Introduction:
e-Health and information governance

e-health
Around the world, health care providers and public health organizations are making unprecedented investments in e-health. The aim: to improve patient and public health outcomes by improving the accessibility and quality of health care services, while driving down costs.

To achieve these strategic imperatives, organizations are implementing a range of e-health solutions, including:

• Health care management systems, which use reporting, analytics and process optimization solutions to improve the performance of back-office, business and clinical processes

• Patient-centric e-health solutions, which empower patients to manage their health more effectively

• Telemedicine systems, which support the remote delivery of health care services

• Electronic prescribing systems, which enable clinicians to create and transmit electronic prescriptions to dispensing organizations

• Health information systems, which store and provide clinicians with access to information related to patients’ health, diagnosis and care provisions

Integrated e-health solutions
Standalone e-health systems deliver clinical and administrative benefits but do not enable organizations to realize the full potential of e-health. To deliver the greatest possible value in terms of cost reduction and improved health outcomes, disparate health care management systems, telemedicine solutions and health information platforms must be able to securely and effectively share data. Doing so requires health networks that connect public health agencies, provider organizations, hospitals, clinics, diagnostic laboratories, health service commissioners and individual clinicians.

To achieve this level of integration, some organizations have invested heavily in integrated health information solutions. These solutions are becoming increasingly common and are known by various monikers: Patient Care Records (PCR), Computer-based Medical Records (CMR), Electronic Patient Records (EPR), Summary Care Records (SCR), Electronic Medical Records (EMR) or Electronic Health Records (EHR).

Accenture has identified three core types of integrated health information system:

Intra-enterprise EMR
These solutions enable clinical and administrative systems within a public or private health care provider to share patient-identifiable information in support of clinical processes. A defining characteristic of this solution type is that data is not electronically shared outside organizational boundaries.
Inter-enterprise EMR
These solutions enable multiple health care enterprises to share patient-identifiable clinical and administrative information in support of clinical processes. Examples include Health Information Exchanges (HIE) and Regional Health Information Networks (RHIN). A defining characteristic of an inter-enterprise EMR is that limited data is electronically shared outside organizational boundaries.

Full EHR
These solutions contain all relevant health information for an individual—including clinical, administrative, claims, wellness, demographic and treatment data, from diverse providers, public health organizations and payers (where relevant). A defining characteristic of a full EHR is that all data is routinely shared outside organizational boundaries—including, in some cases, with organizations not participating in the EHR.

For the purposes of this paper, we use “EHR” as an umbrella term referring to all types of integrated health information systems.

The benefits of EHR
As health systems around the world grapple with burgeoning costs, increasing demand and growing patient expectations for high-quality, personalized care, organizations are turning to EHR to improve the quality and accessibility of health care services, while also reducing the cost. EHR deliver these benefits by:

- Providing clinicians with electronic access to comprehensive medical records that include clinical data from multiple providers and episodes of care. This access enables personalized treatment plans, supports evidence-based clinical decision making, reduces the risk of medical and prescription errors, supports seamless care across care settings and reduces the cost of sharing medical records among providers.
- Connecting health care providers through health networks. Such integration improves the accessibility of specialist care by enabling clinical data and images to be sent electronically to specialists and diagnostic laboratories for assessment. This enhances care quality by encouraging provider-to-provider consultations to support diagnosis and clinical decision making. Health networks also reduce the cost of care because fewer providers require dedicated diagnostic laboratories and specialists.
- Enabling decision makers and researchers to access large amounts of patient non-identifiable clinical data. Information discovery or data mining solutions and clinical and business analytics platforms can use this information to generate insight to drive improvements in process efficiency, care quality and care management. Anonymized or pseudonymized EHR data can also improve the efficiency and effectiveness of clinical research (for example, if used in clinical trials). Moreover, EHR data can be used for epidemiological analysis and biosurveillance, thereby helping improve the effectiveness of disease management, public health campaigns and preventative health strategies.

The case for information governance
While the importance and benefits of sharing health information are widely recognized, organizations have struggled to implement effective EHR solutions. Complex technical, organizational, regulatory and cultural challenges have increased implementation risks and led to relatively high solution failure rates.

Ultimately, many of these challenges are related to information governance.
Information governance defined

Information governance encompasses the processes, functions, standards and technologies that enable high quality information to be created, stored, communicated, valued and used effectively and securely in support of an organization’s strategic goals.

Critical Information Governance Challenges

Interoperability
Achieving interoperability without open or common national or international standards is proving to be a major challenge. Increasingly, organizations are focusing on standards development, standards-driven architectures, translation or terminology services, and certification services to achieve partial interoperability. Full semantic interoperability remains uncommon.

Data integrity
Maintaining the meaning, structure and other characteristics of clinical data when it is stored, modified, processed and communicated between systems is a major challenge, particularly in highly distributed environments.

Access control
Controlling access to clinical data and enabling patients and providers to determine who can access data are important technical challenges. Legal and regulatory restrictions on access to clinical data mean that EHR require robust access control solutions and permissioning regimes.

Security
Preventing unauthorized access to clinical data, ensuring the availability of services and maintaining network integrity are particularly difficult in distributed multisystem environments.

Data handling
Health regulators, watchdogs and self-implemented best practices require providers to implement stringent data handling policies. In many cases, compliance requires organizations to invest in mandatory data handling training, establish enterprise-wide data risk and monitoring functions, and develop and enforce certified data handling policies.

Data quality
Ensuring that data in an EHR is accurate, meaningful and internally consistent is extremely important. Poor quality data affects patient safety, limits the clinical and administrative value of EHR and undermines process and care quality improvements based on clinical analytics. Ensuring data quality is a major challenge in complex multisystem environments—particularly when subsystems use noninteroperable standards and clinical terminologies.

Consent
Developing and implementing effective consent models to meet patients’ and clinicians’ expectations have proved difficult. Patients and regulators reasonably expect consent models to focus on protecting data privacy and confidentiality by restricting the use and dissemination of information. Such restrictions can limit the clinical value of EHR; clinicians may be unable to access medical information relevant to diagnosis or treatment. Finding and articulating the consent basis for data sharing is critically important to EHR success.

Compliance
Although legal and regulatory requirements vary across countries, compliance with privacy, confidentiality, data security, data loss, data protection, data handling and audit regulations remains an important issue for all health care organizations. Organizations must manage information risks effectively in accordance with their legal and regulatory obligations. Addressing compliance requires a coordinated approach across organizations. Enabling IT organizations to collaborate effectively with legal departments, clinicians and administrators to design and implement systems and processes that ensure compliance is a common issue for healthcare organizations.
The key to successful information governance is building an effective information governance architecture—a layer of processes, functions, policies and solutions that ensure the effective and secure creation, storage, communication, valuation and use of information. Effective information governance architectures integrate disparate information, security, access control and content management architectures and include legal, clinical, administrative and IT work streams.

The Accenture Information Governance Framework for Health provides a holistic model of information governance—helping practitioners assess and overcome key challenges by designing more effective information governance architectures. Developed by Accenture professionals and drawing on what we have learned through e-health implementations around the world, the framework disaggregates information governance into five highly interrelated disciplines:

- Data privacy
- Data confidentiality
- Data security
- Data quality
- Data integrity

Each discipline has multiple solution components—that is, the most important processes, functions and technologies within an information governance architecture that enable organizations to overcome the critical challenges they face.

