Secure Patient Identification

Feasibility of a Security Role for Subscriber ID Cards

This Research Paper assesses the feasibility of adding a security role to subscriber and patient identification for use in Real-Time Patient Arrival Registration. The research addresses the question:

*Could a secure subscriber identity token, such as a smart card, reduce medical identity theft, improve privacy, combat fraud by both claim submitters and patients, and enable deterministic patient matching in provider systems?*

November 3, 2014
~ Version 1.0 ~
Disclaimer

This document is Copyright © 2014 by The Workgroup for Electronic Data interchange (WEDI). It may be freely redistributed in its entirety provided that the copyright notices are not removed. It may not be sold for profit or used in commercial documents without the written permission of the copyright holder. This document is provided “as is” without any express or implied warranty.

While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by the Workgroup for Electronic Data Interchange. The listing of an organization does not imply any sort of endorsement and the Workgroup for Electronic Data Interchange takes no responsibility for the products, tools, and Internet sites listed.

The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by the Workgroup for Electronic Data Interchange (WEDI), or any of the individual workgroups or subworkgroups of the WEDI Strategic National Implementation Process (SNIP).

*Document is for Education and Awareness Use Only*

**Not a Recommendation**

This research paper does not make recommendations. It is intended only to answer whether it might be feasible to add modern security technology to Subscriber Identification to achieve certain goals. Assessment of feasibility requires analysis of technology use, practicality, acceptability, and a reasonable accounting of the economics. But drawing conclusions on these subjects does not constitute advocacy for implementation. That decision is policy and includes many other considerations such as alternatives, priorities, law, choices, exception rules, and other policy issues. This research makes no attempt to recommend policy.

**Workgroup for Electronic Data Interchange (WEDI)**

WEDI is a non-profit partnership between patients, providers, health plans, government, clearinghouses, data exchanges, and vendors. WEDI’s domain is where these partners interconnect, where each cannot so easily implement or innovate alone. Secure identification is such a domain.

Inter-disciplinary partners working together can achieve important security goals with new and existing standards. Standards themselves are consensus among partners. The opportunity researched in this paper is whether standard use of newer technology is feasible for improved accuracy and security of patient identification, and to describe the effects to accrue as a result.
CONTENTS

Definitions and Technology Tutorial

PART ONE: Non-Technical

Purpose and Scope
Description of PAR Process
Carefully Balanced Set of Benefits
Development of Identification Standards
The Questions Investigated by the Paper

Provider Options
Positive Patient Identification
Frequently Asked Questions
How Does it Work? (Non-technical)
Summary of Questions

PART TWO: Technical & Detail

1.0 Feasible Design for Using Secure Subscriber Identity tokens to Reduce Fraud
   1.1 Other Operating Environments
   1.2 What Proofs have been documented by the Above Process?
   1.3 How Long must Subscriber identity token be Inserted?
   1.4 The Design Meets Practical Requirements for Healthcare Providers.
   1.5 Start Simple: An Application of Gall’s Law.

2.0 Digital Signatures and Full Data Set
   2.1 The Three Digital Signatures used in Patient Registration
   2.2 Data Elements Included in the Three Digital Signatures

3.0 Components Used in Patient Registration Process
   3.1 PAR workstation
   3.2 Cost of an PAR workstation and Time to Install
   3.3 Central Public Key Database

4.0 Only the Health Plan and its Subscriber Identity tokens are Secure

5.0 Subscriber and Patient Registration
   5.1 Goals for Subscriber and Patient Identification
   5.2 Use of a PIN
   5.3 Use of a Biometric
   5.4 Encounter Sequence Number
   5.5 Trusted Date and Time Using Standard Eligibility Inquiry & Response
   5.6 Why Date & Time are Essential

6.0 Other Design Elements and Issues
   6.1 PAR on Referrals, Orders, Prescriptions
   6.2 Hash Data Element Must Be Calculated by Identity token
   6.3 Identity tokens do not Validate Digital Signatures
   6.4 Security Requirements for a Subscriber Identity Token
   6.6 Why Must PAR be included on the Claim?
   6.7 Exception Handling

7.0 Effectiveness of Patient Registration for Different Types of Fraud
   7.1 Fraud against which the Patient Registration process may be effective
   7.2 Major Fraud Types against which Subscriber Identity tokens are Ineffective
   7.3 Fraud Types Unrelated to Subscriber Identity tokens
   7.4 Amount of Claim Fraud in Healthcare
   7.5 So How Much Claim Fraud might the Process in this Paper Save?
   7.6 Other Issues

8.0 What is Required to Implement the Processes in this Paper?

9.0 Author Group

ATTACHMENTS

Attachment A: Description of Proposed Legislation
Attachment B: Deterministic Patient Matching in Provider Systems
Definitions

1. Secure Identity Token

An Identity Token, such as a smart card, in this paper is an internally secure microprocessor or a secure computer application, identifying one or more persons, with ability to communicate, authenticate a biometric, encrypt and decrypt, and sign a digital signature. A smart card or key fob would meet the functional and security requirements. A smart phone Application would easily meet the functional requirements; however, the authors did not investigate how such an application would meet the security requirements, which are described in §6.4 of Part Two of this report.

2. “Subscriber” Identity Token

This paper uses the generic term, Subscriber, while some health plans use the term, Member, and Medicare uses the term, Beneficiary. A Subscriber Identity token, such as a smart card, may identify more than one person. When it identifies multiple persons, it may be called a Family identity token. The general case in the paper is a subscriber family identity token.

The process described in this paper would require modifications to be made to the WEDI Health Identification Card Implementation Guide, NCPDP Pharmacy and/or Combination ID Card, and ANSI INCITS 284 health card standard. See first row of table in §8.0 for list of modifications that would be needed to support identity tokens.

3. Medical Identity Theft.

Medical Identity Theft occurs when one person uses another person’s name or identification to get prescriptions, medical treatment, or surgery, or when a claim submitter uses unauthorized identification for a fraudulent claim.  

4. “Initiating” Medical Encounter & “Subsequent” Medical Encounter.

This paper differentiates between an initiating encounter and a subsequent encounter, in which the patient is not present, that results from a referral, test, prescription, or other order from the initiating encounter. For example, a patient visits a doctor with a cough and receives a prescription. The doctor visit is the initiating medical encounter, and filling the prescription is the subsequent encounter. A subsequent encounter without patient presence, other than filling a prescription, is generally determinable from the claim item codes.

5. Patient Arrival Registration Number (PAR)

When a plan accepts patient registration signatures, it returns an encrypted PAR number; the subscriber identity token decrypts it; and the provider puts it on the claim. PAR is a new reference number. “PAR” is also used in context to mean the PAR patient registration process or the PAR workstation.

6. Secure and Unsecure

Only subscriber identity tokens issued by plans and PAR workstation microprocessors, registered with certificate authorities, are secure. 80% of fraud is from claim submitters, so the computers, equipment, devices, software, and procedures controllable by claim submitters must necessarily be considered unsecure.

Citation means: “See Section 4.0 in Part Two for more information.”
Tutorial
Encryption, Digital Signature, and Biometric Comparison

1. Symmetric Encryption
A symmetric encryption algorithm applies a Secret Key to a data stream and encrypts the data. Later, symmetric decryption applies the same Secret Key to restore the data stream exactly to its original state. Symmetric encryption and decryption is fast. Its problem is there is only one secret key, and both sender and receiver know it; so it may be unsecure as to proof of origin.

2. Asymmetric Encryption
Asymmetric encryption uses a pair of keys, a public key that can be widely known and a private key. Either key may be used to encrypt; then only the other key is able to decrypt. Which key is to be used to encrypt depends on the purpose. Sometimes, the sender knows only the public key while the receiver knows the private key, in which case encryption is performed with the public key. But if the receiver knows only the public key, the sender encrypts with the private key. Asymmetric encryption is slower than symmetric encryption.

3. Hash Data Element
A Hash algorithm creates a short data element, say 128 bits, from a data stream of any length such that the probability of a changed data stream resulting in the same Hash is very low. For security in the patient registration design, hash data elements are calculated by the identity token and workstation microprocessor, because they are secure.

4. Encryption of a Large Data Stream
Because hashing and symmetric encryption are fast, while asymmetric encryption is slow, encryption of a relatively large data stream consists of the following steps:
- Create a hash data element from the data stream.
- Encrypt the data stream symmetrically using a random secret key.
- Asymmetrically encrypt only the Hash and secret key using one of the asymmetric keys. This is sufficiently fast because it encrypts only two data elements.
- The receiver uses the other asymmetric key to decrypt the symmetric key and the hash data element. Then it uses the symmetric key to decrypt the full data stream.
- To assure data integrity, it recalculates the hash data element and compares it. It could eliminate this step if assuring data integrity after decryption is not important.

5. Digital Signature
A digital signature is asymmetric encryption of the hash using the signer’s private key. The receiver verifies the hash data element from the full data stream, then decrypts the signature using the signer’s public key, which it obtained from a trusted source, and compares the result to a recalculation of the hash. If they are the same, the signature is valid.

6. Biometric Comparison
The purpose of Biometric testing is to prove that the person being identified is physically present. For example, using facial recognition, a numeric template derived from a photograph of the patient is stored securely inside the identity token. During a medical encounter, the patient briefly faces a camera for another photograph that is converted to a numeric template, and the token’s microprocessor determines if the two templates are for the same person, in which case it determines that person is physically present.
Part One
Non-Technical
SECURE PATIENT IDENTIFICATION

Part One

PURPOSE. The Research Paper assesses the feasibility of adding a security role to subscriber and patient identification for use in a Real-Time Patient Arrival Identification (PAR) process. The research addresses the Question: “Could a secure subscriber identity token, such as a smart card, reduce medical identity theft, improve privacy, combat fraud by both claim submitters and patients, and enable deterministic patient matching in provider systems?”

The research finding is that it is feasible to attain these goals using secure identity tokens, such as smart cards, or a smart phone application that meets the functional and security requirements\[\text{§6.4}\].

SCOPE:

1. Inclusive of all U.S. Healthcare. Although pending legislation may focus on Medicare, this research paper pertains to all U.S. Healthcare.

2. The Paper does not Advocate. This paper is not advocacy; it only assesses feasibility of adding a security role to subscriber and patient identification. There may be other questions whether the process described in the paper should or should not be implemented, or in what ways it should or should not be mandatory, voluntary, or incentivized—but these are policy questions, and they are not addressed in the paper.

3. Other Policy. Policy questions are not in the scope of the paper. For example, nothing in this paper would deny treatment if registration of a patient is unsuccessful. That would be policy.

DESCRIPTION OF PATIENT ARRIVAL REGISTRATION

What does Patient Arrival Registration look like to patient? To register at the provider’s front desk or admissions, a patient inserts his or her subscriber identity token, faces a camera or touches a scanner, then waits 5 to 10 seconds. Nothing to remember, nothing to key in.\[\text{§1.3}\]

---

### Problems in U.S. Healthcare Addressed in this Paper

1. Unmatched Patient Record error rate in Master Patient Indexes and Health Data Exchanges may be 10-15%. Could a patient identity token, such as a smart card, could lower that to 2%?

2. Could reduction in unmatched and mismatched patient records improve Patient Safety?

3. Medical Identity Theft is victimizing 1.85 million persons annually. Could a secure patient identity token cut medical identity theft in half?

4. Stolen insurance identification is valuable in the black market. Could the patient arrival registration process in this paper make stolen information unusable for a fraudulent claim?

5. Personal Health records may be disclosed or wrongfully altered. Could a secure patient identity token improve protection of personal health records, especially protect against update for wrong person?

6. Would the process reduce fraudulent claims if it could prove to a health plan that the security token, patient, and provider workstation were physically present at the same time and place? The paper’s lower-bound estimate is $20 to $25 Billion annual savings from the process.
What happens in those seconds? The subscriber identity token, such as a smart card, verifies biometric identification, so the patient is physically present. Then the token and the workstation’s secure microprocessor digitally sign patient identification, insurance identification, provider identity, workstation ID, and the date & time, and it sends this data and signatures to the health plan’s real-time systems. The health plan validates the signatures, the acceptability of the information, and the date & time; and returns an encrypted PAR reference number.

PAR is evidence of the proof. The health plan returns an encrypted PAR. Only the subscriber identity token can decrypt PAR, proving the token is still present so that corrupt software cannot obtain PARs for different dates & times. PAR is a new reference number. It goes on the claim. [Definitions, §1.0(Steps 9-10), §1.2]

What does the proof consist of? PAR documents proof that: [§1.2]

- The patient is who he or she says—another person cannot impersonate.
- The patient is identified by the token—patient is subscriber, spouse, or dependent.
- Patient arrival registration took place in real-time—so current time is known.
- The patient, subscriber identity token, and registered provider workstation are physically present at the same place and time—so a fraudulent claim cannot have a different patient, different plan, unregistered claim submitter, or markedly different time without detection.
- When the provider integrates patient arrival registration with the provider’s systems, it sends the registration and insurance information automatically to the provider’s systems, and it also sends the patient’s biometric template to the providers Enterprise Master Patient Index system to enable deterministic patient matching. [Attachment B]

How is PAR used? The provider puts the decrypted PAR on the claim, and the plan compares it to its records of patient registration for consistency of patient, provider, and date & time. [§1.2, §6.7]

Can a PAR be used on another claim? A PAR reference number is only valid for a given patient, plan, and provider of the Initiating Medical Encounter at the given date & time, and it may be on a claim from another or same provider to the same or different plan for a Subsequent Medical Encounter, where patient is not present, such as prescription, test, or referral ordered by the provider of the Initiating Medical Encounter.
PAR cannot be used on a claim for another Initiating Medical Encounter to a different plan because that plan would have no record of it; or for a different patient because it is specific to the patient; or by a different provider because it is specific to the provider; or for a different time because it is specific to the date or time. And it cannot be sent twice to the same plan because the plan would instantly recognize it as duplicative.  

**Is there a fraud vulnerability with Subsequent Medical Encounters?  Yes, just as there is now.** It would be possible to use the PAR on a claim for a fraudulent Subsequent Medical Encounter where the patient is not present, although the plan would determine if it is medically consistent with its initiating medical encounter. This paper addresses how future enhancements to the process could resolve this vulnerability in §6.1.

**CAREFULLY BALANCED SET OF BENEFITS**

The patient arrival registration process consists of a carefully balanced set of benefits to healthcare providers, patients, and health plans to encourage participation. All parties benefit.

