Chapter 1 : Managing the Integrity of Patient Identity in Health Information Exchange (update)

See the latest version here. This version is made available for historical purposes only. Over the past decade, multiple studies have documented the value of health information exchange HIE. Patient identification integrity is a complex concept, and one that is not well understood throughout the healthcare industry. Many policy makers and industry leaders do not fully comprehend the negative effects of inaccurate patient identification information for even basic health information interchange. Even though most provider settings use a medical record number MRN as a unique identifier to connect records across and within their electronic systems, many of the interfaces across these multiple systems commonly 30 to 50 within a single hospital use some patient demographic data to validate the interfaced transaction. Organizations that exchange health information and do not share a common unique identifier are completely dependent upon the accuracy and completeness of the key demographic data available in both records for successful electronic linking. Healthcare standards for patient identity integrity have been slow to emerge. Existing standards address data format and position within an electronic transaction; however, data content accuracy has yet to be addressed. Historically, little emphasis has been placed on the role patient identification systems play in the quality and safety of healthcare delivery. Local patient identification errors have been contained and managed within the healthcare organizations that create them. Sending the wrong health information to the point of care can create critical patient care issues and risk privacy breaches, degrading consumer trust. The negative effects of local patient identification errors will expand as technology advances and the national health information network continues to expand. To this end, this practice brief outlines how organizations can manage patient identification systems from front-end data capture to back-end quality control as an ongoing process and carry local quality operations into health information exchange efforts. It urges industry stakeholders to recognize that now is a critical time to address accuracy in patient identification systems. Unless the healthcare industry takes the necessary measures to ensure complete and accurate data at the provider and HIE levels, the national strategic efforts under way to improve quality and safety will be more difficult to accomplish. Support for better decision making, effective care processes that improve health outcomes and reduce cost outgrowth, and consumer benefit from health IT through improved access to patient health information are made possible when unbroken and dependable patient identification systems are operating. Patient Identification Processes, Procedures Ongoing, focused management and oversight of healthcare patient identification is critical to both internal operations and regional and national HIE efforts. Cradle-to-grave lifetime records that are accurate, complete, authenticated, and accessible by authorized providers can only occur if these processes are thorough and timely. Organizations must develop policies that ensure key demographic data are accurate and used to link records within and across electronic health record systems. These policies must address the accuracy of information at the initial point of capture using front-end verification, including timely correction of duplicate records and quality monitoring using a duplicate creation rate. Record-linking algorithm effectiveness should be validated prior to linking records within an organization or releasing records to an HIE. Organizations should outline duplicate record validity procedures and ensure they are followed. They must provide staff training at all levels to reinforce the importance of successful health information exchange. A well-managed patient identity integrity program will include an ongoing performance improvement process that assesses error rates and ensures progressive improvement. HIM professionals are well positioned to lead this effort. Technology Efficiencies Health data exchange increasingly occurs across disparate provider organizations using networks and Internet-based technologies. Interoperability requires the electronic transmission of data across organizations and assumes the data exchanged are accurate, comprehensive, current, consistent, relevant, timely, granular, precise, accessible, and well-defined. HIEs currently use a variety of data delivery methods, which determine how patient records are sought and matched. In these scenarios, the receiving provider knows the patients about which it is receiving messages and uses internal procedures to process the