Using the Accenture Information Governance Framework we are working with organizations to develop specific tools tailored to their needs. These toolkits consist of direct controls, risk assessment frameworks and other components to make information governance a tangible part of their organization. These toolkits enable organizations to focus on providing patient care while enabling compliance with patient, regulatory and legislative requirements.
<table>
<thead>
<tr>
<th>Information Governance Disciplines</th>
<th>Information Governance Solution Components</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Privacy</strong></td>
<td>Patient consent models and mechanisms</td>
</tr>
<tr>
<td></td>
<td>Patient-provider relationship-based access controls</td>
</tr>
<tr>
<td></td>
<td>Patient access controls</td>
</tr>
<tr>
<td></td>
<td>Effective data security and data handling policies</td>
</tr>
<tr>
<td><strong>Data Confidentiality</strong></td>
<td>Role-based access control models</td>
</tr>
<tr>
<td></td>
<td>Patient and provider record sealing</td>
</tr>
<tr>
<td></td>
<td>Identification and authentication</td>
</tr>
<tr>
<td></td>
<td>Anonymization and pseudonymization</td>
</tr>
<tr>
<td><strong>Data Security</strong></td>
<td>Message integrity and communications security</td>
</tr>
<tr>
<td></td>
<td>Event audit and alerting</td>
</tr>
<tr>
<td></td>
<td>IT security audit</td>
</tr>
<tr>
<td></td>
<td>Network integrity</td>
</tr>
<tr>
<td><strong>Data Quality</strong></td>
<td>Error correction</td>
</tr>
<tr>
<td></td>
<td>Data validation</td>
</tr>
<tr>
<td></td>
<td>System and interface certification</td>
</tr>
<tr>
<td></td>
<td>Standards driven architecture</td>
</tr>
<tr>
<td><strong>Data Integrity</strong></td>
<td>Code integrity</td>
</tr>
<tr>
<td></td>
<td>System hardening</td>
</tr>
<tr>
<td></td>
<td>Interoperability governance</td>
</tr>
<tr>
<td></td>
<td>Standards-driven architecture and standards management</td>
</tr>
</tbody>
</table>
Data privacy

For regulators, watchdogs, legislative bodies, patients, patient advocates and the public, data privacy—that is, ensuring patients’ medical data can be accessed only with their consent—is the most important issue associated with e-health and EHR. Failure to convince these stakeholders that data in e-health systems is private increases implementation, compliance and reputational risk. To ensure data privacy, effective information governance architectures must include four components:

Patient consent models and mechanisms
High-level frameworks that outline how and in what circumstances organizations will seek patient consent for their medical data to be stored, disseminated, accessed and used. Patient consent mechanisms are authorization or permissioning regimes that are part of EHR access control models. These mechanisms allow patients to specify which parts of their medical records they do not wish particular user groups to have full access to.

Patient-provider relationship-based access controls
Solutions that restrict access to a specified patient’s medical data based on an existing relationship between the patient and the clinician or care provider requesting access to that patient’s data.

Patient access controls
Solutions that provide patients with secure access to their medical data. Access control solutions have three key elements: registration, authentication and authorization.

Effective data security and data handling policies
Policies that minimize information security risk and prevent unauthorized access to information by placing patient interest at the center of information governance policy and by encouraging desirable behaviors among users.

Data confidentiality

Ensuring the confidentiality of data in e-health systems by preventing unauthorized access to and improper use of information is an important part of information governance. The goal: to minimize information security risks (such as data loss and unauthorized or inappropriate use and dissemination of information), thereby reducing compliance and reputational risks and protecting data privacy. Ensuring that data in e-health systems is confidential requires a range of security solutions that monitor, restrict and prevent unauthorized access to information. Moreover, solutions should be able to obscure patients’ identity when data from their medical record is used for purposes other than delivery of care. To help ensure data confidentiality, effective information governance architectures must include four components:

Role-based access control models
Access levels, permissioning and authorization regimes, and access controls that are based on complex real-world job functions (roles) and patient-provider relationships.

Patient and provider record sealing
Solutions that enable patients and providers to restrict or prevent access to information compartments in medical records.

Identification and authentication
These solutions enable the robust authentication of health care professionals to health care systems, as well as the linking of real-world identity to system identity, to ensure that only authorized users can access patient data.

Anonymization and pseudonymization
Solutions that obscure patients’ identities by modifying patient-identifiable clinical data while maintaining data quality. Thus, the data can be used for secondary purposes without compromising confidentiality.

Data security

Data privacy, confidentiality, quality and integrity depend on the ability of e-health systems to maintain data security. Moreover, the security of clinical data is a major compliance challenge for organizations as legislative and regulatory bodies continue to develop increasingly stringent guidelines and certification processes. Ensuring the security of data in e-health systems requires health care enterprises to develop security architectures that proactively manage security risks, effectively identify and prioritize threats, and rapidly address vulnerabilities. To help ensure data security, effective information governance architectures must have four components:

Message integrity and communications security
Solutions that maintain the integrity of data transferred between systems in messages and prevent unauthorized access to and/or modification of messages.

Event audit and alerting
Functionality that enables systems to monitor, log and report security-relevant events.

IT security audit
Manual and automatic processes that test and evaluate the effectiveness of solutions’ information security measures.

Network integrity
Solutions that enable networks to maintain expected functionality, performance and service availability despite unexpected events, such as security threats and spikes in demand.
Data quality

High-quality data is meaningful, accurate and internally consistent; it can be used for its intended purpose. Poor-quality clinical data in e-health systems affects patient safety, quality of care and user adoption. It also increases compliance and implementation risks. However, ensuring data quality is a major challenge—particularly in complex, multisystem environments in which subsystems do not share common technical, data, communication or terminology standards. The key to ensuring data quality in these environments is to develop solutions with intelligent data handling functionality and to implement standardized interfaces and data models that enable subsystems to share information more effectively. With that in mind, effective information governance architectures must include four components:

Error correction
Manual and automatic processes that detect and correct errors in information efficiently and effectively.

Data validation
Validation rules that verify that data conforms to a set of specifications regarding format, quality, integrity, accuracy and structure.

System and interface certification
Roles, processes and solutions that verify that systems and interfaces conform to specifications defined by regulators and Standards Development Organizations (SDOs).

Standards-driven architecture
System architectures that leverage open standards for the recording and coding of data, thereby promoting a high level of data quality through similar data processing across multiple component systems.

Data integrity

Data integrity refers to the validity, accuracy and reliability of data after it has been stored, transferred, retrieved or processed. Failure to ensure the integrity of clinical data has an adverse affect on data quality, system flexibility and performance. To maintain data integrity, the infrastructure underlying e-health systems must maintain data quality and characteristics (format, meaning, rules, relationships and latency, for example) during such operations as storage, retrieval, communication and transfer. Data integrity can be affected by a range of factors. Among them: unauthorized modification of data, poor-quality source code and noninteroperable subsystems. To address these issues, effective information governance architectures must include four components:

Code integrity
Processes that test source code to eliminate bugs that may result in data loss or data corruption during data storage or transfer.

System hardening
Periodic or ongoing processes that reduce security risks by evaluating the effectiveness of security architectures, identifying security risks and undertaking security improvements.