**What are Benefits to Providers & Health Data Exchanges?**  

- Positive patient identification. When interfaced from the Patient Arrival Registration process, the process enables deterministic patient matching in Enterprise Master Patient Index systems and health data exchanges. Probabilistic patient matching, particularly at data exchanges, has a 10-15% error rate of unmatched patient records while deterministic patient matching may have potential to reduce the rate closer to zero. [§1.4, §1.5, Attachment B]
- In 2009 MGMA estimated aggregate savings from automated cards at $2.2 Billion per year. The PAR process with automated conveyance of insurance information from the Identity Tokens would achieve the same efficiency.
- The required provider investment for patient arrival registration is very low, and return of that investment could occur in less than one year.
- The provider is not required to change registration procedures except to put PAR on claims.
- Positive identification of patients may avoid unpleasant resolution of identity theft and compromise of health records that otherwise might involve the provider's patients.
- Automation of eligibility inquiry occurs automatically along with patient arrival registration unless the provider submitted advance inquiry and elects to omit the second inquiry.
- Use of the real-time eligibility transactions in the PAR process could offer routine notice of the patient's status versus the Affordable Care Act's 90-day grace period for non-payment of premium. However, it is our understanding that standard eligibility transactions need update to provide for this information.
- The Subscriber Identity token could be capable of supplying admissions “clip-board” information. This possibility requires research and is not otherwise addressed in this paper.
- It may help with Meaningful Use Stage-3 government regulations. This possibility requires research and is not otherwise addressed in this paper.

---

2 David Batchelor, LifeMed, Inc.
3 Labor savings for either provider or plan from automatic eligibility inquiry are not estimated here because of insufficient data.
What are Benefits to Subscribers and Patients? Subscribers and patients benefit from:

- Reduced medical identity theft. Lower value for stolen insurance information because it is much less useful for claim fraud.
- Improved coordination of patient health records, especially from different providers, by using deterministic patient matching that is enabled by the secure identity token.
- Potential for more accurate, complete, longitudinal personal health records from different providers and different times, and increased privacy.
- Improved patient safety and reduction in redundant tests due to more complete and accurate longitudinal personal health records. [c.f. Positive Patient Identification below.]
- In time, the patient may gain more specific control over how health records are used\(^4\).
- The Subscriber Identity token could be capable of supplying admissions “clip-board” information. This possibility requires research and is not otherwise addressed in this paper.

The average person gets concerned about medical identity theft only after becoming a victim. He or she may receive a high deductible or co-payment bill for medical service or prescription not received, or see such treatment on an Explanation of Benefits report, or be badgered by a debt collector, or see unpaid medical collections on credit reports, or erroneously reach an insurance coverage limit. Worse, his or her health records may be altered for wrong blood type, test results, allergies, chronic illnesses, trauma, or treatments. That could affect future treatment. It could even affect employment opportunity. And it is not easy to correct.

Estimates in 2012 indicate 1.85 million patients are victims of medical identity theft annually\(^5\).

At present, medical identity theft is based only on identifying information, \(^[§4.0]\) which can be easily stolen. Or lose your wallet and the thief knows name, address, and health insurance information. Either is enough for a claim submitter to file a fraudulent claim or a fraudulent patient to receive treatment and cause erroneous update to your health records. Especially, lose a Medicare card, and if the beneficiary ID ends in “A”, that’s your Social Security Number, or “B”, that’s probably your spouse’s Social Security Number.

But with the process described in this paper:

- Medical identity theft will not let the wrong person get medical care because insurance identification is not enough.
- If a claim submitter uses insurance identification without patient participation, its claims would be outliers, subject to statistical analysis and investigation.
- Therefore, insurance information would have less value; so it becomes less likely to be stolen or used, at least for medical insurance reasons.
- If Medicare were to shift to identifiers that are not based on Social Security Numbers, a stolen or lost wallet would not give the finder a Social Security Number.
- So, less identify theft, less theft of insurance ID, less compromise of PHI, and less fraud.

The most important benefit may be the potential for improved care and outcome resulting from more coordinated and comprehensive and accurate health records. [c.f. Positive Patient Identification.]

\(^4\)For example, see ASTM standards for patient identifier, which includes a means to control which health records may be authorized for given medical specialties, diagnoses, and treatments.

\(^5\) Ponemon Institute, Third Annual Survey on Medical Identity Theft, June, 2012.
What are Benefits to Health Plans? Health Plans benefit from:  

- Improved customer service to the plan’s subscribers by enabling deterministic patient record matching, increasing protection against medical identify theft and compromise or wrongful update of personal health records, potentially resulting in improved care and outcome. 
- The subscriber identity token and the workstation microprocessor are secure. The plan cannot assume any other item in the claim submitter’s environment is secure.  
- Reduction in claim fraud. There are no definitive estimates of claim fraud in the U.S., nor distribution by types of fraud. §7.5 suggests savings of $20+ Billion per year from the patient registration process, or approaching 1% of claims. Most savings derive from fraud committed by claim submitters, not patients. Savings would be about 1/3rd of total fraud in healthcare. However, these numbers are tentative, and the authors welcome better data. 
- A health plan’s investment would include: (i) issuing subscriber identity tokens and (ii) enhancing or developing its real-time response systems for patient arrival registration. 
- More eligibility inquiries would be automated, and fewer served by telephone, for a savings in telephone service banks. 
- The plan would instantly recognize duplicate claims that use the same PAR. 
- The PAR process combat the following fraud types in differing degrees: 
  - Entire Claim is for Service Not Provided, without Patient Collusion. 
  - Fraudulent Claim with Patient Collusion. 
  - Fraudulent patient attempts to get medical treatment. 
  - Provider or Administrator Employee Makes Up a Wholly False Claim. 
  - Fraudulent subsequent encounter claims, after enhancement in §6.1 is implemented. 
  - Black Market claims after enhancement §6.1 is implemented.

DEVELOPMENT OF IDENTIFICATION STANDARDS

Why don’t Current Health Card Standards have a Security Function? 

When current health identification card standards were developed, beginning in the early 1990s, the standards group judged that a security function, other than an optional photo, was not feasible in the card standard. It explicitly rejected biometrics because of a card’s low data capacity and limited technology, but it advised monitoring for new security capability. Identity tokens, such as smart cards, now have unique security capabilities. The benefits described above for subscribers, providers, and plans would be due to adding security functions to subscriber identification.6

Current Pending Legislation

There are several bills in Congress that would affect identification cards in healthcare. Two bills specify use of identity tokens. This WEDI Subworkgroup does not advocate for or against pending legislation, and this paper is not intended to evaluate legislation, only to answer questions whether identity tokens could achieve the benefits intended in the bills. [Attachment A]

---

Why is the WEDI Subworkgroup Researching Secure Identity Tokens?

The group’s responsibility, in close cooperation with NCPDP and ANSI INCITS B10, is standardization of health cards, or in the more general case, identity tokens; so the group must be proactively responsive to technological change, to new functional capability—in this case, adding security functions to ID tokens—and to the direction that identification and security in healthcare will be going. It must to be alert to change.

The group, working with NCPDP and INCITS B10, is a good organizational choice to begin research on a security role for health identification. It offers industry-wide representation requisite for consideration of all points of view and to achieve consensus. Moreover, WEDI was at the beginning of health card standardization in 1992, and it publishes an implementation guide that is accepted. ASC X12, originally active in card standardization, declined the role because its charter does not include standards for a physical card, and INCITS B10 working alone has insufficient healthcare representation.

Healthcare organizations that are devoted to a single stakeholder group do not represent all points of view and could have difficulty gaining industry consensus involving other types of stakeholders. It is for this reason that there has been little activity by single-interest groups toward the technology examined in this paper. Hospitals cannot do it alone, nor doctors, nor dentists, nor health plans, nor patients. It requires synergy from all stakeholders to perceive the collective benefits.

THE QUESTIONS INVESTIGATED BY THE PAPER

This research paper investigates how the unique capabilities of identity tokens, such as identity tokens, might improve security in healthcare. It addresses three essential questions:

1. **Could secure identity tokens achieve what is claimed?** The primary question is, could adding a security role to patient identification achieve what is claimed in a manner that is practical, acceptable, and beneficial to the stakeholders? The paper concludes, yes.

2. **How would these security capabilities work and would they be acceptable?** But in order to answer “1” we must understand, first, *how* to use the technology to achieve the goals. That is necessarily a technical question. *How* cannot be answered without understanding use of the technology. And second, what would be the impact on patients, providers, plans, and others? Hence, Part Two of this research paper is technical and detailed.

3. **What change would be needed to ID standards?** Standards for a smart cards or other identity tokens are more involved than just specifying data. Indeed, these standards must specify a computer program, which includes:
   - Permanent and updatable data storage.
   - Communications protocol.
   - Transactions it will receive and send, including transaction content and execution.
   - Processing logic; that is, specifications for computer programs operating inside the token.
   - Assurance of interoperability.

   So, the application must be rigorously designed before specifying a new standard. [§8.0 1st row]
PROVIDER OPTIONS

The provider may elect either an inexpensive stand-alone workstation or the provider may integrate the workstation as a terminal into the provider’s computer systems.

1. Stand-Alone PAR Workstation Option

What is the Stand-Alone PAR workstation? A stand-alone PAR workstation consists of a docking station, a secure microprocessor chip, ports for the subscriber identity token and biometric scanner, and an application computer, such as a smart phone, for communications [§3.1]. The advantages of a stand-alone workstation are:

- Very low cost and quick installation.
- Very little required change to procedures and systems.

What does it cost for a provider to install a Stand-Alone Workstation? This paper estimates: (a) Time to install, one hour; (b) Time to train, 15 minutes per employee; (c) One-time expense estimated at $480 per workstation, and (d) increased communication cost of zero if provider already has Internet Wi-Fi, or $23 to $60 per month otherwise. These are modest expenses, and they are offset by efficiency and accuracy savings plus other benefits. [§1.4, §3.2]

What changes would be needed to provider systems to support a stand-alone PAR workstation? The only required change is to add the PAR number as one more REF number on a claim. No other change is required. [§1.4]

Why is it called a Stand-Alone workstation? It is “Stand-Alone” because it can be installed without necessarily interfacing to any provider systems.

What is the purpose of the Secure Microprocessor Chip in the workstation? The secure microprocessor contained in the workstation controls the PAR process, and provides secure identification of the workstation, registration of the workstation to the provider at a certificate authority, and the workstation’s digital signature sent to the health plan.

What is the purpose of the workstation’s computer? The workstation’s computer controls communications with a wireless printer and with the health plan or, if so interfaced, to the provider’s systems. If the process uses facial or voice recognition as the biometric and if the workstation’s computer is, for example, a smart phone, the phone takes the photos for facial recognition or records the voice. The workstation’s computer itself is not secure; only the subscriber identity token and the workstation’s microprocessor would be secure.

2. The Integrated Platform Option

What is the Integrated Platform option? At the provider’s option, the PAR workstation would be connected to a patient arrival registration application in the provider’s computers. The workstation is essentially the same, but communications, printing, and integration with the provider’s systems would be controlled by the provider’s computers. The advantages of the integrated platform are:

- It uses the same employee access security as already exists for the provider’s computer.
- The information could be automatically sent to the provider’s scheduling, billing, EHR, patient master index, and health data exchange systems.
POSITIVE PATIENT IDENTIFICATION

What is the value of Deterministic Patient Matching in Enterprise Master Patient Indexes (EMPI) and Health Data Exchanges? Currently, patient records are matched from different providers and different times using probabilistic methods such as matching on name, address, birth date, and other data. Error rates may be 10-15%.

The PAR process verifies the patient with a biometric, and it sends the patient’s encounter biometric template along with patient and insurance identification to the EMPI, where the match engine definitively links the patient to existing records.

Many large hospital networks are looking to identity tokens to cut into the error rate. With universal deterministic patient matching, using biometrics from the PAR system, the patient matching error rate might approach zero to 2%.

Such high accuracy offers significant potential over time:

- **For individual patient**: accurate, complete, longitudinal personal health record from different providers and different times; improved patient safety from more reliable health records; reduction in redundant tests.
- **For doctors**: The resource of Evidence-Based Medicine (EBM) enabling the physician to improve care by relating individual data, diagnoses, treatment protocol alternatives, and outcomes of an individual patient to statistical profiles drawn from thousands of patients.
- **For hospitals**: improved metrics on performance and outcomes.
- **For public health**: improved ability to detect and react to public health issues.
- **For disease & treatment research**: accurate and complete longitudinal, de-identified patient health records.

Will Positive Patient Identification at Arrival Registration Reduce Treatment Errors?
It offers potential to improve the integrity of patient health records with the concomitant benefits of accurate individual and statistical information described above, and it adds positive identification to preparation of wristbands and labels that may be used during treatment to reduce errors resultant from mismatched patients. However, it will not eliminate all errors of mismatched patients.

Will Patient Fraud Increase due to High Deductibles and Policy Cancellation?
Yes, it is reasonable that increased patient charges due to high deductibles and cancelation of policies for non-payment of premiums may increase the patient’s payment responsibility and thereby significantly increase incentive to use another person’s health insurance policy. But with real-time patient arrival registration, the need for the subscriber identity token’s presence and the need to pass biometric identification would block one patient using the insurance coverage of another. Only when the patient registration process is not followed would this type of fraud be possible.

---

7 On identification and patient safety: “Failure to correctly identify patients constitutes one of the most serious risks to patient safety and can lead to improper treatment and serious medical errors. Patient misidentification kills, and permits staggering levels of fraud, medical error and privacy violation.” Frank Mann, CEO BiomIDs, Inc., Jan 9, 2012.

8 A vulnerability is that a patient covered by the card passes its biometric test but then, unnoticed or condoned by provider personnel, the covered patient lets a friend or relative be the person treated resulting in fraud and
Effect if many providers and plans do not implement the process. Deterministic patient matching would be most effective if implementation were universal. If the PAR process is adopted but many providers or plans do not participate, the benefit of patient matching would be lessened. Especially, the benefits for an individual patient would not accrue if the patient’s provider does not participate or if the patient’s health plan does not participate. Yet the benefits derived from aggregation of health records would still be achieved depending on sufficient numbers and reasonable statistical distribution across the population.

FREQUENTLY ASKED QUESTIONS

The following address other questions and concerns raised during review of this paper:

What Impact is there to a billing service, clearinghouse, or other entity processing claims? The entity that formats and routes claims does not matter to patient registration process, which in its simplest form is stand-alone. The only relevance is inclusion of PAR on the claim.

But there would be impact if the provider outsources patient registration. [§1.0(Step 7 Alternative)]

Critical Mass of Providers is Needed for Scale and Sustainability. If patient arrival registration process were implemented nationally, adoption by providers in large numbers is requisite to sustain transition toward universal acceptance and usage\(^5\) by patients and private plans. Initially, there must be a critical mass of providers adopting it. That may require a mandate, contract, or other incentive to attain adoption by sufficient numbers of providers. If a bill were passed for Medicare to implement identity tokens, such as specified in current legislation, that would appear to accomplish the requirement. [Attachment A] Yet, any non-participating provider is a vulnerability in the PAR process; so the objective is universal adoption of the process.