incoming transaction. A provider searches the RLS and finds and selects the patient for whom it is searching. Electronic messages are then sent to each of the participating organizations that have stored records pertaining to the patient. Specific types of electronic clinical results are pulled back from each participating organization to the requesting provider, such as lab tests, text-based reports, medication histories, and problem lists. A centralized data model uses both push and pull technologies. Providers search the MPI of this centralized database and pull the corresponding information for the applicable patient across to their system. Record Matching A fundamental and critical success factor for the RLS and centralized models is how the indexes within these databases link records for the same patient from the disparate participating organizations. Many healthcare provider organizations have multitudes of unique identifiers for a patient e. Therefore, once an RLS obtains demographic data from its participating organizations, it must collapse all of these individual demographic records for one patient into a single record. In this model, the HIE links the different provider records for one patient into one record and assigns that patient a unique numeric identifier. This unique identifier is sent back to each participating organization that holds medical records for that patient. Subsequent updates to the HIE by that participating organization use this unique identifier. For example, John Smith has been seen at a physician office, hospital, and lab. His HIE unique identifier, , is included in the identifying data set from each provider. His records from all providers can be retrieved by entering this unique identifier in the search screens. The algorithms available to perform this linking function fall into three main groups: Comparisons are made on selected data elementsâ€”usually the name, birth date, SSN, and sometimes the gender. Exact match and deterministic algorithms are both basic matching tools. With exact matching, the data elements used to search must match exactly with those in the database in order to return a particular record. Deterministic matching is slightly more sophisticated in that in addition to exact matches, partial matches or matches on Soundex codes or those from other phonetic encoding systems may be used to return a record. However, a deterministic match using a substring of the first three letters partial name of the last name would be returned. With wild-card linking, the user enters a few letters of the value being searched and adds a character frequently a common keyboard symbol that instructs the program to return every record that matches the limited letters entered. Intermediate Algorithms Intermediate algorithms use more advanced techniques to compare records. Fuzzy logic and arbitrary or subjective scoring systems are added to exact match and deterministic tools. A field match weight is arbitrarily assigned to key patient identifying attributes, such as last name, first name, date of birth, and SSN. For example, a match on the SSN may be assigned a score of 40 points, while a match of the last name scores Any records presented to the searcher must reach a minimum scoring threshold to qualify for inclusion. Fuzzy logic and rules-based algorithms also may be a component of intermediate algorithms. These tools include nickname tables, rules to address transposition of characters or names, digit rotations, and typographical errors within the MPI database. Intermediate algorithms may include an automated frequency adjustment, which decreases the field match score. Advanced Algorithms Advanced algorithms contain the most sophisticated set of tools for matching records and rely on mathematical theory. The core intelligence within advanced algorithms includes bipartite graph theory, probabilistic theory, and mathematical and statistical models, which are applied to determine the likelihood of a match on specified data elements. Probabilistic matching uses the frequency of a specific element with a probability score assigned to adjust the relative value of the match or mismatch for the specified elements. The weight assigned to each field is relative to the weights assigned to other fields, but only after thorough research across millions of records as opposed to a simple frequency analysis with an arbitrary field weight adjustment. Advanced algorithms also include machine learning and neural networks, which use forms of artificial intelligence that simulate human problem solving. For example, a search for: Whatever algorithm an organization uses to link records, the results should be verified by staff using record-matching validity procedures. When applying designated HIE system requirements, a percentage of records from different participating organizations will be able to be automatically linked if a sufficiently sophisticated algorithm is used. Even with a sophisticated algorithm, the HIE will achieve significantly higher rates of record links if potential overlap records that have a record match weight lower than the autolink threshold are reviewed and manually linked. There will always be potential intrafacility duplicate pairs that must be sent back to that participating organization for staff to

review, validate, and manually combine. False positives and false negatives will always occur with any algorithmic or manual system identifying potential duplicates. A false negative will result when the algorithm or other duplicate identifying process does not identify a true duplicate and the duplicate remains in the database. False positives occur when two records are matched together because they are presumed to belong to one person, when in fact they belong to different people. They are easier to find if a review is completed of each potential duplicate identified by the system. Common pitfalls include linking two closely related people with very similar names and dates of birth who live near each other e. Failure to catch such errors can result in overlaid medical records and subsequently negative health outcomes, serious privacy breaches, and legal ramifications. This causes one patient to have two different medical records within the same facility. For example, patient John Smith has medical record number at facility A and a medical record number at facility B within the same enterprise-wide system. Thus, Smith ends up with two different enterprise identifiers and providers cannot view all clinical information across the enterprise for that patient. On occasion, overlays are caused by an incorrect merge of two records that belong to two different people. How to Measure Duplicate Record Rates Participating organizations such as hospitals and other healthcare delivery systems within the HIE are responsible for maintaining the integrity of the patient-identifying data within their own systems. Organizations that fail to carry out this responsibility not only compromise care within their own four walls, but also contaminate the HIE database and cause administrative complications or compromise care at other participating organizations. Different methods can be found within the healthcare industry to measure the duplicate rate at a given point in time or measure the ongoing duplicate-creation rate. Algorithms used to identify potential duplicate records are also widely different. When choosing algorithm software or vendor consultant services, organizations are advised to investigate and understand proposed measurement techniques and ensure a consistent approach is used for subsequent comparative performance measurements. Below, a basic, best-practice, standardized formula is described to ensure sound unit counting when measuring duplicate rates in any healthcare organization. Facility Duplicate Rate for Static Database Healthcare organizations sometimes choose to analyze their entire MPI database for potential duplicate records at a given point in time i. The organization extracts the MPI data and analyzes that static group of records. A computation determines the percent of records that are potential duplicates at the time the data were extracted within that one database at that one facility. After the duplicates have been evaluated, those that truly represent the same individual qualify to be included in the calculation. The following formula is a standard industry method of computing the actual duplicate record rate in a single database: For example, a facility has 10, duplicate pairs in the database, involving 20, individual records. The database at the time of the analysis contained , individual records. The duplicate rate is computed by dividing 10, by , and multiplying the result by to obtain the percent result. In this example the rate is 2 percent: The total number of registrations should include any opportunity that users have to create a new record when performing scheduling, preregistration, or registration activities. If the scheduling system creates a permanent person or patient record within the MPI database when scheduling an appointment, this represents an opportunity to create a duplicate record and should therefore be included. Accordingly, the definition of the denominator may vary from organization to organization and is dependent upon the configuration and functionality of their applications. If an inbound ADT or scheduling transaction creates a new patient record, and that new record creates a duplicate patient record in the database, it should be counted in the numerator. Presuming that all these activities present the opportunity to create a new record in the database, the formula for determining the duplicate creation rate is:

Chapter 2 : The Integrity Factor: A Journey in Leadership Formation - Kevin W. Mannoia - Google Books

Note: Citations are based on reference standards. However, formatting rules can vary widely between applications and fields of interest or study. The specific requirements or preferences of your reviewing publisher, classroom teacher, institution or organization should be applied.