Interoperability governance
A function that works across organizational and information silos to develop and enforce common standards, protocols and processes to enable syntactic, semantic and/or process interoperability.

Standards-driven architecture and standards management
A standards-driven system architecture conforms to open or common messaging, infrastructure, communication, application, data and clinical terminology standards. Standards management includes the roles, processes and solutions that develop, manage and enforce common technical, communication, messaging and data standards that enable subsystems to share information more effectively.

We describe the Accenture Information Governance Framework for Health in more detail in separate papers—each discussing one of the disciplines and associated solution components and outlining a number of e-health planning and implementation recommendations for health care organizations.
Developing Effective Information Governance: Next Steps

Whether a health care organization is considering, implementing or operating advanced e-health solutions, designing and implementing a successful information governance architecture can be a daunting task.

Information governance challenges affect every part of the health care enterprise and developing effective solutions requires collaboration across organizational silos, functions and information systems. Based on Accenture research and experience from e-health implementations around the world, we believe there are four initial steps toward effective information governance:

Conduct a comprehensive risk assessment and gap analysis of current information governance provisions

Most healthcare organizations have a range of existing information governance provisions across information and organizational silos. This potentially fragmented and disjointed approach to information governance can make it difficult for organizations to develop a clear understanding of how effective and efficient their information governance provisions are and the information risks they face. Health care organizations should conduct a comprehensive risk assessment and gap analysis to enable a single enterprise-wide view of information governance performance and information risks. Using a structured approach to information governance, such as the Accenture Information Governance Framework for Health, organizations should create a consolidated inventory of information governance provisions, build a model to assess their performance and develop strategies to address weaknesses and improve information governance performance.

Identify, analyze, evaluate and prioritize information governance challenges

For a health care organization, the second step toward improved information governance is developing detailed insight into the information governance challenges it faces. This requires a comprehensive program involving IT, legal, clinical and administrative functions to:

• Identify a broad range of current and future compliance, security, data quality and system integration challenges.

• Analyze these challenges to develop a detailed understanding of their root causes.

• Evaluate the impact these challenges are having or are likely to have on quality of care, efficiency, costs, strategic priorities, the workforce, and administrative and clinical processes.

• Prioritize the challenges based on their likely impact and the ability of the organization to address them.

Design solutions and develop strategies to address these challenges

Once a health care organization has a detailed understanding of the information governance challenges it faces, it should develop high-level strategies and design solutions to address these challenges. An organization should conceive of these solutions and strategies as components of an integrated information governance architecture. The ultimate goal: creating an efficient, effective and sustainable information governance function as part of a comprehensive IT governance framework. In most cases, information governance challenges cut across information and organizational silos. Thus, solution design and strategy development must be collaborative processes that involve IT, legal, clinical, administrative and strategic functions—possibly from different organizations.

Develop a detailed implementation plan

Developing the right implementation plan up front is the key to minimizing implementation risk, ensuring long-term stakeholder engagement, reducing the cost of implementation and developing effective information governance. In clinical environments, solution implementation can be challenging, especially if programs disrupt processes integral to the delivery of care or impose new ways of working on clinicians. Implementation plans should include:

• A high level of detail around targets, benchmarks, critical success factors, timetables, release schedules, reporting, coordinating activity and implementation management roles for specific programs and work streams.

• A long-term clinical change management plan that includes communications strategies and programs that support clinical transformation, process re-engineering, user acceptance and training to support specific work streams.

• A comprehensive systems integration plan; from a technical perspective, it should define how information governance solutions will be integrated into organizations’ systems architectures, how solutions will be procured efficiently and how integration programs will be managed.

Realize the benefits of effective information governance

A consolidated enterprise-wide information governance architecture will improve data quality and data security. This will enable health care organizations to address patients’ concerns over data privacy, ensure compliance with regulatory and legislative requirements, maximize the clinical and administrative benefits of EHR and increase physician adoption.
Appendix

Data privacy
Data confidentiality
Data security
Data quality
Data integrity
Data privacy

Overview

Regulators, watchdogs, legislative bodies, patients, patient advocates and the public expect patient-identifiable data in e-health systems to remain private. In practice, data privacy requires organizations to ensure that patient-identifiable data is disseminated and used in accordance with patients' wishes and that access is based on patient consent. To help protect data privacy, organizations must implement policies and processes that enable patients to authorize and restrict access to identifiable data in e-health systems.

Data privacy requires sophisticated, consent-based access control models and permissioning regimes. These solutions should enable patients to define fine-grained access controls based on flexible access levels that can be granted to a range of user groups. This enables patients to determine who is able to access what data in their medical records.

To help ensure the privacy of data in e-health systems, effective information governance architectures must include four components:

- Patient consent models and mechanisms
- Patient-provider relationship-based access controls
- Patient access controls
- Effective data security and data handling policies

Patient consent models and mechanisms

Due to the sensitive nature of clinical data and the prevalence of stringent data privacy guidelines, patient consent should be the prime access control in e-health systems. Electronic patient-identifiable data should be created, accessed and used only with patient consent. However, developing effective consent models that meet patient, clinician and public expectations has proved to be a major challenge.

In broad terms, there are two types of consent models:

- **Opt-in models**—in which patient dissent is assumed and patients must proactively consent for their medical data to be stored electronically, accessed or used. In some cases patient consent will be assumed until withdrawn while in others it will be time limited or renewed at each clinical encounter or episode of care.

- **Opt-out models**—in which patient consent is assumed and patients must proactively dissent for their medical data not to be stored electronically, accessed or used. Patients are usually informed how their data will be used and are invited to opt out if they do not wish for their medical data to be used in such a way.

Organizations should be aware of the trade-offs involved in choosing one consent model over another. Opt-in models usually give patients more control over the use of their medical data. Consequently, opt-in models tend to strengthen data privacy and reduce opposition to EHR from patients, regulators and the public. However, opt-out models often increase the number of patients whose medical data is stored electronically. Opt-out models may also reduce patient-mandated restrictions on the use of data in support of clinical processes integral to care delivery and screening and surveillance programs, as well as epidemiological and clinical research. As a result, opt-out models may maximize the clinical benefits of e-health.

In practice, many health care organizations adopt a hybrid approach in which an opt-out model is adopted for certain functions, such as creating electronic medical data, and an opt-in model is adopted for others, such as sharing and using medical data. While hybrid models may enable health care organizations to capture some of the benefits and avoid some of the pitfalls of using either model exclusively, they can also be extremely complicated. This complexity can lead to scalability problems, high implementation risk stemming from project management and system complexity, increased cost, and confusion among clinicians, administrators, patients and the public.

Patients may wish to restrict access to parts of their medical record to limit the dissemination of very sensitive information or if they are concerned that their medical data may be compromised. As a result, patient consent mechanisms should be part of EHR access control models. Patient consent mechanisms are authorization or permissioning regimes that allow patients to specify parts of their medical record that they do not want particular user groups to have full access to. Patients should be able to define multiple access levels to particular compartments of information that can be applied to a range of user groups. Figure 1 illustrates some example access levels, information compartments and user groups that may be part of fine-grained patient consent mechanisms within a consent-based access control model.
### Patient-provider relationship-based access controls

To protect patient privacy, access to patient-identifiable clinical information in e-health systems should be based on an existing relationship between the patient and the clinician or provider requesting access. Clinicians or providers not involved in the delivery of care services to the patient should be unable to access the patient’s clinical information without explicit consent. Moreover, clinicians and providers should only have access to information necessary for them to fulfill their clinical responsibilities. For example, a psychiatrist may not require access to information on a patient’s surgical history; likewise, a pharmacist may not require access to a patient’s critical care record.