For providers, patient arrival registration is just the first phase toward better patient identity. Looking only at the first phase, implementation of patient arrival registration with a stand-alone workstation is very fast, procedures and systems remain the same, costs are minimal, and costs are offset by savings from accuracy and efficiency. But subscriber identity tokens can be the Identity Tokens sought by providers to achieve deterministic patient matching resulting in significant improvement in accuracy and efficiency of matched health records, a much lower error rate, a reduced risk of error, especially error affecting treatment, and a lower staff. [Attachment B]

Will patients accept biometric verification? It is reasonable that patients will accept non-intrusive biometric verification, such as facial or voice recognition or single fingerprint, if explained, because patients benefit from improved personal health records, protection against medical identity theft, and protection against compromise or wrongful alteration of personal health records.

Consumers already accept facial recognition for drivers licenses, passports, visas, and other identification (although while they readily accept giving an initial reference biometric, most of these applications do not involve overt patient action to obtain an encounter biometric). Consumers also accept intrusive TSA screening at airports in order to board an airplane. They agree to being contamination of personal health records. Registration at a kiosk is especially vulnerable. Hospitals and outpatient clinics, where larger claims are more likely, can largely eliminate the problem by putting a wrist band on the patient.

\(^5\) Concept adapted from *Diffusion of Innovations*, Everett Rogers, 2003.
photographed when using an ATM machine to obtain cash. Consumers know from television crime reports that surveillance cameras are everywhere.

Nevertheless, acceptance of biometric verification is one factor to be measured in pilot programs and focus groups. Without biometric verification, benefit estimates would be reduced significantly.

[c.f. “Summary of Questions for Design and Testing” at end of Part One, §5.3 and Attachment A]

**Would putting a biometric identifier on a token be difficult?** The exact method is left for detail design. It is recognized that obtaining the reference biometric will be a project.

If facial recognition were used, the sponsor, employer or licensed insurance agent, might submit an electronic frontal-face picture securely to the health plan for registration on the subscriber Identity token. Or in many cases, a facial recognition template for the subscriber could be obtained, with legal authorization, from driver license or state-issued ID records. Obtaining the template directly from state records disallows templates being obtained from thousands of counterfeit drivers licenses.

Dependent-only tokens (e.g. student away at school) could be registered in the same way. A spouse would be registered either the same way or as a dependent.

For minor dependents pre-registered on a family token who would like to use the token without being accompanied by the subscriber, the subscriber would be present to pass the biometric test the first time. Then the subscriber identity token would store the dependent’s biometric template on the token and send it to the plan. After that, the dependent would not need the subscriber for future encounters.

Detail design should also look at the ease for a subscriber to change plans. If the change is with the same insurer, there should be no difficulty as the insurer would have the subscriber and dependent biometric templates on file. If to a different insurer, it may be possible to transfer the templates to the new insurer automatically.[§5.3]

**What about Kiosks, Home Health, Telemedicine?** Patients may self-register using a kiosk, or be treated remotely as in telemedicine, or be treated at home as in home health. For kiosk registration, the microprocessor in the kiosk is activated by a log-in (c.f. §1.0(Step 1)). For home health, the provider uses a portable PAR workstation. Telephone patient-provider consultation, as opposed to telemedicine, would not involve patient arrival registration, and it generally bills a small claim of low risk. When telemedicine is an initiating medical encounter, it also generally bills a small claim. When telemedicine bills as a larger claim, it is generally a form of subsequent medical encounter involving equipment for treatment via telecommunication, so there may be a means with that equipment to process the subscriber identity token.[§1.5, §6.1, §6.7]

**Would Telephone Pre-Registration Continue? Yes.** Many providers obtain insurance identification from a patient over a telephone in advance of admission. Telephone pre-registration should continue as now if that procedure continues to be efficient for the provider. To support this function, the subscriber ID would need to be displayed to enable the patient to read it and convey it to the provider.10 Patient Arrival Registration using a subscriber identity token would occur on arrival at the provider’s admissions desk, and it might omit the second eligibility inquiry.

---

10 H.R. 3024 (Attachment A) specifies that the Medicare Beneficiary identifier not be printed in human-readable form on the card. That would eliminate telephone pre-registration and likely result in patient & provider resistance.
Why emphasize subscriber identity tokens when Claim Submitters commit the most fraud? The majority of fraud is committed by claim submitters, not by patients, perhaps by a ratio up to 12:1. Patient Arrival Registration process is effective against fraud committed by claim submitters because it requires that the subscriber identity token is present, the patient is present, the patient is who he or she says, the patient is covered by the card, and the registered workstation is present, all at the same time and place. These requirements make certain types of claim fraud difficult to commit.

Why not just use a second form of identification, such as a drivers license? Since 80% of fraud is committed by claim submitters, asking the claim submitter to check a second form of ID visually is completely ineffective against fraud by the claim submitter. In contrast, new security capabilities, such as biometric verification and digital signatures, enable positive identification and are very secure.

Why not just test the patient’s biometric? This simplistic approach would test the patient’s biometric identifier in the provider’s office. Because the environment is unsecure, it would not give any proof to the health plan that the test was performed, that the test was positive, or the time and place when this allegedly occurred. This method is no better than asking providers to verify a second identification such as a drivers license (see above), but additionally it would require investment, so the return would be a net loss.

Much the same investment would be required by this method such as (i) issuance of identity tokens with reference biometric to all subscribers, (ii) a mechanism to add reference biometrics for dependents, and (iii) a workstation and biometric scanner to obtain the encounter biometric and report whether the two match.

At its best, this approach would detect a portion of patient impersonation fraud; it could not detect claim submitter fraud. It would be vulnerable to a provider accepting the patient even if the biometric test is not performed or if the test fails. It could detect no fraud committed by claim submitters. It could exacerbate mismatching patient records. It may not combat medical identity theft nor ensure safe patient records. In short, it would not prevent enough fraud to repay the investment, and it would return little other benefit.

Would this approach be better if it included date & time? No. Date & time must be confirmed by a secure source, such as by the health plan’s real-time systems affirming the workstation’s date & time. Without confirmation, date & time are unsecure.

Why is insurance information unsecure? Current health insurance cards—or current smart phone applications—only convey information. A claim submitter needs only this information to submit a fraudulent claim. Therefore, stolen information is valuable, leading to medical identity theft, access to and wrongful update of patient health records, and claim fraud. In contrast, the PAR process described in this report, involving a subscriber identity token with biometric verification, and validation by the plan in real time, ensures positive patient identification thereby (1) enabling deterministic patient matching for health records, (2) preventing the wrong person receiving treatment, (3) removing motivation for theft of identification, and (4) making certain types of fraudulent claims difficult.
Could the subscriber use a smart phone as an identity token for PAR? Many plans are enabling subscribers, as an option, to use a smart phone application instead of an insurance card. More research is needed to understand how the application could meet security requirements so that the phone could become a secure subscriber identity token for the PAR process.  

Will new technology supplant identity tokens? The physical form of an identity token is not an issue. So long as it is secure and can communicate, verify biometric identifiers, process data, encrypt and decrypt, digitally sign, and otherwise meet the requirements for this application, it would be acceptable. Also, smart cards, smart phone Applications, and other identity tokens will improve over time.  

Won’t Real-time Patient Arrival Registration be a stretch for private plans? This research paper is intended for all health plans, not just Medicare, but except as there may be new law to mandate it¹², a plan’s implementation of the patient registration process would be optional. The reasons a plan may choose to implement the process are to obtain (a) the financial benefits of reducing fraud and (b) the customer service benefits for their subscribers. These motivations are to be found in each plan’s own analysis of their expected return on investment. It’s up to each plan. Consequently, the status of a plan’s real-time eligibility systems is not relevant to this paper. Additionally, while some plans do not support real-time standard 270/271 eligibility transactions, many of the same plans support direct data entry (DDE) of eligibility inquiries and therefore already have the data base and real-time servers. Implementation for DDE plans is to add translation of the enhanced standard eligibility transaction into the internal form by which their programs respond to DDE eligibility inquiry, and to add processing and data management for the patient registration exchange. That is, DDE plans are not too far behind those plans that already support real-time standard 270/271 eligibility transactions.  

Does the paper include a cost estimate for plans? No. The paper describes what is required to implement the patient registration process. Please see the requirements for plans in the overall list at §8.0 “What is Required to Implement the Processes in this Paper”. The cost for each plan depends on its current systems status and capabilities; for example, if the plan already has a real-time eligibility inquiry system, implementation is enhancement to that system; if not, then implementation requires real-time capability to be added as well. Therefore, cost estimation is necessarily left for the plan. In either case, the benefits to its customers from reduction in identity theft and compromise of private health records, and the financial benefit to plans from reduction in fraud appears to yield a high return on investment.  

Could a health plan elect to implement patient registration in batch mode? No. The PAR includes proof that the patient and provider were in the same place at the time of patient registration. It is the same time because the provider and plan agree to the time within a few minutes. If conducted in batch, date and time could not be proved.  

¹² Proposed reasons for mandating that health plans participate are to facilitate universal use of identity tokens to enable deterministic patient matching. The financial benefit to a plan from fraud prevention is very significant, arguing that a mandate may be unnecessary. This paper assumes implementation is optional for health plans.
Won’t it take a long time to add a reference number to claim standards? No. PAR could be included in standard transactions in a REF Segment; for example, it could be another REF Segment in Loop 2300 in an 837I claim, which loop in the standard already allows for more REFs than specified in the guide. The Reference Identification Qualifier is obtained from an external code list, which means the X12 standard itself need not be changed to add PAR to a standard transaction, only the addition of another REF a loop and a new Qualifier value in the external code list. Inclusion of PAR appears to be standards maintenance. [c.f. HIPAA Claim Standards]

However, while PAR for the initiating medical encounter must be included on a claim, in time it could also be included with suffixes on referrals and test orders and on the claims for these subsequent encounters. Inclusion of the initiating encounter PAR + suffix on subsequent encounter claims is an enhancement that could solve a vulnerability in the future. [§6.1]

Shouldn’t our Priority be to Concentrate on Administrative Simplification? Yes. Especially, shouldn’t we concentrate on automated eligibility inquiry and response since too many providers still telephone for eligibility, and health plans have to employ huge staffs to answer the telephone? The patient registration process described in this paper uses an enhanced real-time 270/271 standard eligibility inquiry and response. So checking eligibility is an added bonus toward Administrative Simplification and therefore the priority is exactly right. [§1.0 Step 7]

Won’t it also take too long to enhance the standard 270/271 real-time eligibility transactions to accommodate new information required for patient registration? No, but if enhancing the 270/271 were to be the obstacle, then the process could as easily employ any transaction format other than the eligibility standard, in which case eligibility inquiry would not be an added bonus. Besides, what’s “too long” when the question here is whether it can be done?

Shouldn’t we start with something simple and enhance it over time? Yes, Absolutely! Starting with simple is what the design in this research paper does. It adds the simplest, feasible security function to insurance identification. It conserves current procedures and systems for insurance identification so that its implementation causes almost no impact to the customs and practices of patients and providers. It defers later enhancement to solve a vulnerability (which exists now) in Subsequent Encounters at which the patient is not present and the claim is significant. It defers to later research analysis of fraud types against which subscriber identity token security capabilities are less effective. And it enables deterministic patient matching to be implemented over time. Please refer to §1.4 “Start Simple” for its application of Gall’s Law on Systems that work. [§1.4 “Start Simple”, §6.1, and Attachment B]

Will this stop all medical identity theft or all fraud? No. No technological process will solve all identity theft or all privacy invasion or all claim fraud. There will still be fraudulent claim submitters willing to risk outlier status, patients willing to cheat, patients willing to collude, and other wrongs that are not subject to the patient registration process. And there are exceptions where the full registration process may be inapplicable. [§1.1, 6.1, 6.7, 7.2, 7.3]

Isn’t this just too complicated? Absolutely not. It is not complicated in the slightest for a patient who inserts a token, smiles, and waits 5 to 10 seconds. It is not complicated for a provider, who receives a PAR number and puts it on the claim. It is amazingly simple for users. Like a radio with two knobs—very simple on the outside; complicated on the inside. [§1.0, §1.3, §1.4]
Yet the process would be a significant development for identity token vendors. The data, transactions, communication, and program logic internal to the microprocessor of the identity token will be significant; yet that is what these vendors are in business to do.

It is only a moderate investment for health plans to issue identity tokens and implement real-time patient registration, while fraud prevention and customer service proffer extraordinary incentive.

Also, the industry could consider shared development of interoperable modules for internal microprocessor applications and for the health plan’s real-time PAR system.

Is Patient Arrival Registration using Identity tokens Practical? Yes. The conclusion of this research paper is that real-time patient arrival registration is practical. For patient and provider there is minimal change. Benefits to the patient are significant and tangible.

The provider invests little for a stand-alone installation, financially gains in accuracy and efficiency, and may avoid unpleasant resolution of medical identity theft that might involve its patients. The process offers the industry opportunity for routine notice of the patient’s insurance premium status versus the Affordable Care Act’s 90-day grace period for non-payment of premium. And the provider and health data exchanges gain opportunity for deterministic patient matching in their Enterprise Master Patient Indexes.

The health plan’s investment is moderate, and the plan receives benefit from improved subscriber service and financially from significant reduction in fraud.

That is, we begin with a simple, inexpensive, and practical system and build upon it over time.

How Does it Work? (Non-Technical)

1. The subscriber identity token is inserted into an PAR workstation that has a secure microprocessor, a smart phone or other small computer, and communications.  
2. The subscriber identity token verifies biometric identification of the patient. It compares an encounter template of the patient to a reference template in the token.
3. The subscriber identity token and the workstation’s microprocessor exchange information on the subscriber, insurance identifiers, patient, workstation, provider, and date & time.
4. The workstation’s microprocessor digitally signs for all the patient and provider data and the date & time, and it sends it to the subscriber identity token. This signature is the provider side of the tripartite proof of patient, provider, plan, with common location and date & time.
5. The subscriber identity token creates a digital signature covering all the data including the microprocessor’s signature and the results of biometric verification, and sends the data, signatures, and date & time via the workstation to the health plan.
6. The health plan verifies the signatures, date & time, and whether patient is enrolled. It assigns a PAR, encrypting it with the subscriber’s public key, signs all the data, and sends it back.
7. The PAR workstation sends the PAR to the subscriber identity token for decryption, proving the subscriber identity token is still inserted, and prints or transmits a report of the patient registration including the decrypted PAR, which the provider includes on the claim.
Summary of Questions for Design and Testing

Security.
1. Can the biometric be spoofed?
2. Can templates obtained from, say, a motor vehicle department be used to spoof?
3. Can the PAR workstation eavesdrop to obtain encounter templates and keys?
4. Is the trust infrastructure for workstation microprocessors adequate?
5. Is it possible, given a public key and sample signatures, to derive the private key?