Jun 13, , 2: As the appetite for risk has fallen, oil and gas operators have had to employ increasingly sophisticated monitoring and control systems to provide safeguards for their wells, pipelines, and production facilities. Yet many firms lack visibility at field or enterprise level because information relating to well production, barrier equipment, and design is held in different departments or various formats. Without an integrated source of well integrity data or a uniform method of analyzing that data, it is difficult for oil and gas firms to effectively manage the human and organizational aspects of risk. Improvements in safety and serious lapses In , a year that saw safety issues related to oil and gas exploration dominating headlines around the world, the rate of fatalities was actually the lowest on record. Despite the continuous improvements in personal safety, the oil and gas industry has had to deal with several process safety lapses in recent years. The most significant of these was the Macondo incident in the Gulf of Mexico. Within months of Macondo, the OGP established the Global Industry Response Group GIRG , which is overseeing industry efforts to determine what can be done on an international scale to improve well incident prevention, intervention, and response capabilities. The GIRG has determined more reliable well safety relied on renewed efforts in four key areas: Creation of an industry-wide well control incident database Assessment of blow-out-preventer reliability and potential improvements to this equipment Improved training and competences and more attention paid to human factors The development and implementation of key international standards pertaining to well design and well operations management Complexity and confirmation bias Benchmarking using such KPIs is critical given that every large organization is, by its very nature, complex. Moreover, different levels of understanding and accountability will exist within any large organization, making it a challenging task to ensure process safety and effective risk management across all aspects of its business. Indeed, even the best designed, engineered, maintained and operated assets and facilities are still vulnerable to human failings and organizational complexity. One recognized example of the latter is the asset based organization model, which can lead to conflicts of interest. Under the asset model, there will be an engineer or someone responsible for managing a group of wells and who must balance good practice against production targets. If that person encounters a situation where they have to weigh safety concerns against production or financial targets, they may be more likely to not elevate concerns when compared to safety engineers. This can be the case where a test has been conducted thousands of times, an abnormal reading is returned on a single occasion, and is therefore more likely to be viewed as an anomaly. Whereas if that test was being conducted for the first time and an abnormal result were returned, it would be cause for major concern. Information on the status of safety-critical well barrier components must be completely dependable, and the components must operate as reliably as possible should a problem arise at any given point in time. Yet many firms continue to rely on handover documentation and a patchwork of bespoke production management databases and spreadsheets to manage data. What is needed is a systematic management system, especially since it can take a long time to gather statistically relevant data. Industry bodies such as the OGP now recommend that systems be implemented for consistent collection and analysis of data and related information on more than just major incidents. One emerging model is the well integrity management system WIMS , which aligns all elements including the business process, handover, data management, and risk management. As a sub-set of asset integrity management, WIMS exist both at a documentation and software level, and combine key well operating and production data within a framework for decision-making, management processes, and organizational structure. A holistic approach An advanced WIMS can interface to a wide range of third-party databases to collate the necessary information for analysis and identification of wells shifting outside critical safe operating limits, for the assessment of equipment reliability and well risk, and for real-time estimation of corrosion in the well tubing. Data can also be acquired directly via tablet PCs in the field, entered manually, or

via spreadsheet loader â€” and synchronized instantly with the central database to provide a comprehensive, singular view. Documenting institutional well integrity management into a software product and working system can have major benefits for a large company when combined with a robust approach to knowledge management and placed in the hands of trained and experienced personnel. It ensures consistency of data, which is vital for oil and gas firms with global operations who need the confidence that the right people have access to the right information at the right time for rapid, informed and consistent decision-making. It also ensures consistency in terms of knowledge management and approaches to well integrity. This is essential given large oil and gas firms tend to have a high turnover staff internally. With operating well data consolidated within a single user interface, the addition of smart functionality enables operators to analyze the well condition automatically in real time and generate concise reports customized to their individual requirements. In addition to the severe curtailment to production and cost of shut-in, there is also the cost of restitution and remediation. The aging of wells in many parts of the world does tend to result in increasing risk of leaks, particularly related to loss of integrity in the outer annuli of the well. At the same time, WIMS can help address the human and organizational factors surrounding well integrity by quickly focusing staff attention on problem areas of an asset, and by providing the ability to manage by exception.

Chapter 3 : Integrity Management in the Prevention of Major Accidents

Managing the integrity factor by James J. Lynch starting at $ Managing the integrity factor has 1 available editions to buy at Alibris.