Protecting patient privacy requires access control models and solutions that restrict access to information and functionality based on real-world patient-provider relationships. These relationships are often very complex and, as a result, e-health systems require fine-grained permissioning and authorization regimes. These permissioning and authorization regimes should be part of sophisticated, role-based access control models that restrict access to clinical information based on real-world job functions and patient-provider relationships.

### Patient access controls

Solutions that provide patients with secure access to their medical data are becoming an increasingly important part of e-health systems. Effective patient access controls are particularly important for Internet-based patient portals. Allowing patients to access their medical records improves the accuracy and completeness of information in EHR while empowering patients to manage their health more effectively and contribute to clinical decision-making processes.

Access control solutions have three key elements: registration, authentication and authorization:

- Registration enables patients to create and manage user accounts that are associated with access rights. By linking user accounts through a single sign-on system, patients can access medical information in disparate systems without creating multiple user accounts.

- Authentication verifies patients’ identity and confirms that user accounts are legitimate. Authentication factors include username and password, digital certificate, security token and biometric identifiers, such as thumbprints. Two-factor authentication, which requires patients to prove their identities using two different factors, is used to reduce security and data privacy risks.

- Authorization grants user accounts access rights and allows or rejects access requests based on these access rights. In most cases, these rights enable patients to access all their medical information held in a system, excluding information sealed by clinicians or administrators.

### Access levels/permissions

| Information is not visible to user group |
| Information is visible to, but cannot be accessed by, user group |
| Information can be accessed by user group but only with patient consent |
| When information is accessed by user group, an alert is generated |
| Information can be accessed by user group, but authorization is time limited and must be renewed periodically |

### Information compartments

| Any freeform data in a medical record |
| Data related to a particular medical specialty (such as psychiatry, oncology or neurology) |
| Demographic data |
| Data associated with a specific episode of care |
| Information on chronic conditions and underlying health problems |
| Prognostic information |
| Pharmaceutical and non-pharmaceutical treatment information |

### User groups

| Individual clinicians |
| Clinical workgroups or departments |
| Provider administrators |
| Public health organizations |
| Researchers |
| Central management functions |
| Patient proxies |
Effective data security and data handling policies

Organizations' data collection, data handling, data security and data sharing policies should minimize information security risks and prevent unauthorized use of information by encouraging desirable behaviors among clinicians and administrators. Desirable behaviors include:

- Collecting, storing and sharing data securely using appropriate security technologies, such as encrypted storage devices and secure communication channels.
- Minimizing the risk of data loss or misuse by maintaining the effectiveness of access controls—for example, not sharing passwords and ensuring that passwords meet certain criteria.
- Proactively identifying and minimizing security and confidentiality risks—for example, printing information only when absolutely necessary, disposing of hard copies securely, anonymizing or pseudonymizing data where possible and removing software that may compromise security, such as peer-to-peer programs.
- Reporting security breaches and unauthorized or improper use of information.
- Restricting physical access to hardware—including laptops, desktops, mobile devices and cell phones—that store or enable users to access sensitive data.
- Educating other users to raise awareness of data security and data confidentiality risks and encouraging them to adopt behaviors that minimize these risks.

Recommendations

Implementing effective data privacy solutions has proved to be a major challenge for health care organizations around the world. Designing solutions that meet the expectations of regulators, clinicians, administrators, managers, patients, the public, politicians and other stakeholders is the most common challenge. However, organizations tend to concentrate on the technical and clinical aspects of data privacy while neglecting the strategic, organizational and cultural dimensions. From Accenture's research and experience from e-health implementations around the world, we believe that to address these issues, health care organizations implementing an e-health systems should:

Consult clinicians, patients and the public when designing consent models

Designing consent models should be a transparent, collaborative process involving a broad range of stakeholders. By adopting a collaborative approach, organizations design more effective consent models that are fit for purpose. Further, by engaging stakeholders early in the process, organizations reduce resistance from patients, clinicians and regulators. This reduces the risk of subsequent—and expensive—system changes to access controls and data privacy solutions.

Communicate the purpose of data privacy measures to clinicians and patients

Organizations should develop effective communication strategies to ensure that clinicians and patients understand why and how data privacy will be maintained. Communication strategies should demonstrate organizations' commitment to data privacy and the effectiveness of data privacy solutions while convincing clinicians and other stakeholders that data privacy controls will not reduce the clinical value of e-health.

Educate patients so they understand data privacy controls

For consent-based access controls to be effective, patients must be able to make informed judgments regarding data use. At a minimum, patients should understand how their medical data will be used, how widely it will be disseminated and what the benefits and potential drawbacks are. Patients should also understand the processes through which they can restrict and authorize access to data.
Data confidentiality

Overview
Preventing unauthorized access to and use of information in e-health systems is a major challenge for health care organizations. Ensuring the confidentiality and security of electronic medical data is becoming increasingly difficult as mobile networks, Internet-based patient and provider portals, health 2.0 technologies and health data banks become more common. Moreover, as EHR become more widespread, health care regulators and watchdogs are focusing unprecedented attention on data confidentiality.

Maintaining the confidentiality of data in e-health systems requires a range of solutions that prevent the unauthorized collection, storage, use and dissemination of information. Data confidentiality solutions are designed to prevent unauthorized access to information by enforcing access restrictions and permissions defined by patients through consent-based access control models.

To ensure the confidentiality of information in e-health systems, effective information governance architectures must include four components:

- Role-based access control models
- Patient and provider record sealing
- Identification and authentication
- Anonymization and pseudonymization

Role-based access control models
To ensure that users have access to the information and functionality they require without compromising data confidentiality, access control models should reflect complex, real-world job functions and patient-provider relationships. To that end, access control models should enable patients to restrict or authorize access by granting permissions to user groups based on their actual job function or role. In most cases, role-based access control models must be quite detailed so that very specific permissions can be granted to individuals or small workgroups based on their roles. Permissions not only define what information a user can see and access, but they also determine how this information can be used and what functionality the user can access.

The figure below demonstrates a simplified role-based access control model based on a range of patient-provider relationships and roles. Each user group requires a set of permissions enabling them to access relevant information and functionality directly related to their role and relationship with the patient. For example, clinicians delivering acute-care services require access to high-level clinical information that may directly affect treatment plans and clinical decision making. On the other hand, clinicians involved in specialist care require access to more detailed clinical information related to their area of specialty across a number of care episodes.

Patient and provider record sealing
To ensure that patient consent is the prime access control in e-health systems, patients must be able to seal parts of their medical record so clinicians and administrators outside a particular workgroup cannot access them. The sealed information compartments may or may not be visible to users outside the authorized workgroup. This enables patients to control access to sensitive information in their medical record—thereby helping to reduce privacy concerns and patient opposition to EHR. However, patient record sealing can have a detrimental impact on the clinical value of e-health and may even affect patient safety.

