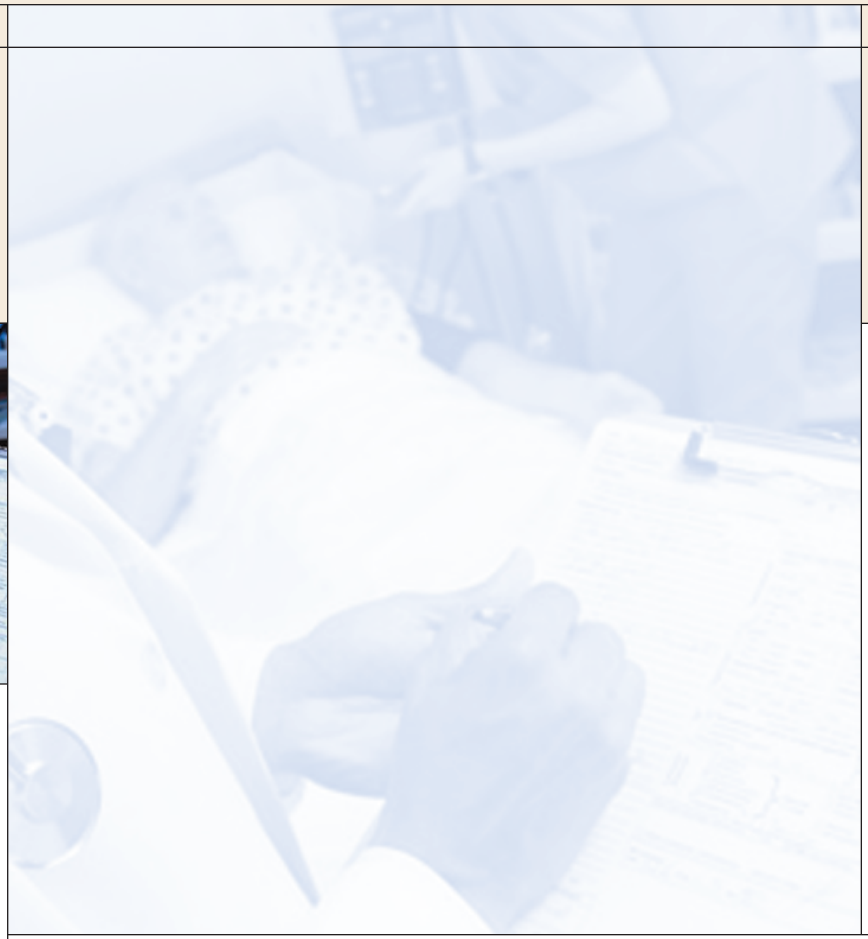
APPLICATIONS

A WHITE PAPER SERIES

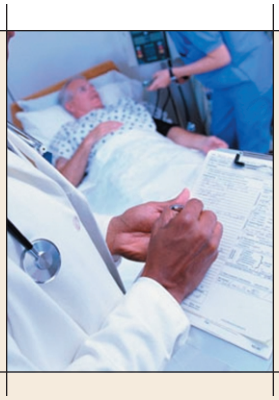
SYNTEL, A U.S.-BASED IT SERVICE PROVIDER WITH AN EXTENSIVE GLOBAL DELIVERY SERVICE, SUGGESTS SPECIFIC BEST PRACTICES FOR REDUCING COSTS AND IMPROVING BUSINESS PERFORMANCE GLEANED FROM HUNDREDS OF APPLICATION MANAGEMENT ENGAGEMENTS AMONG GLOBAL 2000 COMPANIES.

SSN Remediation Approaches for Healthcare Organizations



SYNTEL

Consider IT Done®



SSN Remediation Approaches for Healthcare Organizations

With the growing threat of identity theft and the passage of a number of federal and state regulations (including HIPAA) aimed at protecting the privacy of individuals, healthcare organizations are facing tremendous pressures to address the use of Social Security Numbers (SSNs) as patient identifiers. This has led to proposals for an alternate Universal Healthcare Identifier (UHID) to be used in place of SSNs throughout healthcare organizations, including within their back-office business applications

Because of the serious implications of failing to protect patients' privacy, healthcare organizations need to act now to address this issue. Drawing upon its vast experience providing healthcare industry solutions, Syntel has developed SSN Remediation options and can help organizations customize and implement an approach that best suits their requirements. By leveraging Syntel's healthcare industry and IT expertise, healthcare organizations can not only address these legislative requirements—they can realize ROI and evolve their infrastructure to support the business agility and efficiency they need to compete effectively.