Will you make the commitment? Adherence to moral and ethical principles. In this definition, you are not integrous if you are not acting consistently with the principles that work in life. Integrity is not really an issue of being moral or righteous or "right". It is simply a condition of acting consistently with the principles that work, with each part being in alignment with the other parts. To act otherwise will not work in life. One can think that he can "get away with" not acting in integrity, but that is an illusion. See What Is Reality? We manipulate it to fit with some concept of being good and approved of by others - which is a use that is entirely inconsistent with the definition of integrity. Integrity is simply about "what works". Nothing more, nothing less. In this viewpoint, you see that it works and that it is a "value" that is extremely valuable to living a good life. It comes from the inside out, from the values you hold. It is you creating your own sub game in life. Obviously, as everyone writes about, integrity includes doing what you say you will do; you even keep promises to yourself. In that case, you are said to be "out of integrity". But we often fail to see that if we promise ourselves and discount it or let ourselves not keep the promise, we are hurting ourselves in the long run and often the short run. A viewpoint of integrity is one where we know that our world will not work for us whenever we are "out of integrity" - we will incur problems over and over and over. The game is played on the reality field of life, with the rules being those of the physical world where all that counts is actual results. The strategies are to follow the rules to get the most "points. See the article on this site: Life Value Productivity and link to the almost costless Kindle book from there. It is a manual for running your life. It is the first of the agreements. Love is a word used to mean "for the good" and "truth" simply means reality in which "workable principles" is, of course, a part. So, the two together simply mean aligning with reality and the principles that work in life for the good of oneself and others. If you are to be in integrity, you would pledge to be impeccable with your word - and to see that it is what will work in this world for your own greater good. Doing excellent work is "what works" to produce value in the world. These are other examples of acting in integrity: Not having any disempowering behaviors or attitudes no "sabotaging" or hidden "againstness" Being impeccable in being truthful and honest. Being excellent and skillful in what you do. Always engaging in "fair exchange" that is honest and open. Delivering the value that you know is the right thing to do, even if it is above what the client might expect. It includes keeping ALL your promises. This includes keeping the time promise. And it includes making no excuses or coming up with "reasons why not" or any victimhood stories. See the sidebar articles with more examples. Integrity includes "completing" on effectively installing integrity! All those parts when acting consistently with who you are comprise integrity, AND they also are what comprise focused power. Pretending or holding on to the idea that one is, though a grown up, still a child believing unexamined and untrue beliefs is far "out of integrity". To be in integrity, one must acknowledge and take on the mantle of being a Rational, Nurturing Adult. Success or reasons why not. Note, again, that this is not at all a moral judgment. It is simply about "what works. In the fear world, we use excuses, justifications, reasons. If one is "being integrity" as a chosen way of being i. In the other world, one takes shortcuts and has that be because it is "too hard" to put out the effort to go "the long way around. And, believe it or not, it is more efficient and effective to "be in integrity" - i. The most common "shortcut" is to getting short term "relief" from some current uncomfortability, at the expense of the long term. When you grow up from acting in this child way and go for the long term benefits, you will see your life take a giant leap upward. And with those beliefs you actually create your emotional pain - needlessly! Living in integrity has the highest payoff of all, but to do that one must diminish the imaginary other side of the scale that you think may be greater:

Chapter 4 : Leadership and integrity | Lead on Purpose

The study focused on the critical role that integrity factor plays in effectively managing the marketing executives in Nigerian banks. The study also made a few recommendations for improving the.

CONTACT US Managing the Integrity of Patient Identity in Health Information Exchange update Accurate patient identification is foundational to the successful linking of patient records within care delivery sites and across the healthcare ecosystem to underpin care delivery, data exchange, analytics, and critical business and clinical processes. These goals have increased in importance as health information exchange has evolved over the last decade with the healthcare industry striving to reduce costs, increase interoperability, and transform to a patient-centric care delivery model. Strong information governance that addresses patient identity integrity and accurate patient matching is key to a patient-centric health system and patient-centric processes. This Practice Brief explores the complexity of patient identification integrity, including how organizations can manage patient identification systems from front end data capture to back end quality control as an ongoing process and carry local quality operations into health information exchange efforts. It urges industry stakeholders to recognize that now is a critical time to address accuracy in patient identification systems. Patient Identity Integrity Vital to Healthcare Various components of the healthcare ecosystem will address these goals and execute patient identification integrity activities to: Support care delivery and care coordination within an enterprise, as well as data exchange across healthcare systems. Underpin analytics within and across organizations, including pattern recognition, Big Data, and predictive analytics. Support information governance strategy and practices. This governance must underscore the complexity of patient identity integrity, including people, processes, and technologies. There is no single solution. Patient identification integrity is a complex concept, and one that is not well understood throughout the healthcare industry. The complexity stems from many factors including variability in practices of authentication, data collection, technology, and the historical silo approach to patient identification. Incorrect or incomplete data capture within the healthcare setting can create critical patient care issues and risk privacy breaches, thus degrading consumer and user trust. Health information organizations HIOs support, oversee, or govern the exchange of health-related information among organizations according to nationally recognized standards. HIOs are the recipients of the stewardship and governance applied to patient identification processes, thus HIOs are today highlighting many of the weaknesses in the historical systems and practices. As data exchange methods through Direct messaging, private exchange, or state HIOs continue to evolve, patient identification errors will increase significantly. Policymakers and industry leaders are beginning to recognize the importance of patient identification, as exhibited by the early patient matching recommendations from the Office of the National Coordinator for Health IT ONC Health IT Policy Committee following a public hearing on patient matching hosted by the Privacy and Security Tiger Team in late The scope of the challenges includes factors such as: Proof of identification is not routinely required at the time of data capture and lack of accountability in validating patient identity compounds duplicate and overlay creation. Registration is a high staff turnover area where entry-level employees typically do not have adequate education and training. High-volume registration areas such as scheduling have a much higher risk of duplicate creation and overlays due to the lack of direct patient contact. Specimen registration information typically contains minimal identifiable patient information to locate existing patient records. The abundance of poor quality patient identification data stored and managed in siloed legacy systems causes the potential for data integrity issues. Data quality issues are magnified when source systems are not kept in sync throughout the exchange network. Data error corrections and duplicate remediation practices are not always performed in a timely and comprehensive fashion. Corrections that do occur are often performed by understaffed teams or inadequately trained staff. Variation in the tools and solutions that measure or address patient identification integrity also may compromise data integrity. As mentioned above, identification requirements vary greatly across provider organizations. For example, the request for proof of identity is not always required at registration or check-in. Differences may include one or two forms of identification with or without a photo. Government-issued identification should be