To maintain data confidentiality in certain circumstances, clinicians and administrators may have to restrict or prevent access to information compartments in patients’ medical records. Such action is usually necessary when a medical record contains information related to a third party that cannot be disseminated. Systems and users must be able to identify records that contain confidential information about a third party and restrict access to this information. The ability to seal records should be granted only to a limited number of users. Further, guidelines should make clear under what circumstances records should be sealed.

Identification and authentication
Also critical to data confidentiality: effective provider access controls that enable clinicians and administrators to securely access information in e-health systems and that monitor and prevent unauthorized access and use of information. E-Health systems should have effective access control solutions that enable the robust authentication of health care professionals to health care systems, and the linking of real-world identity to system identity. Such controls help ensure that only authorized users can access patient data. These solutions should support fine-grained role-based access control models and must also meet stringent regulatory requirements regarding data management, data protection and information audit. Compliance requires systems to monitor and log access request, logins and activity so audit trails can be generated.
Access control solutions have three key elements: registration, authentication and authorization:

- **Registration** creates user accounts for clinicians and administrators. These accounts are linked to access rights. Registration can be a complex process in multisystem and multienterprise architectures with role-based access control models. Users may require more than one user account to access different systems. What’s more, each user account may have different access rights and permissions depending on the type of information and system involved. Linking user accounts through a single-sign-on system can improve usability; users must log in only once to access a number of different systems. However, a single-sign-on capability alone does not address the underlying technical complexity of registration in multisystem environments.

- **Authentication** verifies the identity of clinicians and administrators and confirms that user accounts are legitimate. Most health care organizations must meet stringent regulatory requirements regarding authentication. Compliance usually requires systems to employ multifactor authentication in which users prove their identities using at least two authentication factors, such as password, personal identification number (PIN), biometric identifier, security token, smart card and ID card. Mobile and telemedicine e-health solutions require very strong authentication to ensure the security of information communicated across wireless networks and the Internet.

- **Authorization** grants access rights to user accounts. It also restricts or authorizes access to systems based on these access rights. In a fine-grained role-based access control model, access rights are granted to user groups defined by their real-world job-functions or patient relationships. To ensure system flexibility, authorization solutions should enable administrators to efficiently add and remove users’ permissions and modify or create new access levels.

**Anonymization and Pseudonymization**

When medical data is used for secondary purposes other than delivery of health care services, patients’ identity must be obscured to maintain data confidentiality. The seven principal levels of data obscuration (see Figure 2) range from clear, patient-identifiable data to anonymized data. The required level is usually determined by regulators based on local data privacy guidelines and is influenced by a range of factors, including data use and scope of dissemination.

---

**Figure 1: A simplified role-based access control model**

- **Individual:** Patient proxy
- **Clinical workgroup:** Pharmacy
- **Administrative workgroup:** Primary care clinic
- **Healthcare Professional:**
  - **Administrative workgroup:** Hospital inpatient management
  - **Clinical workgroup:** Psychiatric care
- **Individual:** General practitioner
- **Clinical workgroup:** Emergency care

Permissions:
- Users can access, modify and use information on current medications, past medications and abuse/response history, as well as pharmaceutical records
- Users can access, modify and use information on past psychiatric conditions, session notes, hospitalizations and psychiatric treatments
- Users can grant permissions to other user groups and access entire medical record except compartments sealed by physicians
- Users can only access administrative data related to a single hospital admission
- Users can access patient's entire medical record, modify data and disseminate information to other health care providers.
- Users can only access administrative data relevant to appointment booking and outpatient management
- Users can access, modify and use information on patient’s critical history, major surgeries, chronic and/or current conditions and abnormalities
- Users can access patient’s entire medical record, modify data and disseminate information to other health care providers.
- Users can only access administrative data related to a single hospital admission
- Users can access, modify and use information on patient’s critical history, major surgeries, chronic and/or current conditions and abnormalities
- Users can access patient’s entire medical record, modify data and disseminate information to other health care providers.
- Users can only access administrative data related to a single hospital admission
- Users can access, modify and use information on patient’s critical history, major surgeries, chronic and/or current conditions and abnormalities
Recommendations
There are a range of technical challenges associated with implementing effective data confidentiality solutions across complex architectures in distributed environments. However, vendors, systems integrators and health care organizations are developing effective solutions to address these issues. Increasingly, the most important challenges organizations face when implementing data confidentiality solutions are related to organizational and process issues. From Accenture’s research and experience from e-health implementations around the world, we believe health care organizations implementing e-health systems should:

Implement processes that enable IT, legal, clinical and administrative functions to work together effectively in developing data handling policies and role-based access control models
Effective data handling policies and access controls should conform and be adapted to meet regulatory and local legal requirements and reduce information security risks while minimizing disruption to clinical and administrative processes. If data handling policies and access controls have a significant impact on clinical and administrative processes, users are unlikely to adopt desirable behaviors, care quality may suffer and processes are likely to become less efficient. To avoid these problems, organizations should enable stakeholders from across the organization to collaborate in designing access controls. If IT and legal teams design and implement access controls in an organizational vacuum, those controls are likely to be less effective and cost more than those developed through a collaborative approach.

Develop processes and solutions to manage and report data breaches effectively
The financial, organizational, reputational and regulatory consequences of data loss and misuse—including litigation, fines imposed by regulators, a collapse in patient confidence, and data corruption—can be very serious for health care organizations. To minimize the impact of data confidentiality failures, organizations should implement effective processes to manage and report data breaches. In many countries, regulators specify reporting requirements. However, organizations should go beyond simply reporting data breaches; they should also develop an integrated mechanism to proactively manage such breaches. These solutions detect and analyze breaches as quickly as possible to mitigate their impact on patient confidentiality while identifying vulnerabilities that can be addressed immediately.
Figure 2: Seven levels of data obscuration

<table>
<thead>
<tr>
<th>Levels of data obscuration</th>
<th>Possible purposes/uses within health care systems</th>
</tr>
</thead>
</table>
| **Level 1**  
Patient identifiable data, also known as clear data.       | • Clinical processes involved in the delivery of health care services  
• Surveillance and screening  
• Caseload management                                                |
| **Level 2**  
Codification of information—extracts codified or aggregate information from patient-identifiable data. | • Provider-level clinical governance processes, including clinical audit and clinician performance management  
• Distributing activity or patient-based funding  
• Claims processing                                                  |
| **Level 3**  
Two-way linkable pseudonymization—replaces unique identifiers, such as patient name or identifier, with a pseudonym, usually a code or number, from which a patient’s identity cannot be inferred. Two-way pseudonymization allows an authorised healthcare professional to translate pseudonyms to patient identifiers. Linking pseudonyms enables the whole-patient view to be maintained within the pseudonymized information. | • Enterprise and clinical performance management  
• Clinical audit  
• Administrative patient management processes  
• Clinical process optimization                                       |
| **Level 4**  
Two-way pseudonymization—similar to two way linkable pseudonymization but does not enable the whole-patient view to be maintained within the pseudonymized information. |                                                                                      |
| **Level 5**  
One-way linkable pseudonymization—one-way pseudonymization is irreversible because pseudonyms are generated in such a way that patients cannot be reidentified from them. Linking pseudonyms enables the whole-patient view to be maintained within the pseudonymized information. | • Service delivery planning, evaluation and optimization  
• Reporting and analytics  
• Epidemiological research  
• Clinical research  
• Compliance with “freedom of information” and other transparency and accountability legislation |
| **Level 6**  
One-way pseudonymization—similar to one-way linkable pseudonymization but does not enable the whole-patient view to be maintained within the pseudonymized information. |                                                                                      |
| **Level 7**  
Anonymization—removes all unique identifiers and patient identifiable information from data. Anonymization is not reversible and anonymized data cannot be linked to other data. |                                                                                      |
Data security

Overview

Data security has a significant impact on data privacy, confidentiality, quality and integrity. Compliance with stringent data privacy and confidentiality guidelines is possible only if organizations can prevent unauthorized access to and dissemination of data in e-health systems. The quality and integrity of information in e-health systems depends on their ability to prevent unauthorized data modification, as well as data corruption. If information in e-health systems is poor quality or lacks integrity, it diminishes the clinical and administrative value of the solution. In those circumstances, paper-based records and processes cannot be replaced; clinical process improvements driven by clinical analytics and reporting cannot be achieved; and care quality gains based on the implementation of decision support tools cannot be realized.