System.
6. Is the PAR process fast enough?
7. Are the systems using different identity tokens and different health plans interoperable?

Patient.
8. Will patients accept need for biometric?
9. Will patients present their subscriber identity tokens at medical encounters?

Provider.
10. Will the percentage of participating providers be sufficient for a “critical mass”?
11. How long will it take to achieve universal adoption of PAR by all providers?
12. How long will it take for adoption of the subsequent encounter enhancements in §6.1?
13. What percentage of providers will employ biometric templates for deterministic patient matching?

Fraudulent claim submitter.
14. With what propensity and speed will fraudulent claim submitters move out of pilot areas?
15. With what propensity and speed will fraudulent claim submitters shift to other types of fraud?

Health Information Exchange.
16. What percentage of health information exchanges will employ biometric templates for deterministic patient matching?

Health Plan.
17. Will the design for maintaining reference biometric templates be reasonable?
18. What percentage will elect to participate in order to realize the high investment return from prevented fraud while also improving customer service?
19. Will a sufficient percentage of plans participate to enable deterministic patient matching? Does deterministic patient require near universal adoption of PAR?

Legal
20. What new law provisions, if any, would be needed:
   a. to mandate or incentivize necessary participation?
   b. to permit plans to capture biometric templates from state sources?
Part Two

How could subscriber identity tokens be used?

(Technical & Detail)
REAL-TIME PATIENT ARRIVAL REGISTRATION

Part Two

1.0 Feasible Design for Using Secure Subscriber Identity tokens

Step 1: Log-In to Activate PAR workstation

If the workstation is stand-alone, log-in and log-out is via the workstation’s smart phone or other small computer. If it is integrated into the provider’s systems, log-in and log-out is via an instruction from the provider’s computer. In either case, the log-in is processed by the workstation’s microprocessor. Log-out also occurs after an inactive period or absence of power.

After log-in, the PAR workstation will have the following data elements:

13 Note each step is numbered according to the circled annotation in the process chart above.
• Identifier of the workstation.
• Identifier of the provider to which the workstation is registered.
• Identifier of the trusted source of the workstation’s Public key.

Step 2: Patient Log-In using Subscriber’s Identity token

a. Data sent to subscriber identity token. When the subscriber’s Identity token is inserted, the PAR workstation sends the following data elements to the subscriber’s token:
   • Date and time obtained by the PAR workstation via cell phone or Wi-Fi network, or from the provider’s computer systems.
   • Identifiers of the workstation and provider to which it is registered.
   • Identifier of the trusted source of the workstation’s Public key.

b. Data Sent to PAR workstation. In reply, the subscriber identity token will send the following data elements to the PAR workstation:
   • Patient identification = Issuer ID + Subscriber ID + Group ID + Dependent Code
   • Result of Biometric internal comparison (0=not required, 1=pass, 2=pass as dependent, 3=fail). A dependent may have registered a biometric reference template on the token and if that is used for the test, it is marked as “pass”. “Dependent Pass” means the subscriber or spouse provided the successful biometric test.
   • Encounter sequence number
   • Result of PIN internal comparison if applicable (0=not required, 1=pass, 3=fail).
   • Instruction where to send real time patient registration information to the health plan.

Step 3: Workstation Sends Patient Info to Workstation’s Microprocessor

The PAR workstation sends patient information to the microprocessor, and it requests the workstation digital signature, SigWS. The patient information sent consists of:

• Patient identification = Issuer ID + Subscriber ID + Group ID + Dependent Code
• Date & Time obtained by the PAR workstation

Step 4: Microprocessor responds with workstation’s Digital Signature, SigWS

The microprocessor responds with the workstation’s Digital Signature, SigWS, signing for the following data:

• Patient identification = Issuer ID + Subscriber ID + Group ID + Dependent Code
• Identifier of the Workstation
• Identifier of the Provider to which the workstation is registered.
• Identifier of the trusted source of the workstation’s Public key.
• Date & Time obtained from the PAR workstation

Step 5: Workstation’s Signature Sent to Subscriber Identity token

The PAR workstation sends its digital signature, SigWS, to the Subscriber Identity token and requests the Subscriber identity token’s signature, SigSub.

Step 6: Subscriber Digital Signature, SigSub, Sent to PAR workstation
The Subscriber Identity token sends its digital signature, SigSub, to the PAR workstation. The signature covers the following data:

- Patient identification = Issuer ID + Subscriber ID + Group ID + Dependent Code
- Identifier of the workstation
- Identifier of the Provider to which the workstation is registered.
- Identifier of the trusted source of the workstation’s Public key.
- Date and Time from PAR workstation
- Result of Biometric comparison (0=not required, 1=pass, 2=pass as dependent, 3=fail)
- Subscriber identity token’s Encounter Sequence Number incremented for this signature
- Result of PIN comparison if applicable (0=not required, 1=pass, 3=fail).
- Digital signature of workstation, SigWS

**Step 7: Eligibility Inquiry Sent to Health Plan with SigWS, SigSub, and Data**

The PAR workstation sends a simple eligibility inquiry including the Subscriber identity token’s signature, SigSub, the workstation’s signature, SigWS, and all associated data. The PAR workstation does not possess data to make a more specific eligibility inquiry.

The purpose of the inquiry here is for the health plan to validate date & time, subscriber signature, workstation signature, and to determine that the patient (subscriber, spouse, or dependent) is enrolled. The plan also ascertains that the subscriber identity token is not lost, stolen, or deactivated. Often the provider will have sent a more detailed eligibility inquiry; so there would be a code in the standard transaction to indicate its use for patient registration only.

**Alternative.** The health plan might engage an agent, such as a clearinghouse, to perform the function; however, there are several complications: (i) the plan has the file of subscriber public keys and that would have to be available to the agent; (ii) the plan has the files of lost, stolen, and deactivated tokens, and those would have to be available to the agent; (iii) the plan would need to authorize the agent to sign the patient registration data on its behalf, and that would require the agent knowing the applicable private key for the plan; and (iv) engaging an agent requires software and connection to move considerable data between agent and plan daily.

**Step 8: Health Plan Retrieves Workstation’s Public Key**

The health plan retrieves the workstation’s public key from a trusted central source for the purpose of verifying the workstation’s signature, SigWS. The health plan already has within its own files the public key to validate a subscriber identity token’s signature, SigSub.

**Step 9: Health Plan Eligibility Inquiry Response**

The health plan responds to the eligibility inquiry. It sends the following data elements in its response to the PAR workstation:

---

14 A theoretical variation would be for all subscriber identity tokens for a given plan to use the same pair of public-private keys, but that would introduce a serious vulnerability to the security of subscriber signatures, damaging the full fraud reduction potential.
It answers whether the patient is enrolled unless the transaction is coded to be registration only.

If the health plan accepts the patient registration, it returns the plan’s digital signature, SigPlan, signing for the full data set.

The full data set, including information developed by the plan:

- Result of the validation of SigWS and SigSub.
- Date & time from the health plan’s source.
- Result of comparing the date & time sent to the plan from PAR workstation to the date & time maintained by the health plan’s computer. Some discrepancy is expected; so the health plan accepts registration of the patient, workstation, and date & time if the difference between the two dates & times is not greater than, say, 15 minutes.
- The encrypted Patient Arrival Registration number (PAR) assigned by the health plan. The plan encrypts PAR using the subscriber identity token’s public key such that only the subscriber identity token is able to decrypt it. After decryption, the provider includes this reference number on its claim for the initiating medical encounter. It also makes PAR available on referral, test order, and prescription transactions to tie these and subsequent transactions to the patient registration. See §6.1 for fraud vulnerability and solution on subsequent medical encounters.

**Step 10: Decrypt Patient Arrival Registration number PAR**

The PAR workstation sends the encrypted PAR to the Subscriber Identity token. The Subscriber Identity Token decrypts PAR using its private key, which is known only inside this token, and sends the decrypted PAR back to the PAR workstation. This step ensures that the subscriber identity token is physically present at the time and place that the patient is being registered with the health plan. It prevents a fraudulent claim submitter from performing Steps 1 through 6 for a future date, then later performing the remaining steps at the future date and time to get another valid PAR applicable for a future fraudulent claim.

**Step 11: Report or Interface**

- **Simple Report.** The simplest installation is stand-alone; it can be installed immediately with little impact on provider systems. A stand-alone PAR workstation prints results of patient registration on a local printer. The report documents the full registration data set, but the information most essential for the provider is that the patient registration was successful, and it includes PAR for inclusion on the claim and on referral, test order, and prescription transactions resulting from the encounter. Easy use of the report is attachment of it to the folder for the patient’s office visit such that PAR can be readily entered on the claim.

- **Interface to Enterprise Master Patient Index and Other Systems.** But in a more automated installation, installed later at provider’s option, the PAR workstation sends information, including the encounter biometric template, to the provider’s EMPI, billing and EHR systems for deterministic patient matching and use in other processing. [Attachment B]
1.1 Other Operating Environments

The process described above uses the environment for patient registration for the initiating medical environment where the patient appears at the medical practice’s front desk or hospital admissions or similar. There are other environments:

- **Kiosk Registration, Vulnerability to Fraud.** Some providers perform patient registration using kiosks. The patient registration process would work the same. The result is either a printed report that the patient takes to various treatment stations, or the process may be interfaced to the provider’s scheduling, billing, and EHR systems. Kiosk registration is vulnerable to a valid patient passing the biometric test but a companion being the actual patient.

- **Home Health Registration.** The PAR workstation must be mobile. It would work in the same manner—documenting that the subscriber identity token, patient, and workstation are present at the date & time of the home visit. The resulting information would be reported via structured email to the home health provider office. An additional feature of the PAR workstation may be obtaining coordinates from the smart phone’s GPS capability to ascertain where precisely the medical encounter took place. Procedures for mobile usage will be addressed in detail design to ensure against vulnerability to fraud.

- **National Disasters.** The American Medical Association, under a grant from the Centers for Disease Control, completed a study and pilot test in 2012 on how better to manage the medical, living, and rehabilitation needs of persons displaced by national disasters. The project used Hurricane Katrina as a model for natural disaster and included in the study the implications arising from other types of disasters. The AMA study recommended employment of a “Health Security Card” (HSC), which would be an identity token such as the subscriber identity token in this paper. Some displaced persons might already have an HSC and bring it with them during evacuation from home. Others may forget to bring it or not have been issued one, in which case the disaster relief organizations would issue HSCs to them. The HSC would be used to identify, to convey insurance identification, to list salient medical conditions and requisite medications, to record medical encounters, and other data. It would also perform a role in restoring separated children and families.

  A key finding was that persons are much more apt to carry their card if it also serves other functions; for example, if it is also the person’s Medicare or Medicaid card, or other insurance. So it is possible that Subscriber Identity tokens described in this paper could be a means for wider and more reliable acceptance of HSC cards by the populace.

- **Telemedicine.** Addressed as an exception in §6.7.

---

15 Reference: James J. James, MD, DrPH, MHA; Director, AMA Center for Public Health Preparedness and Disaster Response; Health Security Card Grant; 515 N. State Street, HQ 8520; Chicago, IL 60654
1.2 What Proofs have been Documented by the Above Process?

Current paper, magnetic stripe, and bar code cards convey patient and insurance identification only; so anyone who knows the information may be able to capture the patient’s identity, see and modify the patient’s health records, and send a fraudulent claim.

The patient registration described here offers proof at the initiating medical encounter that:

- The subscriber identity token was physically present.
- The patient is enrolled in the health plan and is identified by the subscriber identity token.
- The patient is who he or she says. See §5.3 Biometrics—Dependents.
- The workstation is identified and registered to the provider.
- The above proofs all occurred at the same date & time agreed by workstation and plan.
- All the proofs are identified by a PAR number.

The Patient Arrival Registration number PAR is specific to the initiating medical encounter and is entered on the claim for this encounter. The plan compares the claim to the patient registration record; so because the plan would detect a discrepancy instantly, PAR cannot be used on another claim for a different patient, provider, plan, or date & time, nor on a duplicate claim.

PAR is also entered on claims for subsequent encounters, such as referrals, test orders, and prescriptions resulting from the initiating medical encounter. But if the patient is not present at the subsequent encounter, there is a vulnerability but also a solution, described in §6.1.

1.3 How Long must the Subscriber identity token be Inserted?

The estimated wait time from when the patient inserts the subscriber identity token until the patient can remove his or her token (Steps 2 through 10) is as follows:

<table>
<thead>
<tr>
<th>Steps</th>
<th>Description</th>
<th>Seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Patient Log-In using Subscriber’s Identity token</td>
<td>0.50 – 1.00</td>
</tr>
<tr>
<td>3-4</td>
<td>Obtain workstation’s digital signature</td>
<td>0.50 – 1.00</td>
</tr>
<tr>
<td>5-6</td>
<td>Obtain Subscriber identity token’s digital signature</td>
<td>1.00 – 2.00</td>
</tr>
<tr>
<td>7-9</td>
<td>Health Plan receives and responds to eligibility inquiry &amp; registration</td>
<td>2.00 – 4.00</td>
</tr>
<tr>
<td>10</td>
<td>Subscriber identity token decrypts patient registration reference number</td>
<td>0.25 – 0.50</td>
</tr>
<tr>
<td></td>
<td><strong>Total Time Subscriber identity token Must be Inserted</strong></td>
<td><strong>4.25 – 8.50</strong></td>
</tr>
</tbody>
</table>

The second or two needed for the patient to enter a PIN or provide the encounter biometric template is not added because (i) processes within the subscriber identity token need not be serial and (ii) the patient is occupied by the PIN or biometric so that it does not feel like wait time.
1.4 The Design Meets Practical Requirements for Healthcare Providers.

The following table describes the requirements to install and use a stand-alone PAR workstation as described in this paper. A typical medical practice with multiple physicians would need only one or two PAR workstations per office.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>One-time Capital Cost to Provider</td>
<td>The one-time capital cost of an PAR workstation, is estimated to be $480.</td>
<td>§3.2(1)</td>
</tr>
<tr>
<td>Operating Cost to Provider</td>
<td>No incremental cost if provider already has Wi-Fi Internet, or $23 to $60 per month for cell phone.</td>
<td>§3.2(2)</td>
</tr>
<tr>
<td>Ease of Installation</td>
<td>Less than an hour.</td>
<td>§3.2(3)</td>
</tr>
<tr>
<td>Universality</td>
<td>Subscriber identity token is standard for all subscribers. Workstation microprocessors are standard. Transactions are standard.</td>
<td>§6.4</td>
</tr>
<tr>
<td>No Change in Procedure</td>
<td>The provider’s procedures for registering a patient at the front desk or admissions would be almost completely the same as presently. The only required change is inclusion of the PAR reference number on the claim.</td>
<td></td>
</tr>
<tr>
<td>Effectiveness</td>
<td>Enabling deterministic patient matching, and combating Identity Theft, Compromise of Health Records, and Claim Fraud as described in Part One of this paper.</td>
<td>Part 1 and §7.0</td>
</tr>
<tr>
<td>Evolution from Simple to Complex</td>
<td>The design here for a subscriber identity token process can be implemented to quickly reduce identity theft, privacy invasion, fraud committed by claim submitters, as well as patients, and enable deterministic patient matching. It can be integrated into the provider’s Enterprise Master Patient Index system to enable deterministic patient matching. Later it can be enhanced with processes for provider identity tokens to further combat the remaining claim fraud.</td>
<td>See “Start Simple” below</td>
</tr>
</tbody>
</table>

1.5 Start Simple: An Application of Gall’s Law.

The intent of the process, if implemented, would be to start reducing medical identity theft, privacy invasion, theft of insurance information, and claim fraud immediately. The stand-alone PAR workstation methodology described in this paper meets that requirement. Meanwhile, the initial processes can evolve into more comprehensive, more complex systems that resolve the subsequent encounter vulnerability (c.f. §6.1), enable deterministic patient matching (Attachment B), and use other methods to combat the substantial remaining fraud.