"The Social Security Number (SSN) has a unique status as a privacy risk. No other form of personal identification plays such a significant role in linking records that contain sensitive information that individuals generally wish to keep confidential".[1]

— Mark Rotenberg, Executive Director, Electronic Privacy Information Center

1. INTRODUCTION

Most US healthcare industry databases that contain private information about individuals are designed assuming the Social Security Number (SSN) offers a number of qualities that make it useful as a database key, namely the fact that it is a unique identifier, universal, and secure. In fact, because it is so widely used, the SSN by nature cannot be considered secure. With SSNs appearing on a range of records, from intake forms to medical bills, and within all related medical databases, these numbers can easily slip into the wrong hands. The widespread public exposure of SSNs has greatly contributed to increasing incidents of financial and criminal identity theft, with identity theft being the number one form of consumer fraud. In 2003, 42 percent of all complaints received by the Federal Trade Commission were related to identity theft.[2]

Threats to privacy within healthcare organizations

Medical records may contain personal information related to family relationships, sexual behavior, and substance abuse issues. A number of parties—including insurance and drug companies, employers, employees, and courts—have access to these records. A lack of consistent privacy protection may result in unauthorized or unintended access to this information. Furthermore, there is a push within the healthcare industry to create a national medical records data bank, which could create a centralized and easy target for identity thieves. The victim of identity theft may be denied loans, admission to educational institutions, employment. He or she may experience difficulty securing health and life insurance coverage at a reasonable rate, or securing it at all. Ultimately, the greatest impact may be the loss of dignity and autonomy suffered by this person as the individual spends years and significant sums of money to clear his or her name and credit record.

Regulations to protect privacy

Over the years, the federal government has implemented a variety of regulations to address protecting the privacy of individuals, many of which are closely linked to the use of SSNs (e.g., 1996 HIPAA Privacy and Security Laws and the 1998 Identity Theft and Assumption Deterrence Act). More recently, many state governments have recognized the need to reduce the risks associated with the disclosure and misuse of SSNs by taking measures to limit their use and display. In fact, California Law SB168 specifies how and when SSNs may be used by businesses.[3]

2. ADDRESSING COMPLIANCY

Clearly, healthcare organizations (HCOs) must comply with federal and state legal protections aimed at protecting the privacy rights of patients and stopping identity theft. Some HCOs have already instituted plans to ensure compliance. For instance, the Blue Cross Blue Shield Association has mandated that no Blue Plan shall display a member's SSN on the member ID card; all Blue Cross Blue Shield organizations must be compliant by January 1, 2006.

Those HCOs that do not take measures to protect the privacy of their members' identity and medical records risk the loss of consumer confidence and ultimately, business. Consider IBM's request in early 2003 that all 150 of its health insurance providers stop using SSNs as an identifier. IBM warned these companies that it would take compliance with the request into consideration during the annual renewal process.[4]

Recommended best practices

The California Department of Consumer Affairs has developed a comprehensive set of recommended practices for protecting the confidentiality of SSNs. In summary, the recommendations are as follows:

- **Reduce the collection of SSNs**
- **Inform individuals of the intended use when collecting SSNs, and the consequences of not providing it**
- **Eliminate the public display of SSNs**
- **Control access to SSNs by only allowing access when necessary**
- **Protect SSNs with security safeguards**
- **Ensure your organization is accountable for protecting SSNs by providing training and conducting risk assessments and audits**[5]

Beyond implementing these best practices, Syntel recommends that healthcare organizations implement:

- **An alternative to the SSN as an unique individual identifier**
- **Remediation steps as concerns affected business applications and computer systems**

Targeting the Healthcare Industry

"The fact that HIPAA privacy and security standards are seen as a challenge to some hackers makes the healthcare industry a target…This was precisely the nature of the hack at the University of Washington Medical Center in Seattle in December 2000. A hacker… allegedly gained access to the medical center's network through the affiliated university network and was able to steal 4,000 patient records containing PHI, including patients' dates of birth, Social Security numbers, height and weight and recent medical procedures." [6]

SSN Security Concerns Extend Beyond Healthcare

Beyond protecting the rights of patients, organizations must keep in mind the far-reaching implications of preventing SSNs from being used by anyone other than its owner. "In today's world in which terrorism is a real concern, the SSN is a valuable commodity for criminals at all levels, as it allows individuals to integrate themselves into our society with relative anonymity and commit crimes or acts of terrorism, while avoiding detection".[7]

Advances in database technology

Due to the massive amounts of existing electronic medical records, HCOs must contend with the technological issues surrounding SSN remediation. Fortunately, HCOs can take advantage of the fact that today's database technology enables the use of alternate means of identifying individuals. Healthcare providers and related entities can now conduct searches on multiple identifiers in a timely manner without bogging down system resources. This capability paves the way for establishing a unique health identifier to replace the use of the SSN as the patient identifier.

