Information Governance
The Foundation for Effective e-Health
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.

Information governance—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—is the key to ensuring effective and secure e-Health. e-Health practitioners must be aware of critical information governance challenges when planning, designing and implementing systems. Such awareness is crucial to maximizing the clinical and administrative value of EHR and reducing implementation and delivery risk.

By embracing the breadth of information governance, e-health practitioners can develop effective policies, processes and tools that support the enterprise-wide adoption of common information principles. This consolidated approach to information governance enables health care organizations to effectively manage, maintain and control patient information in support of robust patient care.
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 Accenture Information Governance Framework for Health

To address these critical challenges, high-performance health care organizations are developing information governance functions as part of their overall IT governance framework.

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 organisations 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.
This report is part of a series on the Accenture Information Governance Framework for Health which includes an introduction to the framework and five supplementary reports that each discuss one of the five disciplines of information governance: Data Privacy, Data Confidentiality, Data Security, Data Quality and Data Integrity.

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

About Accenture
Accenture is a global management consulting, technology services and outsourcing company, with more than 181,000 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.