the standard. There is a lack of data standards addressing accurate and complete data capture and data matching for patient identification. And the standards that do exist are limited in scope and adherence is suboptimal. Existing standards are largely targeted at vendor and source system data format and position, not content accuracy, completeness, or relevance to industry changes. However these protocols and standards are not routinely adopted or consistently implemented by vendors, enterprises, or HIOs. Organizations rely instead on data being captured in compliance with older HL7 standards. To support high quality data exchange, AHIMA has published data quality standards that promote accurate, comprehensive, current, consistent, relevant, timely, granular, precise, accessible, and well-defined data. While data exchange is on the uptake, electronically exchanged data rarely meet the standard for each data quality attribute listed above. HIOs currently use a variety of data delivery methods, which determine how patient records are sought and matched. For example, all electronic prescriptions generated within a hospital are automatically sent to a specific pharmacy, or all transcribed documents are forwarded to the provider s listed in the HL7 message. In these scenarios, the receiving provider generally already knows which patient the messages concern and thus uses relevant internal procedures to process the incoming transaction. Data trading partnerships between providers may dictate the content and format of the HL7 message. Electronic messages are then sent to each of the participating organizations that have stored records pertaining to the patient. Specific types of electronic clinical results required by the federal meaningful use requirements are extracted from each participating organization to be shared or exchanged with the requesting provider or in transition of care cases. It provides a means for one healthcare practitioner, system, or setting to aggregate all of the pertinent data about a patient and forward it to another practitioner, system, or setting to support the continuity of care. It is flexible XML-based clinical document architecture. A centralized data model can use both push and pull technologies. Each organization participating in the HIO sends pushes patient demographic along with clinical results to a central database managed by the HIO. Providers search the EMPI of this centralized database and pull the corresponding information for the applicable patient across to their system. Such a person or entity may be an individual provider, a clinic composed of multiple providers, an integrated delivery network, a clearinghouse, or a billing agent. To achieve this objective it is imperative that each contributing organization eliminate the duplicate and overlay records within their enterprise master patient index EMPI files. By correcting the integrity of the patient records at each contributing organization the advanced matching algorithm within the HIO EMPI will be able to accurately link records for the same patient from the disparate participating organizations. Each data trading partner will have different unique identifiers for their patients and these will not correlate across exchanges. In the absence of a nationally recognized patient identifier, the HIO must rely on sophisticated matching technology and the quality and completeness of the demographic data collected and maintained by each participating healthcare provider to create its own unique patient identifier. Therefore, once the HIO EMPI obtains demographic data from its participating organizations, it must link all of these individual demographic records for one patient into a single record. In this model, the HIO links the different provider records for one patient into one record and assigns that patient a unique numeric identifier. For example, patient John Smith has been seen at a physician office, hospital, and lab. Each organization submits their respective information to the HIO. The HIO ascertains, based on the demographic information from the respective organizations, that their records all belong to the same John Smith. Advanced matching algorithms are applied to key demographic attributes such as first, middle, and last name, gender, date of birth, Social Security number if present , phone number, and address in order to reach this conclusion. The algorithms available to perform this linking function fall into three main groups: Whatever algorithm an organization uses to link records, the results should be verified by staff using record matching validity procedures during the initial system deployment and periodically thereafter. When applying designated HIO system requirements, a percentage of records from different participating organizations will be automatically linked if a sufficiently sophisticated algorithm is used. However, a statistically significant sample should always be reviewed to ensure only true overlap records are auto-linked. Even with a sophisticated algorithm, the HIO will achieve significantly higher rates of record linkage if potentially overlapped records that have a record match weight lower than the auto-link threshold are reviewed and manually linked. False positives incorrectly linking