The proposed design conforms to Gall’s Law\textsuperscript{16}: “A complex system that works is invariably found to have evolved from a simple system that worked. A complex system designed from scratch never works and cannot be patched up to make it work. You have to start over with a working simple system.”

2.0 Digital Signatures and Full Data Set

2.1 The Three Digital Signatures used in Patient Registration

1) Digital Signature by the Workstation (SigWS). The workstation's microprocessor signs for data identifying the workstation, provider, source of workstation's public key, Date & Time from the PAR workstation, patient identity, and insurance information. The signature is specific; a fraudulent claim submitter cannot use this signature for another time, patient, or workstation.

2) Subscriber identity token digital signature (SigSub). The subscriber's Identity token signs for all the data, including SigWS, to document that the Subscriber identity token was presented to the workstation at the date & time. A biometric proves that the patient, or a parent confirming for a dependent, was present. See also §5.3 Biometrics—Dependents.

3) Health Plan digital signature (SigPlan). The health plan validates the registration, encrypts PAR and signs the full data set.

2.2 Data Elements Included in the Three Digital Signatures

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Source*</th>
<th>SigWS</th>
<th>SigSub</th>
<th>SigPlan</th>
<th>Claim</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient ID: Plan, Subscriber, Group, DepID</td>
<td>SC</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Workstation ID</td>
<td>WS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>ID of Provider to which workstation is registered</td>
<td>WS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Workstation’s public key trusted source ID</td>
<td>WS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Date&amp;Time from workstation or provider’s sys</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date &amp; Time obtained from health plan</td>
<td>PL</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Result of biometric comparison (0=not req, 1=pass, 2=dependent pass, 3=fail)</td>
<td>SC</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Result of PIN (0=na, 1=pass, 3=fail)</td>
<td>SC</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Subscriber identity token’s encounter seq no.</td>
<td>SC</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes, New</td>
</tr>
<tr>
<td>Address &amp; log-in to send patient registration</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encrypted PAR from Plan</td>
<td>PL</td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAR Decrypted by Subscriber Identity token</td>
<td></td>
<td></td>
<td></td>
<td>Yes, New</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital signature from Workstation</td>
<td>SigWS X</td>
</tr>
<tr>
<td>Digital signature from Subscriber identity token</td>
<td>SigSub X</td>
</tr>
<tr>
<td>Digital signature of health plan</td>
<td>SigPlan X</td>
</tr>
</tbody>
</table>

* SC = Subscriber identity token, WS = Workstation’s Microprocessor, PL = Health Plan.
Middle columns list data in each signature. “X” is intersection of a column and row. Rightmost column is data to authenticate a patient on a claim or referral transaction.

17 Digital Signature is the private-key encryption of a hash data element derived from the data being signed. See Tutorial on Page 5.
3.0 Components Used in Patient Registration Process

3.1 PAR workstation

A stand-alone PAR workstation for this application consists of a docking station, a secure microprocessor, and a dedicated computer with communications capability such as a smart phone or tablet computer. It is conceivable that the workstation could be made from off-the-shelf products, but more likely it would be new design.

Instead of a dedicated computer it could also be an application operating on the provider’s computer so long as it meets the functional requirements below. See “Provider Options” in Part One.

The PAR workstation would have the following characteristics and functions:

- An connection for the subscriber identity token, a secure microprocessor for the workstation, and sufficient computer capacity to format, send, and receive messages to and from the health plan via cell phone or Wi-Fi networks.
- Ability to obtain accurate date and time from cell phone or Wi-Fi network.
- A printer port or an interface to the provider’s computer systems. This can be as simple as wireless printer or, in the case of home health, sending an email.
- If a PIN is to be used, then a numeric keypad or connection to a numeric keypad.
- A sensor for the one or two types of biometrics included in the standard; for example, a camera for a facial recognition photograph.
- The only essential change to provider computer systems to support a stand-alone PAR workstation would be inclusion of PAR on claim. On a Professional Claim, PAR is just another Ref code in Loop 2300. Later, referral, test order, and prescription transactions would also carry PAR reference numbers (c.f. §6.1). The REF qualifier code on external code lists will require addition to support PAR.
- An additional but optional change would be an electronic interface for the information received from the health plan to be sent to the provider systems for use in preparing a claim and other transactions automatically.

3.2 Cost of an PAR workstation and Time to Install

1) **One-Time Cost of Stand-Alone PAR workstation.** The following cost estimates are for an PAR workstation using facial recognition for biometric verification and supporting Subscriber Identity tokens.

The workstation estimated below consists of a custom-designed docking station for a smart phone that has a camera and screen, a built-in identity token reader, and a power supply that is the charging unit that comes with the phone. An included enhancement is a second screen so that the employee could see patient’s photo image and the patient could see his or her facial picture (a “selfie”) at the same time.

Note that the software for comparing facial recognition templates and for digital signatures is internal to the identity token and to the microprocessor.
<table>
<thead>
<tr>
<th>Component</th>
<th>Estimated Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Phone with Camera and wireless connection</td>
<td>$150.00</td>
</tr>
<tr>
<td>An identity token reader</td>
<td>30.00</td>
</tr>
<tr>
<td>A microprocessor</td>
<td>30.00</td>
</tr>
<tr>
<td>A second screen so both patient and employee can see facial picture</td>
<td>50.00</td>
</tr>
<tr>
<td>Custom Docking Station</td>
<td>50.00</td>
</tr>
<tr>
<td>Smart phone software application</td>
<td>50.00</td>
</tr>
<tr>
<td>Wireless printer (not necessary if office already has one)</td>
<td>120.00</td>
</tr>
<tr>
<td><strong>Total One-Time Cost for Stand-Alone PAR workstation</strong></td>
<td><strong>$480.00</strong></td>
</tr>
</tbody>
</table>

2) **Operating Cost of Stand-Alone PAR workstation.** On-going cost depends on whether the office already has a Wi-Fi network with connection to the Internet or if the workstation establishes connection to the plan via a cell phone network.

<table>
<thead>
<tr>
<th>Alternative Method of Connection</th>
<th>Monthly Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection to health plan via cell phone data-only; (e.g. I-Pad 3G)</td>
<td>$25.00 - $60.00</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Connection to already existing Wi-Fi network with Internet</td>
<td>0.00</td>
</tr>
</tbody>
</table>

This operating cost estimate does not include maintenance charges, if any, personnel time that may be needed to order occasional technical service, or other costs. Likewise, it does not estimate personnel savings other than reference to the MGMA estimates from improved accuracy and efficiency.

3) **Time to Install Stand-Alone PAR workstation.** Installation consists of unpacking a box, assigning a cell phone number to the workstation, registering it to the provider, connecting it via Wi-Fi or Blue Tooth to a wireless printer, plugging in the power supply, and positioning it on the provider’s registration desk. Estimate is one hour.

4) **Reasonableness of Cost and Time Estimates.** The point of the above estimates is not absolute accuracy but that the cost and installation time per workstation in medical practices and hospital admissions, even at multiples, would be fully acceptable.

### 3.3 Central Public Key Database

The patient registration process also requires central databases with the public keys of workstations and health plans. These may be operated by digital certificate authorities.

- Access to workstation public keys will be high volume requiring high capacity and highly reliable or duplicate central servers although health plan systems may be able to cache these keys for some reasonable time period to reduce volume.
- Public keys to subscriber identity tokens are stored at the health plan that issued the token; so a trusted public source is not required.
4.0 Only the Health Plan, its Subscriber Identity tokens, and the workstation microprocessor are Secure within the Patient Registration Environment

The direct victim of claim fraud is the health plan and indirectly the employer or other sponsor. Since claim fraud occurs and the health plan is the victim, from the plan’s perspective, only itself, the identity tokens it issues to subscribers, and workstation microprocessors can be considered secure. And since subscriber identity tokens are secure, they are a service to patients to help reduce medical identity theft and the wrongful compromise of health records.

- In the familiar uses of an identity token, the token is read in secure environments. For example, when an identity token is an access key to a building, building management controls issuance of the token and also controls reading the token to access the building. But typically in healthcare, the environment for reading the token is not controlled by the issuer of the token. That is, it is not controlled by the health plan, which is the entity at risk from fraudulent claims.

- Perhaps 80% of fraud in healthcare is perpetrated by claim submitters\(^\text{18}\), which may include false-providers (those entities that appear to a health plan to be providers but are not) and a small minority of valid healthcare providers. Claim submitters may be individuals, sole practices, or organizations.

- Because claim submitters commit such a high percent of fraud, their computers, equipment, software, and procedures must be considered compromised.

- Identity tokens and controlled-issue microprocessors have technological capabilities such as Digital Signature or Internal comparison of a PIN and Biometric, that are extraordinarily difficult to compromise, while cards with magnetic stripe, bar codes, or no technology are inherently unsecure.

- Since a health plan is the target of fraud, only the plan has significant motivation to reduce fraud. A health plan controls the manufacture\(^\text{19}\) and issuance of identification tokens; so the health plan can reasonably consider its Subscriber Identity tokens to be secure.

\(^{18}\) *Healthcare Fraud*, Sara Rosenbaum JD, Nancy Lopez JD, Scott Stifler JD, October 27, 2009; cites National Healthcare Anti-Fraud Association (NHCAA).

\(^{19}\) A health plan may contract for its Identity tokens to be manufactured and personalized by a trusted and highly secure company whose financial investment would be hugely at risk from any compromise during manufacture. A number of identity token manufacturers are certified by Visa, MasterCard, and American Express for security.
5.0 Subscriber and Patient Registration

5.1 Goals for Subscriber and Patient Identification

- **Ideal Goal: Proof that Insured Patient is Present.** The ideal goal is for the health plan to receive proof that (i) the patient is the same person as the subscriber, spouse, or dependent covered by the token, and that (ii) the patient is present at the initiating medical encounter. Biometric identification would achieve this goal, although there would be exceptions such as when the patient does not bring the token or, rare, the biometric test is a false negative.

- **Next Best Goal: Proof that Identity Token is Present.** Next best is for the health plan to receive proof that at least the Subscriber Identity token was present at the initiating medical encounter. While the token might identify a different person than the patient, or the token might have been obtained illegitimately, having at least to prove that the token itself was physically present presents a significant burden for a fraudulent claim submitter to overcome.

5.2 Use of a PIN

- A PIN is a number or code known by the patient. When the Subscriber or patient presents identification, he or she also conveys the PIN to be compared with the PIN registered on the Subscriber's identity token.

- If the registered PIN is carried on magnetic stripe or bar code, it must be machine-readable and the keys to encryption or other protection, if any, would necessarily be known to the industry. Consequently, a PIN on cards with magnetic stripe or bar code is inherently unsecure. This problem has been cited with EMV cards in Europe having both magnetic stripe and chip such that the PIN in the chip had to be different from the PIN on the magnetic stripe because the magnetic stripe was unsecure.

- If the card has no technology such that the registered PIN would be printed on the card, there would be no security of the PIN whatever.

- **The PIN Could be Compared at the Health Plan.** The registered PIN could be stored at the health plan and not be carried on a token with magnetic stripe, bar code, or any technology. The patient would enter the PIN, but it would not be tested locally. Rather, it could be sent in real-time as part of patient registration and tested by the health plan.

- **But an identity token Can Compare PIN Immediately.** If a PIN is used, the better design is for the registered PIN to be carried in an identity token, and the token performs an Internal comparison of the PIN from the patient to the PIN in the token. Differences would be detected on the spot. If caused by incorrect keying, the patient could immediately reenter it. The token will not disclose the PIN; it simply accepts the correct PIN when entered.

---

20 The preferred method is for the Subscriber to key the PIN into a workstation rather than telling the PIN to the desk person.
- **Proof that Subscriber identity token was Present.** If the entered PIN and the registered PIN are the same, the Subscriber Identity token will digitally sign that the two PINs are the same. As described below, the digital signature means that the token was present; yet the patient was not necessarily present because the token and PIN might have been obtained illegitimately. That is, an identity token PIN methodology improves the likelihood that the patient is covered by the health insurance, but does not prove it.

- **Problems.** The problems if a PIN methodology were to be adopted are left for detailed design. These include:
  
  o **Conversation-capturing.** If the conversation between the PIN workstation and token reader is not secure, it would be possible to capture the correct PIN. This method was a problem when EMV readers were fraudulently altered during manufacture.
  
  o **Trial & Error.** A way to determine a PIN would be to try different PINs repeatedly until one works. If the PIN is 4 digits, on average it would take 5,000 tries (assuming only one PIN works). Defense is for the token to count the sequential number of unsuccessful tries and terminate after a small number. The procedure for reactivation of the token is an exception issue left for detail design.
  
  o **PIN Forgotten.** Many Subscribers will forget their PINs. Although it might not be necessary to reissue tokens because of forgotten PINs, the process to advise the Subscriber of the correct PIN must be highly secure; otherwise, that process itself would be an avenue for fraud.

### 5.3 Use of a Biometric

- Biometric verification greatly strengthens positive identification because (i) it assures patient is the purported person and (ii) that the patient is present at the initiating medical encounter.

- If biometrics are supported in standards, whether one or two, the provider’s PAR workstation would need to support use of all supported types.

- Types of biometric verification might be facial recognition, voice recognition, single fingerprint, iris scan, or other biometric. For example, the Department of State, with 75 million photographs on file, uses facial recognition during visa screening. Or recently, a convicted killer who escaped from Fort Leavenworth in 1974 was located by comparing an ID photo when the man was 23 to his current Florida driver license photo when he was 63 using facial recognition. The success of Barclay’s use of voice recognition in the U.K. for high value customers resulted in expansion to all customers.

- Which biometrics might be specified in token standards is left for later design. Facial recognition, voice recognition, and single fingerprint seem the least intrusive.