Ensuring data security requires health care enterprises to develop security architectures that proactively manage security risks, effectively identify and prioritize threats and rapidly address vulnerabilities. To help ensure the privacy, confidentiality, quality and integrity of information by enabling secure data collection, data sharing and data management, effective information governance architectures must include four components:

- Message integrity and communications security
- Event audit and alerting
- IT security audit
- Network integrity

Message integrity and communications security

Maintaining the validity of data transferred between systems in messages is critical to ensuring data integrity. Effective communications security solutions prevent message corruption, reduce the risk of data loss and help organizations meet data security requirements by ensuring message security and integrity. These solutions prevent and detect unauthorized access to messages; encrypt and authenticate messages; and enable automatic message validation.

Event audit and alerting

To ensure compliance with stringent audit requirements and maintain data quality and integrity by preventing unauthorized access, an EHR should monitor, log and report security relevant events. Such events include access requests, database queries, logins, configuration changes, file and network access, firewall reporting, attempted violation of access control rules, and the modification and communication of restricted information.

When security-relevant events occur, the system should automatically generate alerts. As part of ongoing vulnerability management and compliance programs, IT organizations should develop effective security alert management processes to ensure that legal, clinical and administrative functions are aware of potential risks. Increasing awareness of security risks across the organization helps to increase system security by driving changes in users’ behavior and data handling processes and policies.

IT security audit

Health care organizations should conduct periodic IT security audits to ensure that data is properly protected from unauthorized access, that all relevant security threats and vulnerabilities have been identified, and that data handling processes are correctly configured to minimize security risks. IT security audits may be conducted by a third party and typically include a number of components. Among them: compliance verification, security standards certification, security assessments, penetration testing and user awareness testing. In some cases, regulators also require organizations to include a number of certified assessments in their IT security audits.

Network integrity

Data security can be affected by network integrity and resilience—that is, a network’s ability to deliver expected functionality, performance and service availability during unexpected events. Networks should be resilient enough to continue operating as designed regardless of security threats, spikes in demand or other incidents. This level of network resilience ensures the availability of processes and services that maintain data security across the network. Further, high network resilience reduces the risk of data corruption and data loss as a result of service unavailability and interruption during data transmission; helping to maintain data quality and integrity. Network integrity solutions should promote network resilience by automatically detecting and addressing security threats and unwanted network traffic; preserving network bandwidth by managing and prioritizing legitimate traffic; and generating reports on network performance to help network administrators and decision makers manage networks more effectively.
Figure 1: Four Components of data security

Recommendations

A health care enterprise’s security architecture plays a vital role in maintaining data privacy, confidentiality, quality and integrity by identifying and addressing security risks and vulnerabilities efficiently and effectively. However, data security is not just a technical issue; users’ behavior, organizations’ corporate strategy and changing market conditions are often major factors in creating or exacerbating information security risks. From Accenture’s research and experience from e-health implementations around the world, we believe that organizations should as a minimum take the following actions to help ensure data security:

Launch a proactive and comprehensive data security assessment

To ensure that data in e-health systems is secure, organizations must have an accurate and comprehensive understanding of current and potential security risks and vulnerabilities. A data security assessment should deliver a detailed inventory of all data assets and should document current data management practices, regulatory requirements and key vulnerabilities, along with the probability and possible impact of threats. The aim of a data security assessment is to develop a risk-based view of data assets, a strategic awareness of vulnerabilities and threats, a clear understanding of the severity of impacts and a foundation for investment in data security.

Ensure adequate audit capabilities

To reduce compliance and reputational risk, an EHR should automatically monitor and record all permission changes, data errors, access requests, data transfers, alterations to medical records and data breaches. With this monitoring and recording, organizations can efficiently and effectively develop detailed audit trails should the need arise. Failure to implement adequate automated capabilities increases the cost of complying with auditing requirements in certification criteria. Inadequate auditing can also significantly impair an organization’s ability to maintain data quality and integrity as access controls and security measures are less effective.

Develop a comprehensive change program to drive user compliance with data handling and IT security policies

To minimize security risks, all users must follow data security and data handling policies. However, driving changes in clinicians’ behavior and making training “stick” can be major challenges. Clinical change management can be difficult. Compounding the challenge: “Normal” change management strategies—even those based on best practices for organizations outside health care—are often ineffective. To address these issues, health care organizations should develop long-term change programs that target changes in organizational culture and user attitudes toward security and confidentiality. It is important for organizations to engage senior clinicians early on to act as change champions—encouraging the clinical workforce to follow data security policies.

For more information on Accenture’s data security solutions see www.accenture.com/security
Overview

High-quality data is meaningful, accurate, internally consistent and can be used for its intended purpose. Failure to maintain the quality of data in e-health systems can:

- Reduce patient safety if, for example, treatment plans are based on erroneous test results or prescription data is inaccurate
- Affect quality of care if clinical systems that support evidence-based medicine and enable physicians to develop more personalized treatment plans, such as Clinical Decision Support Systems (CDSS) and Computer Physician Order Entry systems (CPOE), are less effective
- Reduce user adoption rates because clinicians and administrators continue to use paper-based records to avoid errors resulting from poor data quality
- Adversely affect the performance and effectiveness of information discovery, clinical and performance analytics, business intelligence, reporting and audit platforms

Ensuring data quality is a major challenge—especially in distributed environments in which subsystems do not use common technical, data, communication, messaging or terminology standards. To overcome this challenge, organizations can implement solutions with intelligent data handling and data management functionality that identify data errors and poor quality data. Organizations can also improve data quality by enabling subsystems to share information more effectively through standardized data architectures and interfaces. To help ensure high-quality data in e-health systems information governance architectures must include four components:

- Error correction
- Data validation
- System and interface certification
- Standards-driven architecture

Error correction

Errors within an EHR occur for a variety of reasons, including data-entry errors by users, use of poor translation lexicons and ineffective data migration. An EHR should have effective processes for detecting and correcting errors. Such processes help minimize the impact of errors on clinical and operational risk, patient safety and care quality. Stringent data quality regimes that minimize user-generated errors at the point of entry and robust data migration testing procedures can reduce the probability of errors occurring—enabling organizations to focus resources on correcting errors.