3.

UNIQUE HEALTHCARE IDENTIFIER: ALTERNATIVE TO SSN

HIPAA's administrative simplification provisions include a requirement that the Secretary of Health and Human Services (HHS) adopt a standard unique health identifier for all related constituents in the health care system[8]. However the Department of Health and Human Services has yet to publish a standard, and while a variety of proposals for a Unique Health Identifier (UHID) have been published by various organization, none have been adopted as a standard. In fact, a universal standard may never be adopted; instead, individual organizations may need to define their own UHIDs.

Evaluating UHID candidates

The American Society for Testing and Materials (ASTM), a standards development organization accredited by the American National Standards Institute, has published the *Standard Guide for Properties of a Universal Healthcare Identifier (UHID)*, which provides 30 criteria for evaluating any proposed UHID. The 30 criteria are designed to support the following four basic functions of a unique healthcare identifier:

1. **Positive identification of patients when clinical care is rendered.**
2. **Automated linkage of various computer-based records on the same patient for the creation of lifelong electronic healthcare files.**
3. **Provision of a mechanism to support data security for the protection of privileged clinical information.**
4. **Use of technology for patient records handling to keep healthcare operating costs at a minimum.**[9]

While these criteria are worthy of consideration, ultimately, the selection of an UHID format may be dictated by off-the-shelf tools that HCOs utilize to implement an SSN remediation initiative.

4.

SSN REMEDIATION APPROACHES AND SOLUTIONS

Completely replacing the SSN as an unique patient identifier within healthcare organizations is not a practical option because healthcare organizations will need to reference it when conducting such tasks as running credit checks or verifying a patient's identity over the phone. Furthermore, due to the sheer volume of existing records that contain SSNs as identifiers, organizations will need to keep these in place in order to link old and new IDs and records.

When assessing which technology applications need remediating in order to protect patients' privacy, HCOs should take a methodical approach. (See Figure 1.)

Syntel recommends two alternatives to the use of the SSN as a patient identifier. Regardless of which approach is chosen, each option requires that organizations generate a new UHID and map existing SSNs to this new UHID. The resulting "SSN-UHID" number will be translated as needed to properly populate and interact with various applications (e.g., claims processing and ID card printing) throughout the organization.

With a UHID strategy in place, the next step is to integrate it into UHID Generation methods.

Approach one: Map and Swap

The first and most desirable approach is to use the SSN as one of many attributes associated with the patient to generate the UHID, in which case the SSN would only be referenced internally to ensure the integrity of a patient's records. For all computer processing related to a patient's records and account, the UHID would be used and only this identifier would be visible on any external documents, records, Web sites, etc. The SSN would be swapped with the UHID for almost all transactions permanently, and except in some situations, a cross-reference between the SSN and UHID may not have to be maintained at all.

STEP 1

First, identify compliance issues and timeframe(s) applicable to the organization's setting(s). While all organizations must comply with federally-mandated regulations, additional regulations vary by state and by healthcare entity.

STEP 2

Second, identify the impacted entities throughout the organization—this extends to policies, processes, and employees (including contractors); computer systems; and customers, providers, and vendors.

STEP 3

Third, once the compliancy issues and timeframes have been mapped to the various entities, it is time to establish a new UHID format, as well as rules for cross-referencing the UHID and SSN. Organizations will benefit from referring to the criteria published by the ASTM standard guide in choosing a new UHID format.

STEP 4

Finally, HCOs will need to evaluate and select the solution approach that is most appropriate for their environment and situation.