similar records belonging to two different people , false alarms detecting records that do not belong to the same person , and false negatives not detecting multiple records belonging to the same person will always occur with any algorithmic or manual system for identifying potential duplicates, linkages, or overlays. Common pitfalls include linking: Two closely related people with very similar names and dates of birth who live near each other, such as cousins who are named after the same individual Two individuals living in a dense urban area with the same common name, date of birth, and address Twins with the same first name Failure to catch such errors can result in fragmented data due to missing clinical information or overlaid medical records and, subsequently, negative health outcomes, serious privacy breaches, and legal ramifications. HIOs and data trading partners should adopt a process of periodically measuring their false positive and false negative rates and include formal communication mechanisms to alert appropriate departments and staff when it is determined that duplicates or overlays may impact clinical or business operations. It is important to realize that most healthcare information systems employ basic algorithm matching techniques and these techniques usually only identify 10 to 40 percent of the existing duplicate records. A few healthcare information systems employ intermediate algorithm matching techniques, which will identify 50 to 70 percent of the existing duplicate records. Sophisticated EMPI solutions incorporate advanced algorithm matching techniques that can identify up to 98 percent of the existing duplicate records. However, the advanced algorithms are not commonly used in healthcare. When choosing algorithm software or vendor consultant services, organizations are advised to investigate and understand proposed measurement techniques to ensure the highest degree of accuracy. The record matching algorithm and procedures employed by the provider should be examined via an independent audit using advanced matching algorithms to validate that they work correctly. This process will help to minimize or eliminate those records that match inappropriately false positives and any excessive reporting of records that do not belong to the same person false alarms as well as records that should match but fail to do so false negatives. Basic Algorithms for Linking Records Basic algorithms are the simplest technique for matching records and this approach is used by most healthcare information systems today. Comparisons are made on selected data elementsâ€”usually the name, date of birth, SSN, and sometimes the gender. Exact match and deterministic algorithms are both basic matching tools. With exact matching, the data elements used to search must match exactly with those in the database in order to return a particular record. Deterministic matching is slightly more sophisticated; in addition to exact matches, partial matches may be used to return a record. However, a deterministic match using a substring of the first three letters partial name of the last name would return both Smith and Smithe. Wild-card searching involves the user entering a few letters of the value being searched and adds a character frequently a common keyboard symbol that instructs the database program to return every record that matches the limited letters entered. It is important to note that most healthcare information systems employ basic search and matching techniques to locate patient records and identify potential duplicates. Therefore, many organizations that rely on their healthcare information system to maintain the accuracy of their patient index are often dependent on information technology staff to write customized reports, usually based on SQL queries. These queries and reports, although better than the basic duplicate reports contained in most healthcare information systems, still utilize basic matching techniques to identify potential duplicates. Basic algorithms typically only identify between 10 and 40 percent of the existing duplicate records within the MPI. Intermediate Algorithms for Linking Records Intermediate algorithms use more advanced techniques to compare records. Fuzzy logic, nickname tables, phonetic encoding and arbitrary or subjective scoring systems are added to exact match and deterministic tools. A field match weight is subjectively assigned to key patient identifying attributes such as last name, first name, date of birth, and SSN. For example, a match on the SSN may be assigned a score of 40 points, while a match of the last name scores Conversely a mismatch would also be assigned a subjective negative value on SSN and last name. Records presented to the searcher must reach a minimum cumulative scoring threshold to qualify for inclusion. Fuzzy logic and rules-based algorithms also may be a component of intermediate algorithms. These tools may utilize nickname tables, rules to address transposition of characters or names, digit rotations, and typographical errors within the MPI database. Phonetic encoding is typically utilized in intermediate algorithms. Intermediate algorithms may

include a limited automated frequency adjustment. With these types of algorithms, a search for Elizabeth Jones would return records for Betty Jones as well as Elizabeth Jones.

Chapter 5 : Environmental resource management - Wikipedia

In virtually all philosophy disciplines, from Plato through LifeSpring, integrity is cited as the major component of what makes life work and indeed the foundation for being happy, from "the virtues" of Plato, where it is a matter of ethics and not morality, to current writings, even as the basis for achieving your goals in life.