Systems may be able to detect some errors automatically through sophisticated data validation rules, error checking and event and exception handling routines; however, in many cases, critical errors are related to the accuracy of data and are difficult to detect automatically. When automatic error detection fails, users must attempt to detect errors manually. CDSS and CPOE systems may help clinicians to identify errors by highlighting logical inconsistencies in medical data and generating alerts to highlight possible errors.

To ensure that errors can be corrected efficiently, organizations should have standardized correction policies and processes. These processes should enable users to manage system alerts efficiently and to report and correct errors as quickly as possible. They should also log all errors and ensure that all alterations to patients’ medical data are recorded. Further, these changes should be either visible or flagged so other users are aware data has been changed to correct an error. For audit purposes, when alterations are made to medical information, systems should record the identity of users who make changes, as well as the time, date and reason for those alterations.

Data validation

Solutions should validate clinical and administrative data in an EHR to ensure it is meaningful, complete and secure. Whether entered by users or communicated from other systems, information in an EHR should conform to a set of specifications or validation rules. Validation rules should ensure data is formatted and structured correctly and uses a compatible language, ontology and terminology. They should also check that the characteristics of data—meaning, rules, relationships, latency—are intact. Clinical applications should also have some capacity to validate the accuracy of information through manual and electronic processes that reconcile data and highlight logical inconsistencies in information.
System and interface certification

As countries around the world move toward regional and national EHR, regulators are becoming more prescriptive regarding the adoption of open standards, system capability and flexibility, clinical application functionality and data quality. Moreover, under pressure from regulators, organizations are increasingly using standards developed by health care standards development organizations (SDOs)—such as HL7 and openEHR—to enable interoperability, minimize costs and reduce implementation risks. To ensure compliance with SDO specifications and regulatory requirements, organizations should develop strong system certification and interface certification programs. Based on regulatory requirements and SDO specifications, these certification programs design and execute tests to verify compliance and identify required system changes.

System certification programs may verify the compliance of a range of hardware and software components, standards, processes and policies to evaluate system characteristics, such as security, performance, availability, data management, functionality and interoperability. Interface certification programs use detailed specifications, usually based on SDO specifications, to verify the compliance of interfaces between systems and applications. These programs verify that interfaces conform to a series of interoperability and data management standards that enable them to transfer information effectively between systems.

Standards-driven architecture

Data quality in e-health systems is affected by the ability of subsystems to share information effectively. To achieve semantic and/or syntactic interoperability, e-Health systems require a system architecture that leverages open standards for the recording and coding of data. Standardized data architectures promote a high level of data quality by enforcing common data processing, formatting and storage across multiple component systems. These standards enable those systems to share information effectively without undermining data quality.

Recommendations

Data quality can be affected by a range of factors, including data entry standards and practices and information security. However, in most cases, the most important factor affecting EHR data quality is the ability of subsystems to share meaningful and accurate information. Connecting "islands" of health data within and across enterprises has proved to be a major challenge. Despite efforts by governments and SDOs around the world, universal standards for full and ubiquitous semantic interoperability remain distant. Even so, organizations can realize some of the benefits of sharing high-quality data efficiently and effectively without universal EHR standards or significant expenditure on a unified e-health architecture. From Accenture’s research and experience from e-health implementations around the world, we believe that health care organizations implementing e-health systems should:

Consider a service-oriented architecture as a means of achieving interoperability in the short term

Achieving interoperability by enforcing common standards and implementing complex interfaces can be prohibitively disruptive and expensive in the short term. A more efficient approach: gradually implementing open standards over time as legacy systems are retired or integrated, infrastructure is updated and new applications are developed. However, to meet the short-term need for interoperability, organizations should consider replatforming toward a service-oriented architecture (SOA). This shift involves implementing an SOA and moving existing applications from multiple, noninteroperable platforms to an integrated SOA—without significantly changing applications’ programming language or functional environment. In the long term, full semantic interoperability will be achieved by implementing common EHR standards. In the short term, a level of interoperability can be achieved through an SOA.

Adopt open or common standards and terminologies wherever possible

Designing, selecting and implementing EHR standards and clinical terminologies are complex processes. Even open standards and terminologies often must be customized to reflect organizational, technical and clinical idiosyncrasies and so are subject to a number of organization-specific interpretations. As a result, adopting open standards cannot guarantee interoperability. However, it is likely that governments around the world will continue to push for greater e-health integration to achieve national EHR and will exert pressure on organizations to adopt open and interoperable EHR standards. Therefore, to reduce future costs of EHR integration, organizations should immediately begin implementing—and pressuring vendors to develop—systems based on any available open national or international standards.

Involve clinicians in designing and configuring clinical applications

Applications’ data validation and error-detection rules should reflect real-world logic in terms of understanding of relationships between concepts such as treatments and diagnoses; identifying illogical and inaccurate information using fine-grained parameters; and detecting incomplete data or information that lacks meaning through rules based on clinical and business logic. To achieve this level of intelligent data handling, clinical subject matter experts must be involved in the design and configuration of clinical applications. Even "off-the-shelf" products should be carefully configured to reflect local clinical practices and processes.
Data integrity

Overview

Data integrity refers to the validity, accuracy and reliability of data while it is being stored, transferred, retrieved or processed. Data with integrity retains its meaning and clinical or administrative value after it has been communicated or used. Failure to ensure the integrity of data in e-health systems adversely affects data quality and system flexibility and performance. That, in turn, has a negative impact on patient safety, quality of care, compliance risk and user adoption.

To maintain data integrity, the infrastructure underlying e-health systems should prevent data corruption and data loss. It should also maintain the quality and characteristics of data—format, meaning, rules, relationships and latency—during operations such as storage, retrieval, communication and transfer. Data integrity can be affected by a range of factors, including unauthorized modification of data, poor-quality source code and noninteroperable subsystems. To address these issues, effective information governance architectures must include four components:

- Code integrity
- System hardening
- Interoperability governance
- Standards-driven architecture and standards management

Code integrity

In many cases, data corruption and data loss during storage and use are the result of bugs in source code. Maintaining data integrity requires high-quality source code verified through extensive static code analysis. Code with high levels of integrity has fewer functional defects and security vulnerabilities that may affect data integrity. Ensuring code integrity during the development and unit testing stages reduces costs associated with fixing bugs discovered later in the implementation lifecycle.

System hardening

Ensuring the security of infrastructure underlying e-health systems is important in maintaining the integrity of networks, messages and data. System hardening is a periodic or ongoing process of reducing security risks by evaluating the effectiveness of security architectures, identifying security risks and undertaking security improvements—including removing vulnerable and unnecessary services and applications and updating security configurations and access controls. System hardening is particularly important if systems are currently configured to maximize ease of use rather than security.

Interoperability governance

Enabling subsystems that use different standards and clinical terminologies to share clinical data effectively and maintain data quality is a major challenge. Compounding the challenge is organizational and process issues associated with clinical data sharing. In many cases, providers and physicians use different processes and formats for recording and storing clinical data. Interoperability governance is a function that works across organizational and information silos to develop and enforce common standards, protocols and processes to enable syntactic, semantic or process interoperability (see Figure 1).