Figure 1. Implementing Remediation Steps: SSN Remediation Timeline

UHID generation methods

There are essentially two options for generating a UHID. Generate a random number for each patient or custom design a fuzzy logic with parameters such as Last Name, DOB, etc., to generate the UHID. Regardless of how the UHID is generated, healthcare organizations should keep some related issues in mind. Groups may ask insurers to use custom and/or group-generated IDs to replace SSNs as patient identifiers. Down the line, state or federal mandates may require organizations to use an UHID completely different in size and structure to the one an organization chooses today. Mergers and Acquisitions will pose unique challenges in merging subscriber databases and ensuring consistency between unique identifiers. Finally, privacy of the alternate identifiers is no less important. Care must be taken to ensure that, if the number is accessed by an unauthorized person, related personal and private information will not be easily accessible. Again, the selection of an UHID format may be dictated by the off-the-shelf tools used to generate the UHID. Due to these issues, HCOs may want to choose a solution that offers them the most flexibility to handle these future scenarios and that provides the best mechanism for protecting patient privacy, regardless of which ID is used.

Because the SSN would not be used for processing, little chance exists that HCOs would expose it and violate patient privacy rights. This fact alone makes the Map and Swap approach a highly desirable option that the entire healthcare industry would benefit from. However, in the interim, there will be situations in which the SSN will have to be used so organizations must plan to gradually move towards this model.

While a desirable option, healthcare organizations need to recognize the following implications of the Map and Swap approach. First, the technological impact will be significant. Since the UHID will likely be alphanumeric and may have a length of nine or more characters, healthcare organizations' computer systems will require extensive changes (e.g., database field reprogramming). Second, due to the number of systems impacted (see Figure 2), this approach will result in long testing cycles and consequently, long project cycles. Third, the significant system impact and long project cycles will make this the more costly of the two approaches. (See Figure 3.)

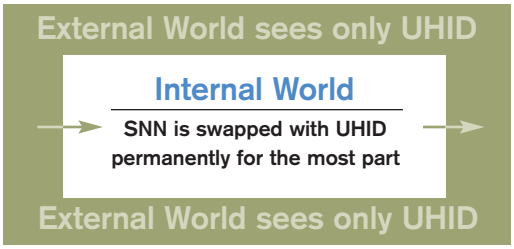


Figure 3. In the Map and Swap approach, the SSN is not visible to the public.

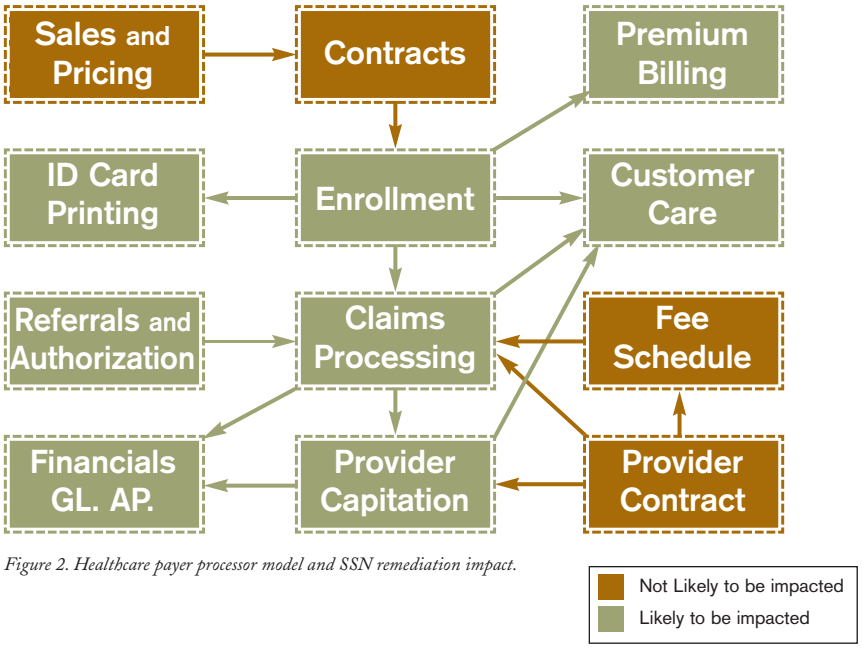


Figure 2. Healthcare payer processor model and SSN remediation impact.

Approach two: Map and Wrap

In the Map and Wrap approach, the SSN will continue to be used most of the time for internal processing; the UHID will only replace the SSN for external communications. Because of this, only those systems that relate to external communications will need to be modified to accommodate translating the SSN to the UHID or vice versa. With less impact on systems across the organization, this solution requires less testing and thus can be implemented more quickly and inexpensively.

