As soon as health care providers, third-party payers and consumers get used to conveniently access, download, disseminate, and exchange individual, group, and organizational information through wireless fast-speed Internet connections and other forms of modern digital technology, we can anticipate ongoing and escalating demands for new capabilities in online and e-health care services delivery. One group of such capabilities includes ubiquitous computing and decision support, which is the topic of the opening article in this issue.

Here, Woollatt, Koop, Jones and Warren present a multicriteria framework for middleware technology assessment, with a focus on choosing among wireless handheld devices and ubiquitous decision support architecture. Some of the generic criteria proposed within their framework include security, performance, maintainability, maturity and availability, flexibility, and feasibility. To achieve a desirable middleware technology decision, the authors essentially advocate the use of an initial brainstorming session, followed by a series of iterative scenario-based analyses, taking into account experiences gained from prototyping and field testing of the various technological options. An application of this methodology is also illustrated through the case of a podiatry and diabetes care network. Specifically, the authors argue that performance issues are key considerations in the handheld space, while major changes in the choices of architectural approach are driven chiefly by connectivity concerns and other constraints. Their article closes with a look at future research directions in the area of health informatics standards for wireless handheld and ubiquitous decision support technologies.

With new wireless capabilities come new ways of delivering health care services online. Again, these possibilities will eventually lead to calls among health informatics professionals, researchers, and end-user communities for building and securing better performing wireless networks and improved standards and connectivity for telemedicine and other health computing applications. The second article exemplifies this. Extending the wireless aspect of the expanding digital technology, Chigan and Oberoi focus on the important area of sensor networks, more particularly on how to provide “Quality of Service (QoS) over the wireless channel between the Body Sensor Network (BSN) Gateway and the wireless Access Points (AP).” As wireless sensor network technologies play an increasingly active role in telemedicine, these applications promise to efficiently and effectively transmit the periodic report data and the emergency messages from one location quickly and reliably to another. Yet, unlike the voice and multimedia applications typically supported by traditional QoS techniques, providing sufficient QoS in telemedicine is complex due to the unpredictable nature of emergency data. The authors therefore investigate several alternative schemes for QoS support in telemedicine, and propose an express dual channel (EDC)-based QoS mechanism. Not only is the EDC-based QoS mechanism “simple and resource efficient,” but it also provides
“the bounded maximum delay guarantee for the unpredictable emergency data transmission for telemedicine.” Just as with the other contributors, the authors also close their article with a look at future work.

Not surprisingly, the increasing emphasis on digital technology means it’s time for us to take a fresh look at privacy, security, and confidentiality issues. These topics are now hotly debated in HISI. Accordingly, effective strategies are needed to ensure greater patient data privacy, to maintain the trust and confidentiality among doctor-patient relationships, and to promote a more widely accepted security frameworks for health care computing usage. The next three articles to follow cover the challenges of IS/IT implementation, with particular emphasis on security, privacy, and confidentiality.

First, the Botsis-Syrigos article covers simple, generic, and key challenges faced in many IS/IT implementation experiences. Essentially, their discussions centered on IS/IT implementation challenges within an Oncology unit (Sotiria Hospital, Athens, Greece). A three-module system, comprising the Electronic Patient Records (EPR), the image archive, and the laboratory module, is proposed by the authors. The EPR is simply a database of clinical results, physician orders, and other administrative data. The image archive is essentially a step toward digitizing radiological images while the laboratory module basically stores information about the patient blood samples. As noted, these modules interoperate under strict data security policies. As noted, major benefits gained with the deployment of such a system include improved health care services delivery, end-user satisfaction, and long-term cost savings.

Next, the Medlin-Cazier study, which extends the IS/IT implementation challenges, examines a bag of special issues of growing significance in the age of pervading health digital technologies: password selection, security (cracking and hacking) in relation to password selection, and privacy standards in the context of HIPAA, the Health Insurance Portability and Accountability Act of 1996. Analysis of these passwords has shown a link between the length and strength of a password, as well as the need to train employees on password choices. The authors investigate whether the passwords created by employees of a health care agency followed “strong” or “weak” password practices. Their empirical results indicate the need for more comprehensive password policies and employee training within health care agencies.

Focusing on yet another closely related topic, that of “confidentiality,” is the Lending-Dillon study. This time, instead of studying health care employees in general, the authors study nurses in particular with the aim of gaining insights into their perceptions of “the confidentiality of computerized charts” and “if these perceptions influence nursing self-efficacy.” Results from mailed questionnaire responses just before a hospital-wide IS/IT implementation indicate that nurses “recognize confidential information” and that they “do not think that computerized records are more or less confidential than paper records.” Perceived confidentiality is also found to relate to self-efficacy. Accordingly, the authors argue that as nurses who have “lower self-efficacy also think that the data found in a computer is less confidential and that there is less of a need for confidentiality for computerized data, hospitals should take steps to improve self-efficacy by enhancing confidentiality training.” Altogether, these studies on privacy, confidentiality, and security within various health care organizations and settings show that, in general, health care agencies must take special precautions with their employees, including nurses, when it comes to privacy, security, and confidentiality issues.

Last, but not least, the need for a more robust technology infrastructure to monitor clinical errors, effectively leading to a reduction in adverse drug events, cannot be underestimated in an era of digital technology explosion. This is precisely the topic of our last article: “An Information Technology Architecture for Drug Effectiveness Reporting and Post-Marketing Surveillance.” Here, Gupta, Woosley, Crk, and Samikar propose an IT architecture for initiating a tracking of adverse drug events in an outpatient setting as part of the post marketing surveillance program to reduce such costly events. Technologically, the architecture will support the deployment of a Web-based drug effectiveness reporting and tracking system that “builds on previous studies analyzing the involvement of community pharmacies in identifying and reporting adverse drug events.” The article also
details major requirements of such a tracking and reporting system, suggest the critical factors that may affect system implementation success and use, and recommend IS/IT solutions that meet these requirements.

Altogether, the articles appearing in the current IJHISI issue are concerned with the study of key HISI issues during this period of health digital technology revolution.

Joseph Tan holds a professional diploma in civil engineering from Singapore Polytechnic, an undergraduate degree in mathematics and computer science from Wartburg College, IA, a master’s degree in industrial & management engineering from the University of Iowa, and a PhD in management information systems from the University of British Columbia (UBC). He has been a tenured associate professor, teaching in the Department of HealthCare & Epidemiology, UBC, for many years prior to serving as a professor and head of the Information System and Manufacturing (ISM) Department, School of Business, Wayne State University. Professor Tan publishes widely in numerous computing, ergonomics, information systems, health education, e-health, and e-business journals and has served as a guest editor and member of various journal editorial boards. He sits on key organizing committees for local, national, and international meetings and conferences. Professor Tan’s research, which has enjoyed significant support in the last several years from local, national, and international funding agencies and other sources, has also been widely cited and applied across a number of major disciplines, including healthcare informatics and clinical decision support, human processing of graphical representations, ergonomics, telehealth, mobile health, and e-health promotion programming.