Developing effective interfaces and enforcing common standards and communication protocols through standards management processes may enable organizations to achieve a level of syntactic interoperability. Syntactic interoperability enables subsystems to communicate data, but it does not enable receiving systems to interpret, process or use it. Syntactic interoperability limits the benefits of data sharing; manual data entry and modification is required, data quality cannot be ensured, analytics and reporting platforms are less effective, and performance improvements resulting from process automation and optimization cannot be realized.

To ensure data quality and maximize the clinical and administrative value of EHR, systems require semantic interoperability in which subsystems can automatically interpret, process and use data received from other systems. In many cases, a level of semantic interoperability is achieved within enterprises by implementing an “off-the-shelf” EHR that is part of a unified e-health architecture that includes a suite of clinical applications and medical devices. However, achieving semantic interoperability across enterprises is more difficult—mostly because there are no open national or international standards for clinical data.

Current efforts to achieve semantic interoperability across health care organizations involve developing:

- Common reference models for representing clinical data that specify at a high level how information should be recorded, organized and managed in a medical record, such as the openEHR Reference Model and HL7 Clinical Document Architecture
- Standardized clinical data structure definitions that specify restrictions, rules and requirements for data used for specific clinical and administrative purposes such as openEHR Archetypes and HL7 Templates
Process Interoperability
Data created, used or modified in clinical and administrative processes can be used effectively by other processes

Semantic Interoperability
Subsystems can automatically interpret, process and use data received from other systems

Syntactic Interoperability
Subsystems can communicate and exchange data but cannot automatically interpret, process or use information received from other systems

• Common ontologies—that is, models that describe a health-related domain and define the attributes of and relationships between concepts in that domain

• Standardized coding systems for clinical concepts, classifications and clinical terminologies such as SNOMED-CT and LOINC

To maximize the benefits of syntactic and semantic interoperability, clinicians, administrators and researchers must use combined data effectively to improve care quality, identify and realize efficiencies, and improve patient and public health outcomes. This approach requires a level of process interoperability that enables discrete clinical and administrative processes to effectively leverage data produced, used or modified by other processes. For example, clinical terms should be used consistently across organizations to represent exactly the same diagnosis or treatment. Clinical and administrative processes do not have to be standardized, but users must adopt the same data entry and data management standards across enterprises.

Standards-driven architecture and standards management

The most effective way for organizations to achieve interoperability—within and among enterprises—is to develop a system architecture that conforms to open or common messaging, infrastructure, communication, application, data and clinical terminology standards. While there are a range of solutions that enable interoperability in nonstandardized architectures—for example, vocabulary servers and terminology services that enable systems using different terminologies to share information—the most effective means of achieving interoperability is to develop standards-driven architectures.

Within an enterprise, a standards-driven architecture enables organizations to achieve a level of semantic interoperability more efficiently. Standards also increase system flexibility as applications, devices and hardware and software components can be integrated into system architectures more efficiently and effectively. Standards-driven architectures also address some of the critical challenges associated with implementing inter-enterprise EHR. Achieving interoperability across enterprises that have system architectures based on common or open standards, even if those standards vary, is easier than integrating complex, nonstandardized architectures with a number of noninteroperable interfaces.

Developing and enforcing common technical, communication, messaging and data standards is an important step toward a standards driven architecture. A standards management lifecycle should be developed to ensure standards are used and maintained correctly across the organization. This requires standards management processes that monitor and enforce changes and updates to standards, retire standards and ensure that new hardware and software components are standards compliant.

Standards management within enterprises with strong IT governance processes is far easier than across enterprises with discrete IT governance strategies. A critical challenge for organizations implementing inter-enterprise EHR is to coordinate and standardize each enterprise’s standards management strategy. Simply developing standards will not necessarily enable greater interoperability if those standards are not used or maintained uniformly across subsystems.
Recommendations

Maintaining and improving the integrity of data in e-health systems without adversely affecting system flexibility, reliability and performance are complex challenges. However, given the potential impact of low data integrity on care quality, compliance and efficiency, these are challenges organizations should strive to meet. There are a number of strategies, solutions and standards organizations can use as part of a comprehensive data management strategy to improve data integrity. From Accenture’s research and experience with e-health implementations around the world, we recommend the following actions:

Implement effective data integrity checkpoints and edit checks

To maintain data integrity and quality, organizations should develop a library of standard data elements and use data integrity checkpoints and edit checks to ensure data conforms to data standards. Data integrity checkpoints verify that data’s characteristics meet data integrity specifications after it has been created, stored, processed or used. Edit checks enforce data rules and standards and are an important part of data cleansing. They detect and correct, delete or highlight errors, inconsistencies and missing data.

Target process interoperability through comprehensive clinical transformation and process optimization strategies

Organizations often fail to maximize the clinical and administrative value of syntactic or semantic interoperability because clinical and administrative processes and workflows are noninteroperable. In other words, data created, used or modified by discrete processes cannot be used effectively by other processes. Achieving process interoperability requires clinicians and administrators to use applications in the same way for the same purpose, to refer to concepts using the same terms, to use terms consistently and to adopt common data entry practices and rules regarding content, format and frequency of updates. Process interoperability also involves process reengineering to create efficient “touch points” and synergies between processes that enable meaningful, accurate and up-to-date information to flow between processes. To achieve process interoperability, organizations should develop clinical transformation and process optimization strategies, supported by adequate clinical change management programs, to maximize user adoption, encourage desirable user behavior and reengineer clinical processes.

Aim to achieve a level of interoperability that will deliver tangible clinical and administrative benefits by developing specific use cases

Too often, health care organizations invest in interoperability without a set of specific use cases that demonstrate how interoperability will add value by improving clinical decision making, care quality and process efficiency. Without specific use cases, organizations often target an inadequate or unnecessary level of interoperability that either limits the clinical and administrative value of interoperability or needlessly increases the cost of achieving it. In many cases, the most efficient solution is for organizations to target different levels of interoperability across systems, clinical departments and functions depending on specific use cases. This approach enables organizations to concentrate resources on achieving high levels of interoperability in areas where it will deliver the most significant clinical or administrative benefits.
About the Accenture Institute for Health & Public Service Value
The Accenture Institute for Health & Public Service Value is dedicated to promoting high performance in the health care sector and in public service delivery, policy-making and governance. Through research and development initiatives, the Institute aims to help health care and public service organizations deliver better social, economic and health outcomes for the people they serve. Its home page is www.accenture.com/healthpublicservicevalue.

Contacts
Global Lead
Mark Knickrehm
Health Industry Lead
mark.a.knickrehm@accenture.com
+1 310-426-5202

North America
Marylou Bailey
Health Industry Lead
marylou.y.bailey@accenture.com
+1 727-897-4124

Europe, Africa and Latin America
Javier Mur
Health Industry Lead
javier.mur@accenture.com
+34 93-227-1058

Asia-Pacific
Bill Higbie
Health Industry Lead
bill.higbie@accenture.com
+61 3-98388188

Project Team
Andrew Truscott
Accenture Health Practice
Asia-Pacific

Giles Randle
Researcher, Institute for Health and Public Service Value

Julie McQueen
Director of Research, Institute for Health and Public Service Value

Greg Parston
Director, Institute for Health and Public Service Value

About Accenture
Accenture is a global management consulting, technology services and outsourcing company, with more than 190,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world’s most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$21.58 billion for the fiscal year ended Aug. 31, 2009. Its home page is www.accenture.com.

High performance. Delivered.