At the same time, because the SSN will still be widely used across systems, the possibility of exposing the SSN on some form of communication (and thus violating the patient's privacy) will still exist. Since the translation of the SSN to UHID or vice versa will need to be introduced at appropriate times during business processes (which will likely change over time), maintaining these routines will become an on-going part of system administration and maintenance.

In this approach, care must be taken to ensure that HCO representatives never divulge or ask for the SSN in an unsecured communication and thereby compromise the patient's privacy. (See Figure 4.)

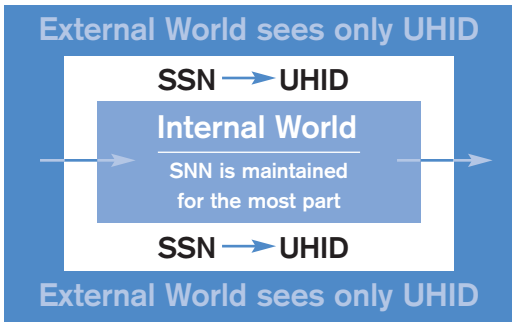


Figure 4. In the Map and Wrap approach, the SSN could possibly be exposed.

* These product names, marks, logos, and symbols are trademarks of their respective owners.

UHID generation tools

As HCOs evaluate the best way to implement an SSN remediation project, the decision will largely hinge on the sophistication required to generate the UHID. For instance, will a new UHID be generated and will a cross-reference with the SSN need to be maintained (as in Syntel's Map and Swap approach)? Or will there be an on-going requirement to translate between the SSN and UHID (as in Syntel's Map and Wrap approach)? Depending on the chosen approach and the organization's unique requirements, healthcare organizations will also want to consider the relative importance of other features, such as a matching algorithm capability to accurately and quickly compare and link data from different sources.

Out-of-box Enterprise Master Person Index solutions

The Enterprise Master Person Index (EMPI) is a solution that supports the creation of a unique identifier and cross-references the various patient identifiers from multiple systems throughout the enterprise. As opposed to the facility-centric view provided by the traditional Master Person Index (MPI), the EMPI provides an individual-focused view of patient activity across the organization. Several out-of-box solutions based on the EMPI concept are available to generate the UHID as described earlier, including the following:

- **SeeBeyond™ eIndex™ Global Identifier***
- **McKesson Horizon Passport***
- **Siebel® Universal Customer Master***

Custom and in-house solutions

Some HCOs may consider handling an SSN remediation project in-house. If so, they will want to assess the availability of sufficient technical resources to provide the insight needed to determine the optimal solution, as well as the ability to implement the solution. Additionally, organizations will want to ensure their solution addresses both immediate and future requirements, to ensure the optimal return on investment.

HCOs could decide to simply issue new non-SSN IDs and handle old accounts separately, but the impact across enterprise-wide systems makes this an impractical and costly approach. The result will be a hodge-podge solution that will only serve as a type of band-aid.

5.

ADDED BENEFITS TO SSN REMEDIATION: OPPORTUNITY TO EVOLVE INFORMATION SYSTEMS

As HCOs assess their options in protecting their patients' privacy, they will realize the opportunity to evolve their enterprise information systems to keep pace with the latest technological innovations. This becomes increasingly important to ensure that the data contained within legacy systems is accessible throughout the organization and even via the Internet.

The Service-Oriented Architecture

While Service-Oriented Architecture (SOA) models have existed for some time, they are taking on new meaning in this age of electronic interconnectedness. The SOA model helps organizations efficiently reuse application business logic across multiple channels. It also enables organizations to logically and effectively connect legacy and new applications, providing a solid foundation for organizations that wish to move toward a real-time enterprise model. (See Figure 5.)