The most common cause of pressure wounds and skin integrity issues is constant pressure to the skin as it gets squeezed against a surface such as a bed or wheelchair. Continued pressure reduces blood flow to the area, causing injury. Pressure wounds and skin integrity issues usually happen if a child remains in one position for a long time. Other causes of pressure sores and skin integrity issues include: Sliding down a chair or bed. Pulling across a chair or bed. Irritation from sweat or other bodily fluids. Children who are at risk of developing bed sores and skin integrity issues often: Use braces, casts or a wheelchair. Spend a lot of time in one position. Have trouble thinking clearly. Have difficulty managing their health. Pressure Wound Symptoms and Prevention If your child is at risk for pressure wounds and skin integrity issues, you should check for signs of problems every day. Your health care provider can help you evaluate any signs of developing wounds. A red or pink appearance on lighter skin. An ashen, blue or purple appearance on darker skin. Pain in the area. A firmer, softer, warmer or cooler feeling in the area compared to other parts of the body. Although daily skin checks offer the best chance of preventing problems, children at risk of pressure wounds and skin integrity issues should also: Drink plenty of water. Eat a balanced diet. Keep their skin clean. Schedule regular visits with orthotists, seating practitioners and durable medical equipment vendors to make sure braces and seating fit properly. Change position every two hours when in bed. Change position for at least two minutes every hour if using a wheelchair. Get out of a wheelchair every few hours. Avoid excessive layers of clothing, sheets or materials. Avoid dragging or pulling skin across surfaces when moving from a wheelchair to a bed transferring. Our integrated care model is centered on treatment for complex conditions, such as those that can lead to problems with skin integrity or bed sores. Gillette specialists certified in wound care, test skin integrity, help with wound management, and educate your family about pressure wound prevention and skin integrity issues. If you ever notice issues during a routine skin check, or have questions about preventing pressure wounds, contact Gillette and speak to a nurse. Pressure mapping uses special mats to create a map of pressure distribution, pinpointing the highest areas of pressure. This information helps therapists and seating specialists recommend ways to reduce pressure in these locations. Our surgeons are experts in closing difficult-to-treat wounds. We also specialize in pressure wounds and skin integrity issues caused by limited mobility or loss of sensation. Videos Our videos provide useful tips if your child is at risk of pressure wounds and skin integrity issues due to immobility or loss of sensation.

Chapter 6 : Managing the Human and Organizational Factors of Well Integrity | Utilities | Energy Digital

The integrity factor for leadership formation, according to Mannoia, is an Â¡Â§intentional integration of Â¡K two pursuits, uniquely patterned in Scripture for every Christian leader.Â¡Â¨ The two pursuits are Â¡Â§unseen foundationsÂ¡Â¨ of Â¡Â§being before GodÂ¡Â¨ and performance flow out of oneÂ¡Â¦s being.

Job Rotation[edit] Job Rotation is an approach to management development where an individual is moved through a schedule of assignments designed to give him or her a breath of exposure to the entire operation. Job rotation is also practiced to allow qualified employees to gain more insights into the processes of a company and to increase job satisfaction through job variation. Separation of Duties[edit] Separation of duties SoD is the concept of having more than one person required to complete a task. It is alternatively called segregation of duties or, in the political realm, separation of powers. Without those few and far between expert level techs who can have or get the administration rights to view all aspects of any given production process it will be nearly impossible to determine the underlying cause and can lead to outrageous decisions as to what the problem must of been. Or nobody realizing the automated software machine was running into RAM issues because every automated job was set to auto start at exactly 6: With the concept of SoD, business critical duties can be categorized into four types of functions, authorization, custody, record keeping and reconciliation. In a perfect system, no one person should handle more than one type of function. In information systems, segregation of duties helps reduce the potential damage from the actions of one person. IS or end-user department should be organized in a way to achieve adequate separation of duties Control Mechanisms to enforce SoD There are several control mechanisms that can help to enforce the segregation of duties: Audit trails enable IT managers or Auditors to recreate the actual transaction flow from the point of origination to its existence on an updated file. Good audit trails should be enabled to provide information on who initiated the transaction, the time of day and date of entry, the type of entry, what fields of information it contained, and what files it updated. Reconciliation of applications and an independent verification process is ultimately the responsibility of users, which can be used to increase the level of confidence that an application ran successfully. Exception reports are handled at supervisory level, backed up by evidence noting that exceptions are handled properly and in timely fashion. A signature of the person who prepares the report is normally required. Manual or automated system or application transaction logs should be maintained, which record all processed system commands or application transactions. Supervisory review should be performed through observation and inquiry and the trust built with directory one-level up managers. To compensate repeated mistakes or intentional failures by following a prescribed procedure, independent reviews are recommended. Such reviews can help detect errors and irregularities but are usually expensive can raise questions as to how much can an outside independent review once a quarter know about your processes compared to people within and what level of trust can be built with those independent reviewers. Least Privilege Need to Know [edit] Introduction The principle of least privilege, also known as the principle of minimal privilege or just least privilege, requires that in a particular abstraction layer of a computing environment every module such as a process, a user or a program on the basis of the layer we are considering must be able to access only such information and resources that are necessary to its legitimate purpose. This principle is a useful security tool, but it has never been successful at enforcing high assurance security on a system. Benefits Better system stability. When code is limited in the scope of changes it can make to a system, it is easier to test its possible actions and interactions with other applications. In practice for example, applications running with restricted rights will not have access to perform operations that could crash a machine, or adversely affect other applications running on the same system. When code is limited in the system-wide actions it may perform, vulnerabilities in one application cannot be used to exploit the rest of the machine. In general, the fewer privileges an application requires the easier it is to deploy within a larger environment. This usually results from the first two benefits, applications that install device drivers or require elevated security privileges typically have addition steps involved in their deployment, for example on Windows a solution with no device drivers can be run directly with no installation, while device drivers must