- The elements are:

---

A biometric template would be registered on the Identity token. A template is not the scan image itself but a number derived from the image. For example, the token would not have a picture of a fingerprint or eye or face; rather it would carry a number calculated from the image. The number is called a template.

- The biometric template on the Identity token is called the *reference* template.
- Reference templates are also maintained in health plan files.
- When the Subscriber Identity token is connected to the PAR workstation, the patient touches a fingerprint pad or supplies a facial picture or iris scan. The sensor converts the biometric into a template. This is called the *encounter* template.
- The encounter template is sent to the Subscriber Identity token.
- The Identity token compares the encounter and reference templates, a process called Internal comparison. If the templates match, according to the token’s matching algorithm, the patient is valid.

- **But Sometimes it Doesn’t Work.** For example, the ridge patterns of the patient’s fingerprint might be insufficiently distinct. However, since the purpose is verification, not identification, the matching algorithm can be calibrated to minimize false negatives. Yet a few will occur, so there would be an exception process such as shifting to a different biometric type for that patient, or shifting to use of a PIN.

- **Initial registration** of the reference biometric template on the Subscriber Identity token is a design task. The methodology for initial registration would be influenced by choice of biometric type. For example, if facial recognition were used, the sponsor, such as an employer or licensed insurance agent, could take an electronic frontal-face picture and send it securely to the health plan for registration on the subscriber Identity token; or it might be obtained from drivers license or state ID files. The subscriber spouse’s photo could either be registered in the same way as the subscriber’s or as a dependent’s photo.

- **Dependents.** For dependents who would like to use the token without being accompanied by the subscriber, the subscriber would be present the first time, pass the biometric test, and the subscriber identity token would then register the dependent’s biometric template such that the dependent would not need the subscriber for subsequent encounters.

A health plan may issue a subscriber identity token to some dependents directly—for example, to young adults. These tokens are the same as any subscriber identity token, and registration of the dependents biometric template is done the same as for the subscriber.

- **Changing Plans.** Ideally, when a subscriber changes health plans, the reference templates and other data would be transferred automatically to the new plan.

- **Spoofing Biometric Verification.** There may be attempts to spoof the biometric sensor. For example, to spoof a fingerprint, the fraudster might make up a plastic finger with the ridges to match a person’s finger, although there are liveness tests to defend against this. Or to spoof facial recognition, the fraudster might hold a picture of the patient to the camera. The defense against a photograph at the encounter is to detect movement, not of the

---

23 A static photograph may be used to register the *reference* template initially. It is the *encounter* template used for verification that detects motion in order to detect efforts to spoof facial recognition.
photograph, but in the person’s face; for example, the camera may take several split-second photos to detect facial motion.

### 5.4 Encounter Sequence Number

- Consider the following scenario. A valid and honest Subscriber presents his or her Identity token, but the claim submitter is fraudulent. So the PAR workstation obtains a valid Digital Signature from the token to confirm that the Subscriber Identity token was present today. Then in a few seconds its dishonest software obtains, say, 10 more Digital Signatures, each with a different date. It now has 10 valid Digital Signatures for fraudulent dates to register the same patient on a different date without the patient or the identity token being present.

- The best defense for this is to have a correct date and time obtained from a trusted source. (see the date & time problem below) and to use the subscriber identity token to decrypt the PAR number from the health plan, proving the subscriber identity token was present for the full patient registration.

- The other defense is for the Subscriber Identity token to assign a sequence number every time it calculates a digital signature, and it would store the last sequence number.

- The Encounter Sequence Number is included within the Digital Signature. Say the sequence number for today’s claim is 01 and the patient presents the token again tomorrow at a different provider and its sequence is 12, the gap having been caused by the 10 signatures fraudulently obtained. The first fraudulent claim might be dated a week from now, and it would have a sequence number of 02. The health plan’s computers would immediately detect the inconsistency and flag the claim with an earlier date but later Encounter Sequence Number. This works as well for a fraudulent claim dated earlier.

- The value of the Encounter Sequence Number is in downtime registration when the date & time cannot be verified, as when the plan’s systems or connection is down.

- The marginal cost of using an Encounter Sequence Number on an identity token is zero.

### 5.5 Trusted Date and Time Using Standard Eligibility Inquiry & Response

- An identity token cannot maintain a clock. It loses power when it is disconnected. It depends on the PAR workstation to which it is connected to obtain the date and time. But the PAR workstation must be considered potentially compromised because it is controlled by the claim submitter.

- So the way the correct date and time is included in the subscriber and workstation signatures, thereby tying patient-provider-time to the specific data set, is to use the date and time from the PAR workstation, then verify it at the health plan against the plan’s own date and time. The plan only accepts the patient registration if the two times are very close, say within 15 minutes. The two times are obtained as follows:
  - The PAR workstation obtains the date & time from: (a) its smart phone if that is the workstation’s computer, or (b) from the provider’s computer or the Internet.
  - The Health Plan obtains the date and time from an Internet connection or other source.
Could the date and time be obtained from NIST using the National Time Protocol? Yes, but that does not lessen the need for the subscriber identity token to be given the date and time, and since that could be unsecure, the need for the plan to verify it.

An exception left for detailed design is the procedure during downtime when the health plan’s real-time eligibility inquiry/response, or the connection to it, is inoperative.

The process is for the Subscriber’s Identity token to sign a data set that includes (a) identification from the token, (b) the PAR workstation’s date & time, and (c) signed identification of the workstation. It requests that the health plan determine the validity of the signatures, accept the data set including date & time, and issue a PAR number encrypted using the subscriber identity token’s public key. After decryption by the subscriber identity token—proving the token is still present—the provider uses the PAR on its claim. The plan makes the following tests:

- **Is the subscriber identity token’s signature valid?** Each subscriber identity token has its own pair of public-private keys. The health plan, upon issuing the token, kept a record of its public key, and it uses that public key to validate the subscriber identity token’s signature. (Only the token knows the private key).

- **Is the date & time that is contained in the request within a reasonable range, say 15 minutes, of the actual time?** The reason the PAR workstation’s date and time must be included within the Subscriber identity token’s signed request is that otherwise the request would be constant for any given subscriber-workstation pair such that many apparently valid dates could be obtained by repeated requests.

- **Is the Workstation’s signature valid?** The plan accesses a trusted public source of workstation public keys to validate the signature.

- **The subscriber identity token must not be lost, stolen, or deactivated.** If the token is on file as lost, stolen, or deactivated, the plan rejects the patient registration request.

### 5.6 Why Date & Time are Essential

If the signed request were not to include the Date & Time, then the Subscriber’s digital signature would not prove the token was present for the patient, workstation, plan, and time. Without that proof, the purpose of the digital signature would be defeated, because without variable data elements, the data set would be constant for a given patient and workstation and therefore could be repeatedly used for any date on many fraudulent claims.

However, by including the date and time, the signature constitutes proof that the token was present at that workstation’s location and with the patient’s biometric, that the patient was present.
6.0 Other Design Elements and Issues

6.1 PAR on Referrals, Orders, Prescriptions—a Vulnerability and Solution

The initiating medical encounter, for which patient registration was completed, may give rise to subsequent encounters such as referred medical treatment, off-site laboratory, medical test, review of test, prescription, and other medical work. In many of these cases the patient and the subscriber identity token will be present so that patient registration would occur again.

However, in some cases the patient and token may not be present. In those cases, the order for the subsequent encounter should include the Patient Arrival Registration number (PAR) from the initiating encounter. A claim made for the subsequent encounter should include that PAR. Yet this introduces a vulnerability in that the PAR is just information and could be used on multiple claims involving the same patient.

The vulnerability appears principally to be from large dollar drug, controlled substance, and DME prescriptions and might be resolved by requiring presentation of the subscriber identity token for receipt. Home delivered prescriptions could use the mobile PAR workstations used for home health. Yet mail order would remain vulnerable.

Initially. Patient Arrival Registration should be implemented as described here first to realize the majority of benefit immediately.

The solution. Then later, as providers are increasingly able to order subsequent encounters electronically, the solution would be added to the Patient Registration process as follows:

- The initiating provider’s electronic order for a subsequent encounter would carry its PAR plus a Suffix.
- The initiating provider would send an electronic copy of the order to the health plan, identifying it with PAR + Suffix, and in that way alerting the plan to expect a claim for the ordered service.
- The claim for the subsequent encounter would include PAR + Suffix enabling the plan to link it with the initiating encounter.
- The claim or claims for review of test results (i.e. a claim for work subsequent to the subsequent encounter) would carry the same PAR + Suffix because the test and reading the test can be linked together by the plan.
- When the initiating and subsequent encounters are covered by different health plans (for example, when medical insurance and drug insurance are different plans), then there would be a mechanism for the subsequent encounter plan to obtain information about the initiating encounter.

6.2 Hash Data Element Calculated by Identity Token or Microprocessor

When an identity token or the workstation’s microprocessor signs a data set, the Identity token or microprocessor must calculate the Hash data element that, when encrypted with the Private key, becomes the digital signature. Since the claim submitter’s equipment and software is potentially compromised, using it to calculate the Hash would open the possibility that the signature would apply to altered data. See Tutorial on Page 5.
6.3 Identity Token does not Validate Digital Signatures

The Subscriber Identity token, upon receiving a digital signature from the workstation’s microprocessor, does not validate it. Rather, the health plan validates digital signatures. The reason is that in order for an identity token to validate digital signatures, it would require the applicable public keys. That would consume excessive time and be unsecure.

6.4 Security Requirements for a Subscriber Identity Token

Any Subscriber Identity Token must be incorruptibly secure from the perspective of the health plan, which is the primary entity at financial risk. The token must also meet the functional, practical, financial, and other requirements as described for it in this paper.

The security requirements that must be included are:

- Identifiers for the plan, subscriber, spouse, and dependents.
- Reference biometric templates for the subscriber, spouse, and dependents.
- A pair of private and public keys such that only the token knows the private key.
- Token calculates the Hash for a data stream it encrypts or signs so that an outside source cannot create a Hash for different data than the token thinks.
- Asymmetric\textsuperscript{24} Encryption using the token’s private key.
- Digital Signature using the token’s private key.
- Asymmetric Decryption using the token’s private key.
- Communication only with transactions standardized for the PAR application.
- No outside computer, reader, or person can be capable of penetrating the data, code, or keys inside the security token.

Without these security elements, it is not possible to prove the patient and provider are physically present at the same time and place, and it is that proof that is the essence of adding a security role to health identification.

What types of Identity Tokens meet all the requirements?

1. A smart card meets the security, functional, practical, and financial requirements. The card may have electrical contacts or it may work in proximity. Smart cards will be very widespread as bank cards comply with the October 15, 2015, transition deadline from magnetic stripe only to cards with magnetic stripe and microprocessor chip. Merchant terminals by the millions are currently in transition to support smart cards. Federal Agencies are directed to shift to chip cards and to use terminals that support chip cards.

2. A key fob would be capable of meeting all the requirements in that is would contain the secure microprocessor, can communicate in proximity, and is inexpensive. Some oil companies used them, but it is our understanding consumer acceptance was not stellar.

3. A smart phone Application could meet the functional, practical, and financial requirements. It meets the financial requirements assuming the subscriber supplies the phone. Some

\textsuperscript{24} Asymmetric encryption consists of symmetric encryption of the data followed by asymmetric encryption of the hash and the random key used for the symmetric encryption. See Tutorial on page 5.
subscribers would not supply the phone; so those subscribers would still require another form of secure identity token such as a smart card. The research did not investigate the methods for a smart phone Application to meet PAR security requirements.

Could PAR process be compatible with increasing use of smart phones to identify subscribers? Ideally, yes. Many plans are enabling subscribers, as an option, to use smart phones instead of insurance cards and also for other purposes. After installation of an appropriate Application, the smart phone will display insurance identification now conveyed by a health insurance card. It will display the information in matrix code for a device in the provider’s office to read, and it will also display it in readable form so that the subscriber is able to convey the information over a telephone just as he or she can do now by reading the insurance card.

In the ideal, a subscriber could have an optional Application for his or her smart phone to convey insurance information and that the same Application could also support other functions of the PAR process. So the remaining research is to understand how the Application would meet the security requirements, and assuming that effort is successful, a smart phone Application could be used as a subscriber identity token in the PAR process.

But the PAR workstation was described as using a smart phone as a computer. Is that secure? The workstation’s computer does not have to be secure. It coordinates exchange of data and manages communications. The subscriber identity token, which is secure, creates the subscriber’s digital signature, and the secure microprocessor in the workstation creates the workstation’s digital signature.


The form taken by a “identity token” is not an issue. So long as it is secure and can communicate, verify biometric identifiers, process data, encrypt and decrypt, digitally sign, and otherwise meet the requirements for this application, it may be acceptable in another form such as a keychain fob or a secure smart phone Application. Moreover, identity tokens will improve in the future.

6.6 Why Must PAR number be included on the Claim?

The question is why the Patient Arrival Registration number (PAR) that identifies successful registration is required on the resulting claim since the plan could readily link its record to an incoming claim? Because that would open a vulnerability.

The plan returns a PAR number in encrypted form; the subscriber identity token decrypts it; and the plan puts the decrypted PAR on the claim. That proves to the plan that the subscriber identity token was still inserted when the plan returned acceptance of patient registration.

Decryption of PAR (§1.0 Step 10) on the claim prevents a fraudulent claim submitter, using corrupted software, from performing the early steps of the process (Steps 1 to 6) multiple times with different future dates, then later performing the remaining steps (Steps 7 to 11) at each of the future dates and times to get valid PARs applicable for future fraudulent claims.
6.7 Exception Handling

This paper is not intended to describe procedures for exceptions. Instead, it defers analysis of exceptions until detailed design. Notes for some common exceptions are:

- **Accept Small Claims.** If the encounter is telephone consultation, such that the subscriber identity token was not validated, then the plan may elect to accept a claim so long as the claim amount is below a threshold and does not result in a large subsequent DME, drug, or similar claim.

  However, the health plan’s statistical analysis would highlight any provider with an unusually large percentage of claims that are lacking subscriber signatures and are below the threshold. So this exception is not a likely source of significant fraud.

- **Patient is Generally Present for Larger Claims.** If a telephone consultation results in a test order, say a CT Scan at a hospital or clinic, such that the amount will be above the threshold, the patient would generally be present for the test and would register at that time. Or if the telephone consultation results in an expensive prescription, even if the patient cannot be present (possibly due to illness), the subscriber identity token could still be required to obtain the prescription, especially for controlled substances.

- **Telemedicine.** With telemedicine encounters the provider and patient are physically in different locations such that the patient registration process described in this paper is inapplicable. In most cases these may be processed in the same manner as subsequent encounters inasmuch as an initiating medical encounter would generally have preceded use of telemedicine. Some such encounters will tend to be small claims as noted above. Finally, some encounters may remain exceptions not compatible with the patient registration process. It may also be possible to include, along with other telemedicine equipment, a method to employ the patient’s subscriber identity token such that it can be known that the subscriber identity token is present, although employing a biometric would likely not be practical.