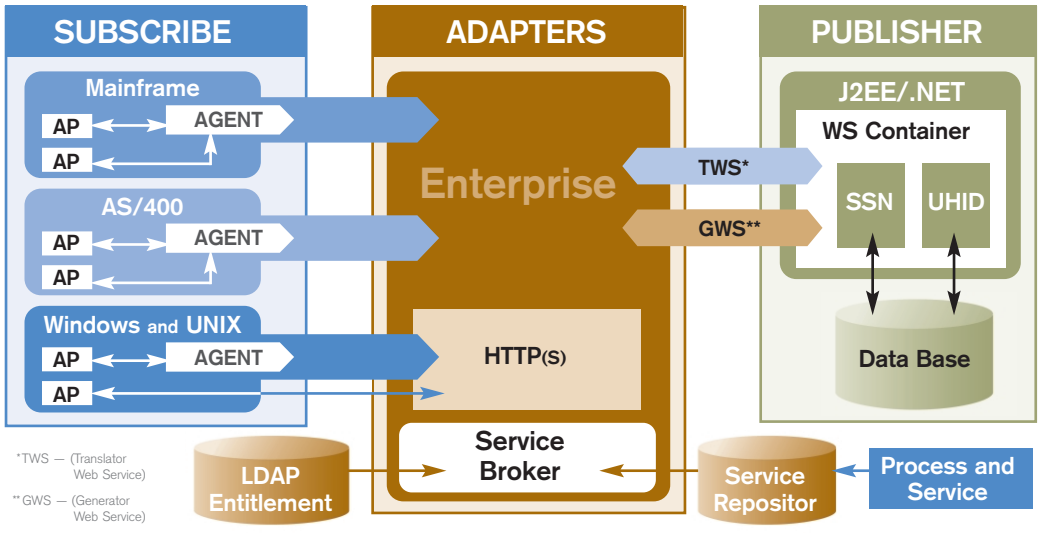


Figure 5. Migration to Service-Oriented Architecture helps HCOs seamlessly connect data and reuse business application logic.

Realizing the Real-Time Enterprise

Gartner's definition of the real-time enterprise concept is that it helps organizations achieve "competitive advantage by using up-to-date information to progressively remove delays in the management and execution of its critical business processes".[10] RTE techniques enable faster access to patient information and quicker execution of business processes, ultimately adding significant value to initiatives such as data warehousing and customer relationship management (CRM). According to Gartner, healthcare organizations must possess these characteristics to improve quality of care while reducing costs.

Benefits beyond compliance

By investing in new and emerging technologies to address the issue of ensuring patient health information privacy, organizations will not only meet legal requirements and industry best practices, but will also realize a return on investment. Implementing an SSN remediation solution will provide healthcare organizations with insight into system interdependencies which they can leverage to support the implementation of other required HIPAA identifiers (NPI, NHI, NEI, etc.) and other strategic business initiatives. In fact, forward-looking organizations will seize this opportunity to streamline business processes, workflows, and infrastructure usage.

While pursuing the vision of linking HCO systems to strategic goals (such as ensuring patient health information privacy) may require an unforeseen budget allocation, the ultimate savings through efficiency should outweigh the initial costs. On an industry level, the White House estimated in 2002 that the healthcare industry would incur costs of approximately $18 billion over a ten-year period to implement privacy-related measures. It also estimated that the healthcare industry would realize almost $12 billion in savings due to these measures. "Further, there will be additional savings in the long term because patients will have more faith in the health care system, so they will be less likely to withhold vital information from their doctors, and will more readily seek care".[11]

6.

CONCLUSION

As HCOs contend with compliance deadlines and complex system architectures, they will benefit from the expertise and support of a skilled IT vendor. Healthcare organizations can leverage Syntel's extensive healthcare industry experience and our unique perspective on the specific process issues, technology implications, and regulatory factors affecting healthcare providers to successfully implement technologies that meet requirements and drive business results.

Syntel Offers SSN Secure Remediation Solution

Syntel has developed a comprehensive SSN Remediation offering—SSN Secure—that helps healthcare organizations assess their options and ultimately implement the most appropriate solution, whether it is custom or out-of-the-box. The Syntel process consists of field-tested steps to ensure a successful project. Each engagement consists of Syntel working with the customer to:

- **Complete an initial exposure assessment across both operational (i.e., policy, process, and people) and technical aspects of the organization.**
- **Establish project goals and objectives.**
- **Create a project execution strategy that aligns with the organization's goals and objectives.**
- **Create a communication and training plan that will help the customer address the required cultural changes throughout its organization.**
- **Perform a detailed impact analysis that provides the customer with insight into the extent of changes throughout the enterprise systems.**
- **Assist with appropriate tools and technology selection.**
- **Define a solution approach that meets the organization's goals and objectives.**
- **Implement the solution in accordance with the customer's timeline.**

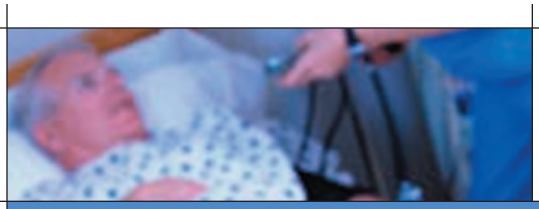
Partnering with Syntel

As the first U.S.-based firm to launch a Global Service Delivery model in 1992, Syntel has perfected this model to deliver reduced time-to-market, enhanced efficiencies, and quality improvements for large-scale IT projects in the healthcare and insurance marketplaces. Syntel is able to deliver complex IT projects with outstanding quality and competitive pricing.