be installed separately using the Windows installer service in order to grant the driver elevated privileges Mandatory Vacations[edit] Mandatory vacations of one to two weeks are used to audit and verify the work tasks and privileges of employees. This often results in easy detection of abuse, fraud, or negligence. Job Position Sensitivity[edit] Security Roles and Responsibilities[edit] Levels of Responsibilities[edit] Senior management and other levels of management understand the vision of the company, the business goals, and the objectives. Functional management, whose members understand how their individual departments work, what roles individuals play within the company, and how security affects their department directly. Operational managers and staff. These layers are closer to the actual operations of the company. They know detailed information about the technical and procedural requirements, the systems, and how the systems are used. The employees at these layers understand how security mechanisms integrate into systems, how to configure them, and how they affect daily productivity. Classification of Roles and their Responsibilities[edit] Data Owner The data owner information owner is usually a member of management, in charge of a specific business unit, and is ultimately responsible for the protection and use of a specific subset of information. The data owner decides upon the classification of the data that he is responsible for and alters that classification if the business needs arise. This person is also responsible for ensuring that the necessary security controls are in place, ensuring that proper access rights are being used, defining security requirements per classification and backup requirements, approving any disclosure activities, and defining user access criteria. The data owner approves access requests or may choose to delegate this function to business unit managers. And it is the data owner who will deal with security violations pertaining to the data he is responsible for protecting. The data owner, who obviously has enough on his plate, delegates responsibility of the day-to-day maintenance of the data protection mechanisms to the data custodian. Data Custodian The data custodian information custodian is responsible for maintaining and protecting the data. System Owner The system owner is responsible for one or more systems, each of which may hold and process data owned by different data owners. A system owner is responsible for integrating security considerations into application and system purchasing decisions and development projects. The system owner is responsible for ensuring that adequate security is being provided by the necessary controls, password management, remote access controls, operating system configurations, and so on. This role needs to ensure that the systems are properly assessed for vulnerabilities and must report any to the incident response team and data owner. The security administrator role needs to make sure that access rights that are given to users support the policies and data owner directives. Security Analyst This role works at a higher, more strategic level than the previously described roles and helps to develop policies, standards, and guidelines and set various baselines. Whereas the previous roles are "in the weeds" and focusing on their pieces and parts of the security program, a security analyst helps define the security program elements and follows through to ensure that the elements are being carried out and practiced properly. This person works more at a design level than at an implementation level. Application Owner An application owner, usually the business unit managers, are responsible for dictating who can and cannot access their applications, like the accounting software, software for testing and development etc. Change Control Analyst The change control analyst is responsible for approving or rejecting requests to make changes to the network, systems, or software. This role needs to make sure that the change will not introduce any vulnerability, that it has been properly tested, and that it is properly rolled out. The change control analyst needs to understand how various changes can affect security, interoperability, performance, and productivity. Data Analyst The data analyst is responsible for ensuring that data is stored in a way that makes the most sense to the company and the individuals who need to access and work with it. The data analyst role may be responsible for architecting a new system that will hold company information or advising in the purchase of a product that will do this. Process Owner Security should be considered and treated like just another business process. The process owner is responsible for properly defining, improving upon, and monitoring these processes. A process owner is not necessarily tied to one business unit or application. Complex processes involve a lot of variables that can span across different departments, technologies, and data types. Solution Provider This role is called upon when a business has a problem or requires that a process be improved upon. User The user is any individual who routinely uses the data for work-related tasks. Product Line Manager Responsible for explaining business

requirements to vendors and wading through their rhetoric to see if the product is right for the company Responsible for ensuring compliance to license agreements Responsible for translating business requirements into objectives and specifications for the developer of a product or solution Decides if his company really needs to upgrade their current systems This role must understand business drivers, business processes, and the technology that is required to support them. The product line manager evaluates different products in the market, works with vendors, understands different options a company can take, and advises management and business units on the proper solutions that are needed to meet their goals.

Chapter 7 : The Integrity Factor

One emerging model is the well integrity management system (WIMS), which aligns all elements including the business process, handover, data management, and risk management. As a sub-set of asset integrity management, WIMS exist both at a documentation and software level, and combine key well operating and production data within a framework for.

Chapter 8 : Pressure Wounds and Skin Integrity Issues | Gillette Children's Specialty Healthcare

Managing the Integrity of Patient Identity in Health Information Exchange (update) Accurate patient identification is foundational to the successful linking of patient records within care delivery sites and across the healthcare ecosystem to underpin care delivery, data exchange, analytics, and critical business and clinical processes.

Chapter 9 : Managing the Integrity of Patient Identity in Health Information Exchange ()

The objective of this article is to draw attention toward the three main factors that test the integrity of project management practitioners and sponsors in a capital industrial project environment. This article suggests some of the possible ways to encounter those challenging factors and manage them for success.