- **Patient does not bring Subscriber Identity token, and the Claim Amount is Larger than the Plan’s Threshold.** This exception will occur frequently in emergency and trauma centers. If the medical condition requires treatment, then the provider would obtain insurance information on a delayed basis as it does now, and the plan may or may not require the subscriber identity token. If the patient is subsequently admitted or held for observation, it would be reasonable to require the subscriber identity token later.

  In non-emergency situations in which the claim amount is significant, the health plan may allow some exceptions but would impress on the provider the necessity for the patient to present the subscriber identity token. In time, patients would increasingly bring their Subscriber identity tokens just as they bring bank cards to a store. Moreover, the provider desires the biometric for patient matching, further encouraging the patient to bring the token.

- **Patient forgets PIN.** This will happen frequently and the vulnerability introduced by restoring the PIN is an argument against using a PIN. The procedures for when a patient
Secure Patient Identification

forgets the PIN are left for detailed design. The Provider might also be required to confirm that a second form of identification was used, but that does nothing for fraud by the claim submitter. Even without the PIN, the system described here would still give proof that the subscriber identity token was physically present.

- **False Negative on a Biometric Test, but Provider is Certain of Patient’s Identity.** Similar to a patient forgetting a PIN, the system would still give proof that the subscriber identity token was physically present, but it would not offer the biometric proof that the patient is the person purported to be insured. Statistical analysis would be able to highlight a provider or patient with an outlier percentage of this circumstance.

### 7.0 Effectiveness of Patient Registration for Different Types of Fraud

#### 7.1 Fraud against which the Patient Registration process may be effective:

1) **Mass Fraudulent Billing.** Claim submitter, typically using lists of stolen insurance information, without Subscriber collusion, makes up a fraudulent claim. This type of fraud is an example of mass billing using stolen names and insurance information.

   If the claim is for an Initiating Medical Encounter, the false provider would need to obtain a digital signature without the physical token. This is a nearly insurmountable obstacle that would dramatically reduce this major type of fraud. Because the stolen information’s usefulness has been dramatically reduced, it would have much lower value such that the incidence of its theft would be similarly reduced; so Medical Identity Theft would be reduced.

   However, the Identity Theft Resource Center (ITRC), using HHS tracking data begun in 2009, estimates tens of millions of individual health records have been mined primarily to purchase prescription drugs. Filling a prescription is a Subsequent Medical Encounter and initially is a vulnerability—with a solution§6.1—described as Fraud Type #6 below.

2) **Entire Claim is for Service Not Provided.** Valid Provider who has previously treated a given patient, but without patient collusion, submits a claim for service that was not provided such that the entire claim is fraudulent. The claim submitter must supply proof that the token and valid patient were present. To prove the token was present would minimally require access to the Subscriber Identity token, and that would be difficult, though possible25, so fraud of this type would be greatly reduced, not totally blocked. Using a biometric without patient collusion would stop nearly all instances of this type of fraud.

   However, exception procedures that allow treatment when a patient does not have his or her token opens a window for fraudulent claims that lack patient registration. These claims may be spread across a range of patients and plans such that the number to any one plan might be low and, without consolidation of the information, the plans would find detection difficult. The size of the problem might be affected by contract incentives and by how strictly or liberally plans design the exception for not proving valid patient registration.

---

25 For example, a nursing home may collect insurance cards in its health department and a person may borrow them overnight to make up fraudulent claims asserting the exception that the patient could not be present. This practice, even if spread over days or weeks, would tend to show as a statistical outlier. It can be countered if patient registration would normally be accomplished using the same approach as for home health encounters.
3) **Fraudulent Claim with Collusion.** Claim submitter, with collusion from a covered patient, makes up a fraudulent claim. The Subscriber’s collusion would enable proof the token was present, and from biometric verification, that the patient is a covered person; so a subscriber identity token will not stop this type of fraud one encounter at a time.

However, reasons this type of fraud will be reduced for schemes involving many patients and multiple encounters include: (i) involving many people in crime increases the risk of detection, (ii) patient registration must be completed for every claim, and arranging for the subscriber identity token and patients’ presence is a lot of work, (iii) proof of patient participation has deterrent value to the patient, (iv) proof of a valid registered workstation has deterrent value to the provider.

See also §7.3(12) *Fraudulent Personal Injury Claims*, which are usually liability claims and do not involve health insurance or subscriber identity tokens.

4) **Patient Borrows or Steals a Token.** Patient uses the benefit token of another person to obtain medical treatment. Biometric verification would detect this fraud. A PIN would seldom be an obstacle.

Also, the Subscriber may validly sign in, but if the employee is unobservant, or if a kiosk is used, the actual patient might be a companion, so an identity token would have done little. A defense used in hospitals and outpatient clinics is to attach a wrist band to the patient immediately during registration.

Overall, a significant portion of this fraud and identity theft will be stopped. It is thought currently to be a low percent of overall fraud except in Medicaid or similar. In the future, although there may be reduction in the number of uninsured persons who might perpetrate this fraud, non-payment of subsidized premiums and avoiding deductibles may cause it to increase.

5) **Employee Makes Up a Wholly False Claim.** A provider’s, claim administrator’s, or other employee involved in the claim process, in a trusted position to accomplish this fraud, uses a patient’s insurance information to submit or process a fraudulent claim unknown to the provider. When paid, the employee diverts (embezzles) the payment to private purposes. (See also the more difficult fraudulent claim, §7.2(9) *Valid Claim with added Fraudulent Item.*

At present, making up such a fraudulent claim, consisting of insurance information that is readily available from the provider’s files, is easy. Detection is possible, such as by audit of a direct deposit account, but defense is otherwise limited to the insured person reporting it based on the explanation of benefits notice. So if the employee chooses patients carefully, the patient is unlikely to report the fraudulent claim.

But in the design here, it would be stopped by either: (i) necessity to prove the subscriber identity token was present, or (ii) necessity of passing the patient’s biometric verification test.

6) **Fraudulent Claim from Subsequent Encounter.** A valid subsequent claim submitter submits a claim for treatment, test, or prescription that was not ordered or is for greater value (i.e. up-coded) from what the initiating physician ordered. These claims carry the PAR that
link them to the initiating medical encounter so that statistical analysis can make this fraud somewhat more difficult to commit. Initially, it continues to be a vulnerability as it is now.

But later enhancement to the Patient Registration process where the initiating provider sends electronic orders, with copies to the health plan, would substantially eliminate this type of claim fraud. (c.f. §6.1).

7) **Black Market Fraud.** Patient in collusion with a claim submitter, resells medical supplies, durable medical equipment, or other supplies. This is usually a form of subsequent encounter directed by a physician prescription and can be addressed in the same manner as §7.2(6) above.

### 7.2 Major Fraud Types where Subscriber Identity Tokens are Ineffective:

8) **Up-coding.** Valid Provider, without Subscriber collusion, up-codes one or more claim items on an otherwise valid claim. This type of fraud includes billing for treatment, say, by an MD but having the treatment performed by an assistant. Subscriber Identity tokens are ineffective against up-coding, so other methods are needed.

9) **Valid Claim with added Fraudulent Item.** Valid Provider, without Subscriber collusion, or a claim administrator, adds a fraudulent item to an otherwise valid claim. This fraud is very difficult to detect. The Subscriber Identity token digitally signed for a valid encounter. The patient is unlikely to give negative feedback about an additional claim item on the explanation of benefit report to an otherwise fair description of the encounter as he or she remembers it. And the additional item could easily appear logical and reasonable to the patient. Therefore, Subscriber Identity tokens are ineffective against this fraud type, so other methods are needed.

### 7.3 Fraud Types Unrelated to Subscriber Identity tokens:

10) **Embezzlement.** Provider's or administrator's employee or agent acting for self, submits valid claim for larger amount than what provider intended to submit such that the employee diverts—that is, embezzles—the extra amount for personal use while provider records show only the intended amount. This is embezzlement, not health insurance fraud. A Subscriber Identity token is not relevant to this type of fraud.

11) **Cash Pill Mills.** “Pill mills" are frequently cash operations not involving insurance and therefore are not claim fraud and do not involve subscriber identity tokens. Profit comes from the difference between the low retail price charged by a pharmacy versus the high street price re-selling the drug; so insurance reimbursement may not be sought because it leaves a trail.

In most cash pill mill operations, prescriptions are written by a licensed provider authorized to prescribe pills. If conducted as a cash transaction, there is currently no mechanism to track the prescriptions written by the provider.

12) **Fraudulent Personal Injury Insurance Claims.**

There may be fraudulent claims for medical treatment that are not health insurance related and therefore will not involve Subscriber Identity tokens. These claims may be submitted under liability provisions to property and casualty insurers and may be supported by official
accident reports. The medical treatment may or may not be necessary, may or may not have occurred, may have been performed by unlicensed persons, and may have been up-coded. Also, there may be no provider-insurer pricing contract so that the retail claim amounts would be high for any given medical treatment.

But this paper deals with using identity tokens that identify subscribers to health insurance; so it is inapplicable to fraudulent personal injury insurance claims that are filed directly with non-health insurers since these claims do not involve subscriber identity tokens.

To the extent that injured persons have health insurance, it may be effective to require submission of medical claims first to that insurer for subrogation to the liability firm, and that process may bring costs within contract pricing and may offer fraud defenses. This issue is not otherwise explored in this paper.

7.4 Amount of Claim Fraud in Healthcare

The Institute of Medicine reported a lower-bound estimate of total fraud in U.S. healthcare to be $75 Billion per year\textsuperscript{26}, a number it found to be largely substantiated by other studies using differing methodologies. By \textit{lower-bound} it meant the lowest amount from reasonable estimation. $75 Billion is about 3\% of total expenditures of $2.27 Trillion\textsuperscript{27} per year. But the median estimated fraud by industry for all industries is over 5\%\textsuperscript{28} based on audit sampling. This suggests 3\% for the health industry is low; if it were 5\%, total fraud would be about $113 Billion per year.

Dr. Rosenbaum, et.al.\textsuperscript{29} estimate that about 80\% of healthcare Fraud is committed by claim submitters, and that about 20\% of Fraud is committed by patients, plans and payers, and miscellaneous other entities or persons. This paper concerns fraud committed by claim submitters and patients; so it uses a lower bound estimate of $65 Billion total per year by claim submitters and patients, ascribing $60 Billion of it to claim submitters. When there is collusion between claim submitter and patient, this paper ascribes it to the claim submitter.

Yet there are no definitive calculations of the amount of Healthcare Claim Fraud in the U.S.. The only effective way to estimate undetected fraud is a time-consuming process requiring statistically valid samples of claims, legal access to records, and teams of auditors to research each claim from primary sources. Even at that, significant instances of fraud could be overlooked, and pilot tests will cause shifts in fraud type and location. Such measurement of U.S. healthcare fraud has not been done in sufficient scale to be definitive. So necessarily, this paper uses estimates of limited accuracy. The authors genuinely welcome better data.

\textsuperscript{26} \textit{The Healthcare Imperative: Lowering Costs and Improving Outcomes}, Institute of Medicine, 2012.


\textsuperscript{28} \textit{Countering Fraud for Competitive Advantage: The Professional Approach to Reducing the Last Great Hidden Cost}, Mark Button, Jim Gee, Wiley, 2013, Chapter 5. Large studies across different industries indicate an average fraud loss rate above 5\% with significant variation by industry; pp.16-17. [Contrast 5+\% all-industry average to the lower 3\% used in this paper.]

\textsuperscript{29} \textit{Healthcare Fraud}, Sara Rosenbaum JD, Nancy Lopez JD, Scott Stifler JD, October 27, 2009, report to National Healthcare Anti-Fraud Association (NHCAA).
7.5 So How Much Claim Fraud might the Process in this Paper Save?

Just as the $65 Billion per year estimate is tentative, it is not known how the $65 Billion is distributed among different types of fraud. Assuming the subscriber identity token requires a biometric such as facial recognition, then a summary of the effectiveness of the Patient Arrival Registration process for fraud types described in §7.1 and §7.2 above might be as follows:

<table>
<thead>
<tr>
<th>Type of Fraud</th>
<th>Amount of Loss</th>
<th>Effectiveness of Patient Registration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Mass Fraudulent Billing</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>2 Entire Claim is for Service Not Provided without Patient Collusion</td>
<td>Med</td>
<td>High</td>
</tr>
<tr>
<td>3 Fraudulent Claim with Patient Collusion</td>
<td>Med</td>
<td>Med</td>
</tr>
<tr>
<td>4 Patient Borrows a Token</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>5 Employee Makes Up a Wholly False Claim</td>
<td>Med</td>
<td>High</td>
</tr>
<tr>
<td>6 Fraudulent Claim from Subsequent Encounter (after electronic advice of order for subsequent treatment is implemented).</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>7 Black Market Fraud (after electronic advice of order for subsequent treatment is implemented).</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>8 Upcoding</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>9 Valid Claim with Added Fraudulent Item without Patient Collusion</td>
<td>High</td>
<td>Low</td>
</tr>
</tbody>
</table>

Potential reduction in fraud from the Patient Registration process described in this paper would appear to be very substantial but less than half the $65 Billion per year. It suggests potential savings may be in the range of $20-$25 Billion per year\textsuperscript{30}, or about 1% of total expenditures. That is, the average plan may save about 1% of annual claims paid. Some plans, such as Medicare and Medicaid, may save more; some, such as VA and commercial plans, may save less than 1%.

7.6 Other Issues

1) **Legitimate Error.** Claims may be incorrect due to unintentional error. Such errors are not fraud. In fact, the amounts in error could go in either direction.

2) **Differing Judgment.** There is significant professional judgment inherent in diagnosis, treatment, and coding of claim items. Differing judgments honestly reached are not fraud.

3) **Need for Metrics to Determine Success of Fraud Prevention.** Proposed legislation directs Medicare to establish metrics by which it is to report on the success of the pilot. The metrics will be difficult. For example, upon introduction of identity tokens in a test area—an event that will quickly become known in the market—fraud will decline because fraudulent claim submitters will move out of pilot areas, distorting test metrics.

\textsuperscript{30} Put in perspective, fraud savings estimated here would be 4 to 5 times annual U.S. government investment in, for example, energy research and development: President’s Council of Advisors, *Accelerating the Pace of Change in Energy Technologies through an Integrated Federal Energy Policy*, pp 13-15.
Current estimates of fraud are mostly judgmental extrapolation from detected fraud, and that’s not a metric. Instead, metrics before and after will require determination of fraud amounts using laborious methodology described in the last paragraph of §7.4.