Syntel has developed an internal Healthcare Center of Excellence, through which it offers customized healthcare industry services leveraging its experience across a variety of healthcare industry functions. These services address application development and management, enterprise application integration, data warehousing, enterprise resource management, customer relationship management, health plan solutions, digital healthcare, Medicaid solutions, and regulatory compliance. Syntel crafts each solution around its deep understanding of the issues facing HCOs across claims processing, enrollment, eligibility and benefits, sales and marketing, premium billing, contract administration, revenue cycle, supply chain, departmental systems, and clinical data systems functions.

To date, Syntel has helped numerous organizations on both the payer and provider side—including Humana, First Health Services Corporation, Blue Cross Blue Shield of Georgia, Aetna, HCA, and Hanger Orthopedic Group Inc.—stay ahead of a wide range of technology developments. In short, Syntel has the experience, methodologies, and consultant training to help your organization protect patient privacy rights while implementing an infrastructure that will enable business agility and deliver measurable ROI.

See back cover for references.



about SYNTEL:

References

1 Mark Rotenberg, Executive Director, Electronic Privacy Information Center and Adjunct Professor, Georgetown University Law Center, Testimony and Statement for the Record, Joint Hearing on SSNs and Identity Theft, Subcommittee on Oversight and Investigations, Committee Financial Services, and Subcommittee on Social Security, Committee on Ways and Means, U. S. House of Representatives, November 8, 2001, www.epic.org/privacy/ssn/testimony_11_08_2001.html

2 Federal Trade Commission, National and State Trends in Fraud & Identity Theft, January – December 2003, January 22, 2004, http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf

3 Fight Identity Theft, California Law SB 168 (Debra Bowen) Identity Theft Prevention Questions and Answers, http://www.fightidentitytheft.com/legislation_california_sb168.html

4 CSO Magazine, Five Ways to Fight ID Theft, March 2004, http://www.csoonline.com/read/030104/idtheft.html

5 California Department of Consumer Affairs, Office of Privacy Protection, Recommended Practices for Protecting the Confidentiality of Social Security Numbers, June 2002; revised January 2003, http://www.privacy.ca.gov/recommendations/ssnrecommendations.pdf

6 Computerworld Magazine, Do no harm: HIPAA's role in preventing ID theft, June 12, 2003, http://www.computerworld.com/databasetopics/data/story/0,10801,82051,00.html

7 Social Security Administration, Office of the Inspector General, Social Security Number Misuse fact sheet, updated June 2003, http://www.ssa.gov/oig/executive_operations/factsheet1.htm

8 United States Department of Health & Human Services, Health Insurance Portability and Accountability Act of 1996, http://aspe.hhs.gov/admnsimp/pl104191.htm

9 Joint Healthcare Information Technology Alliance, National Health Identifier for Individual Issue Summary, http://www.jhita.org/identif.htm

10 Gartner, Inc., Architecture Agility for Healthcare or Life Science RTEs, March 3, 2004

11 Health Privacy Project, Myths and Facts about the HIPAA Privacy Rule, updated September 22, 2003, http://www.healthprivacy.org/info-url_nocat2303/info-url_nocat_show.htm?doc_id=173435

Syntel provides custom outsourcing solutions to Global 2000 corporations. Founded in 1980, Syntel's portfolio of services includes BPO, complex application development, management, product engineering, and enterprise application integration services, as well as e-Business development and integration, wireless solutions, data warehousing, CRM, and ERP.

We maximize outsourcing investments through an onsite/offshore Global Delivery Service, increasing the efficiency of how complex projects are delivered. Syntel's global approach also makes a significant and positive impact on speed-to-market, budgets, and quality. We deploy a custom delivery model that is a seamless extension of your organization to fit your business goals and a proprietary knowledge transfer methodology to guarantee knowledge continuity.

SYNTEL
525 E. Big Beaver, Third Floor
Troy, MI 48083
phone **248.619.3503**
info@syntelinc.com

ISO 9001 2000 SEI CMM LEVEL 5