solutions will be cost-effective and easy to use"

The personal email domain is entirely compatible with the NSTIC principles.

Shouldn't the patient identifier be confidential?

There are no practical examples of confidential identifiers. Credit card numbers are not confidential and neither are social security numbers. Pretending that identifiers are confidential leads to fraud as these identifiers are misused. Fraud can best be

prevented by checking the identifier against networked information. Spam can be reduced by avoiding the publication or non-health-related use of the unique patient identifier but that's just common sense rather than confidentiality.

Can the Health Email ID personal domain identifier facilitate patient registration?

Yes. A personal domain linked to a personal healthcare email address can vastly reduce the hassle and errors associated with the typical multi-page patient registration forms. The personal domain can link to a personal health record of preferred health care institutional portal with the current information. Securing access to that PHR or portal is facilitated by standards such as OpenID Connect that share WebFinger and other Internet practices with the proposed Health Email ID solution.

Does Health Email ID support "fresh" second opinions?

Yes. The proposed system is voluntary and can support multiple identities for the same person. Anyone wanting to limit the influence of prior records on a consultation can simply create one or more temporary health email addresses expressly for that purpose.

How does a personal health domain work with User Managed Access?

UMA is a new standard for secure sharing of Internet-connected health records. UMA can secure a wide range of connections including HIPAA and non-HIPAA, sensitive

42CFR Part 2 mental health records, access from mobile devices, and access from open-source or community-managed services. UMA does not depend on a unique patient identifier for its operation but it shares many of the Internet standards that underlie Health Email ID as unique patient identifier. The mechanism that links a personal health domain to a Web page of voluntarily disclosed identity attributes can also be used to voluntarily associate an UMA Authorization Server.

Is Health Email ID a patient identifier or a health records sharing solution?

Both. Health Email ID is a security and privacy solution for Internet-connected health records. It is especially powerful when mated with modern health information coding standards such as FHIR. Health Email ID is a voluntary identity solution when the individual owns and controls the associated domain as recommended in this Proposal. As an identifier, the personal domain approach does not specify or restrict the method of authentication of its owner. The choice of the registrar authentication process is driven by the choice of registrar. To support the broad privacy and security requirements of healthcare, wellness, and medical research, the registrar's authentication process is completely separate from the authentication process of any particular health service provider. Authentication with Health Email ID can be strong, pseudonymous, or weak as appropriate for the specific health service provider that one registers with.

Health Email ID becomes a health records sharing solution if and when a health service provider is willing to accept a records sharing authorization that is digitally signed by the patient-subject of the requested records or their legal proxy. Typically, the method of access for Internet-connected patient records will be based on the FHIR standard. The method of associating a FHIR resource sharing request with a digitally signed patient authorization is still under active development. Health Email ID will adopt best practices for a patient-centered health records architecture based on Internet standards.