One of the bills would give Medicare the power to audit, and that is essential not only for measurement but for investigation of suspicious claims.

4) **Other Tests During Pilots Programs.** In addition to measuring success of the pilot programs in meeting objectives, Alpha tests and pilot programs offer opportunity to ensure the integrity of the process. See “Summary of Questions for Design and Testing” at the end of Part One.

5) **Shift in Types of Fraud.** Patient Arrival Registration is effective against certain types of fraud. There will be reduction in those types, but it is reasonable that a perpetrator who is blocked in one type of fraud may shift to some extent to another type within healthcare or to fraud in another industry. Going the other way, it is also reasonable that deterrence in certain types may cause reduction of healthcare fraud in other types as well.

### 8.0 What would Implementation Require?

The process in this paper reduces medical identity theft, enhances privacy, reduces the value of stolen information, and combats claim fraud by documenting proof that the Subscriber Identity token and valid patient were present at the initiating medical encounter. The process also gives opportunity for deterministic patient matching in Master Patient Indexes and Health Data Exchanges. The modifications to systems, procedures, and infrastructure would be:

<table>
<thead>
<tr>
<th>Development Category</th>
<th>Development Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Health Card Standards:</strong> changes to each of following:</td>
<td>Add Identity token technology such as private-public key encryption, digital signature, and comparison of PIN and biometric.</td>
</tr>
<tr>
<td>- ANSI INCITS 284:2011 and any of the affected ISO or other standards referenced by INCITS 284.</td>
<td>Data and storage fields for full data set the Subscriber Identity token digitally signs.</td>
</tr>
<tr>
<td>- WEDI Health ID Card Implementation Guide</td>
<td>Program logic</td>
</tr>
<tr>
<td>- NCPDP Health ID Card Implementation Guide</td>
<td>- to register dependent’s biometric template on token.</td>
</tr>
<tr>
<td>Substantially the same specs are needed for the workstation’s microprocessor</td>
<td>- to perform internal comparison of PIN and biometrics.</td>
</tr>
<tr>
<td></td>
<td>- to send and receive data to the PAR workstation.</td>
</tr>
<tr>
<td></td>
<td>- to sign the full data set, including digital signatures from the workstation including identification and date &amp; time.</td>
</tr>
<tr>
<td></td>
<td>- Programming and testing of the new specifications</td>
</tr>
<tr>
<td><strong>Specifications for a Smart Phone Application</strong></td>
<td>Program logic to perform the functions of the Smart Phone Application in place of Subscriber Smart Card.</td>
</tr>
<tr>
<td><strong>Manufacture, Personalization, and Issuance to Subscribers</strong></td>
<td>Secure manufacture</td>
</tr>
<tr>
<td></td>
<td>Secure personalization, including Subscriber reference biometric template.</td>
</tr>
<tr>
<td></td>
<td>Secure issuance to Subscriber, separate communication of</td>
</tr>
<tr>
<td>Development Category</td>
<td>Development Details</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Modify HIPAA & NCPDP Transaction Standards and Implementation Guides | PIN and activation code.  
- Eligibility Inquiry / Response (add Patient Registration Reference Number, full data set, and signatures from subscriber and Workstation, and in Eligibility response add plan’s signature).  
- Healthcare Claims (add Patient Registration Reference Number)  
- Referral (add Patient Registration Reference Number)  
- Test Orders (add Patient Registration Reference Number)  
- Prescription (add Patient Registration Reference Number) |
| New Transaction Standards                                | • None                                                                                                                                                                                                                |
| Other Standards                                          | • Agree standard calculations of Hash data elements, encryption, decryption, and other functions such that the computations performed by Identity tokens and by various computers with various data storage formats always yield the same result. |
| New Infrastructure Systems                               | • Trust infrastructure for workstation microprocessor keys.                                                                                                                                                            |
| Modify Health Plan, Payer, and Administrator Systems; e.g. Medicare Parts A, B, D, and Advantage Plans. Also other plans such as Medicaid, VA, private plans if they implement the process. | • Perform the processes described in this paper for Subscriber Identity token usage.  
• New PIN and Biometric Management System if used by the Plan.  
• Modification to claim and other systems for communications, storage, reporting, exception processing related to the additional data and digital signatures.  
• Logic to ascertain that the digital signatures of Subscriber Identity token (SigS) and Workstation (SigWS) are valid and consistent with the data set submitted with a claim or other transaction.  
• New logic to process exceptions such as patient did not present a token, PIN or biometric did not test positive although provider is certain of the patient’s identity, and such other exceptions as will be identified during detailed design.  
• Analytical and statistical systems enhanced to use the new information created by the processes described in this paper.  
• Ability to include incident reports, such as an unacceptable Date & Time and invalid signatures, and to merge this information into the plan’s analytical and statistical systems.  
• Modification or new procedures relevant to the new processes  
• Training of operating, client service, and manager personnel. |
<p>| Provider Systems. Method described in this paper would include medical practices, | • Perform the clerical procedures described in this paper to use the PAR workstation for Subscriber Identity token usage.                                                                                           |</p>
<table>
<thead>
<tr>
<th>Development Category</th>
<th>Development Details</th>
</tr>
</thead>
</table>
| hospitals, clinics, labs, and other providers and provider agents such as billing firms. | • Modification or new procedures relevant to Patient Registration Reference Number.  
• Training of personnel. |

### 9.0 AUTHOR GROUP

#### 9.1 Disclaimer
 Participation in the Author Group to write, review, comment, or revise this research paper does not imply endorsement by the individuals or organizations.

#### 9.2 Contributors to Writing or Editing this Report

<table>
<thead>
<tr>
<th>Person</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peter Barry*</td>
<td>Peter T Barry Company</td>
</tr>
<tr>
<td>Alan Gardner*</td>
<td>RxResults, LLC</td>
</tr>
<tr>
<td>Ken Masslon*</td>
<td>UnitedHealth Group</td>
</tr>
<tr>
<td>David Batchelor</td>
<td>LifeMedID, Inc, CEO; Board of Directors Smart Card Alliance</td>
</tr>
<tr>
<td>Gloria Davis</td>
<td>Nextgen Healthcare, EDI Development Coordinator</td>
</tr>
<tr>
<td>Chuck Erickson</td>
<td>Kaiser Permanente, Business Systems Manager</td>
</tr>
<tr>
<td>Walter Hamilton</td>
<td>Intl Biometrics &amp; Identification Assoc, Vice Chairman</td>
</tr>
<tr>
<td>Mitchell Hansen</td>
<td>MediSmart, OTI America Inc., VP Business Development</td>
</tr>
<tr>
<td>Sandra Jamison</td>
<td>Humana, Provider Process Consultant, Integration Dept.</td>
</tr>
<tr>
<td>Michael P. Magrath</td>
<td>Smart Card Alliance Health &amp; Human Services, Chairman</td>
</tr>
<tr>
<td>Michael L. Nelson</td>
<td>Equifax Identity &amp; Fraud Solutions, VP Strategy &amp; Bus Devel</td>
</tr>
<tr>
<td>Joan Robinson</td>
<td>BlueCross BlueShield Association, Project Manager</td>
</tr>
<tr>
<td>Megan Murphy Ryan</td>
<td>Aetna Inc, Senior Project Manager</td>
</tr>
<tr>
<td>Robert M. Tennant</td>
<td>Medical Group Management Association, Sr. Policy Advisor</td>
</tr>
<tr>
<td>Randy Vanderhoof</td>
<td>Smart Card Alliance, Exec Director; EMV Migration, Director</td>
</tr>
</tbody>
</table>

* CoChairs WEDI Health ID Card Subworkgroup
Attachment A
Description of Proposed Legislation

At the time of writing this paper, there are three bills pending in Congress:

- **SB 612**
  - Medicare Cards:
    - SSN Replaced, new ID
    - SSN not printed or stored
    - New Beneficiary ID
  - Purpose: Anti ID Theft

- **HR 2828**
  - Medicare Cards:
    - Pilot Smart Card Program
    - SSN Replaced, new ID
    - SSN not printed or stored
    - New Beneficiary ID
  - Fraud Penalties Doubled
  - Audit Power
  - Purpose: Anti Fraud

- **HR 3024**
  - Medicare Cards:
    - Pilot Smart Card Program
    - SSN Still Used for ID
    - SSN Not Displayed
    - SSN Stored on Chip
  - Purpose: Use Smart Cards:
    - Reduce waste, fraud, abuse
    - Reduce Identity Theft
    - Quality of Care
    - Accuracy, Efficiency
    - Evaluate patient matching


1. It applies to Medicare, not to any other government or private health plan. However, if it proves successful for Medicare, a reasonable inference is that it might be extended by law or practice to other health plans. Therefore, card standards would need modification.

2. It directs a pilot program for Medicare to issue smart cards—defined only as cards with integrated circuit (microprocessor computer chip) embedded in each card—to Medicare Beneficiaries and Medicare Providers. The pilot is to operate in five areas of the U.S.

3. It directs Medicare to establish metrics by which it is to report on the success of the pilot.

4. If the pilot is successful, Medicare is to take the program nationwide.

5. H.R. 3024 has no provision for audit as does H.R. 2828. Audit power is essential.

6. Unlike the other two bills, H.R. 3024 envisions continued use of a Social Security Number as the base identifier of a beneficiary. It would not print the beneficiary identifier on the card but encode it inside the chip. But SSN would then still be used in all records and claims.

7. H.R. 3024 lists benefits to accrue from passage of the bill and its implementation:
   a. As this paper describes, using Subscriber smart cards could significantly deter and reduce certain fraud types, reduce medical identity theft, and help protect health records.
   b. Current health card standards with magnetic stripe or bar code would equally achieve accuracy and efficiency. MGMA estimates $2.2 Billion per year potential savings for medical practices and hospitals due to accuracy and efficiency from magnetic stripe, bar code, or smart card technology. [MGMA 2009]
   c. See Attachment B on how to achieve Deterministic Patient Matching.
   d. This paper does not address the quality of care benefits cited in the bill except as to patient safety and reduction in redundant tests as a result of improved integrity of matched patient records.

---

31 Biometric verification is required in the bill for provider identity tokens and optional for subscriber identity tokens.

32 The tradeoff of the beneficiary’s identifier not being readable on the card is that the beneficiary would be prevented from conveying it to a provider over the telephone, a routine and efficient practice. And it might be of little value because SSN would still used in the beneficiary identifier, and SSN would still be in files, included in claims, and otherwise visible. [c.f. *Removing SSN from Medicare Cards*, Peter Barry, September 9, 2013].
Attachment B

Deterministic Patient Matching into Provider & Exchange Systems

“Start with a Simple, Inexpensive, Practical System and Build Upon It Over Time”

Section §1.5 describes the principle of starting with a simple system that works and then building upon it one phase at a time toward greater functionality and more comprehensiveness. Real-time Patient Arrival Registration is the simple system in §1.5 upon which the industry can build. Three development and implementation phases include the following:

1. Real-time Patient Arrival Registration with Subscriber Identity tokens—the subject of this paper.
2. Use of PAR + Suffix on Electronic Referrals, Orders, Prescriptions, and their claims. [§6.1]
3. Integration of Patient Arrival Registration with Provider Systems for the purpose of Deterministic Patient Matching. The remainder of this Attachment B describes this third phase.

Data Integrity and Matching of Patient Records in Provider Systems

1. Statement of the Problem

Patient records in a health organization necessarily contain data errors, patient mismatches, and unmatched patient records due in significant part to difficult patient identification methods. The error rate may be 10% to 15% of patient record sets. It is inefficient, inaccurate, potentially dangerous, and costly.

But positive patient identity enables deterministic solutions and directly improves administrative efficiencies, validates patient identity, reduces fraud, misidentification, billing errors, and eliminates duplicate records. Positive patient identity especially improves Health Information Exchanges as they have difficulty in exchanging patient record information if there are duplicate or overlaid records and misidentification—it’s hard to exchange records if you are unsure which duplicate record information to exchange.

2. Current Trends

Healthcare is adopting proprietary deterministic identity solutions using ID cards with biometrics in combination with probabilistic processes. Because probabilistic identity solutions still have an unacceptable margin of error within the healthcare industry, adding deterministic ID tokens brings the error rate toward zero. Non-standard Identity Token technology has already been adopted by over 250 hospitals, plus affiliated clinics and physician groups, and by some data exchanges. Annual savings for a large provider are millions of dollars.

A fourth phase is currently less defined but probable. The second paper, “Provider Identity tokens”, is anticipated to describe further anti-fraud enhancements. There may be other phases over time.
3. Need for Labor and Systems for Data Integrity and Matching Patient Records

A health organization and its affiliates will usually operate multiple systems. Each system includes some of the same patient information thereby challenging a fundamental law of data integrity that if you maintain the same data in two places then, over time, both will get it wrong. A given patient may be registered in the same system more than once due to typographical, spelling, transposition, alias names, address changes, or other factors affecting identification. The records for a given patient in one system may not be linked to same patient in another system.

Worse, patient safety is threatened when two different patients get linked as one. This contaminates the personal health records of both patients and potentially could lead to misdiagnosis or treatment based on erroneous health information.

4. Probabilistic Patient Matching

A health enterprise includes all its disparate systems and data from multiple subsidiaries and affiliates, and it must match a patient to his or her records in any of the different systems while ensuring data for the patient is consistent and correct across the systems.

a. Enterprise Master Patient Index (EMPI). The EMPI system will create a unique identifier for each patient and cross-index that identifier to each of the other systems.

b. The Match Engine. Most health enterprises use a probabilistic approach to matching patient records using such information as name, date of birth, gender, Social Security Number, Address, insurance identification, and other information. For example, “Sherry Turnbuckle” in one system, and “Sherri Turnbuckle” in another, with the same the birthdates, are likely the same. But if the last name is “Smith”, the odds are lower, and so forth. Probabilistic matching can never be 100%. Probabilistic matching would still be necessary to match old records to new and match encounters when patient registration is not done\(^3^4\).

5. Solution: Use Patient Arrival Registration for Deterministic Patient Matching

Originally HIPAA specified a unique national patient identifier. That would have aided definitive matching of patient records. But the HIPAA patient identifier was halted. Besides, a national identifier would not prevent borrowed ID from contaminating patient health records.

Another approach is to employ an “Identity Token” (sometimes called a security token). The question would then be what is the best identity token for this application. For patient matching, it would be anything physically present that identifies the patient, or more securely, by verifying the patient’s identity with a biometric. Sounds like the Subscriber Identity token.

The Patient Arrival Registration process verifies the patient with a biometric. By sending the patient’s encounter biometric template along with patient and insurance identification to the EMPI system, the match engine would definitively match the patient to existing records. Deterministic patient matching would significantly reduce errors and costs.

\(^3^4\) An additional alternative might involve a “Big Data” firm, operating with more information than available to the provider or health information exchange, to match patient records. This is still a probabilistic method.