

How Nursing Informatics Are Used In Clinical Practice

Posted on September 5, 2019

This course provides a broad understanding of how nursing informatics supports clinical practice, professional judgment, project management, virtual learning, advanced nursing roles, and the safe use of personal devices in healthcare. The original reflection correctly emphasizes electronic health records, the Technology Informatics Guiding Education Reform initiative, the TANIC self-assessment, and cybersecurity concerns associated with bring-your-own-device programs. These subjects remain essential, but nursing informatics is broader than computer competence. It involves the disciplined use of data, information, knowledge, technology, and workflow to improve care. Informatics tools can make information available quickly, but they can also introduce copied errors, alert fatigue, privacy breaches, downtime, and automation bias. The nurse remains responsible for verifying information and applying professional judgment. (McGonigle & Mastrian, 2022)

Nursing Informatics

Nursing informatics integrates nursing science with information and analytical sciences. It supports the collection, organization, communication, and use of clinical information. Nurses contribute data every time they record vital signs, symptoms, interventions, education, medication administration, or patient response. These entries later influence handoffs, decisions, quality measurement, reimbursement, research, and public-health reporting. Informatics competency therefore includes understanding how one documentation choice affects people and systems beyond the immediate shift.

Data, Information, Knowledge, and Wisdom

A common informatics framework distinguishes data, information, knowledge, and wisdom. A temperature of 39°C is data. Recognizing that it is elevated and increasing over time creates information. Connecting the trend with the patient's condition and evidence about infection creates knowledge. Deciding to reassess, obtain cultures as ordered, notify the provider, and monitor for deterioration requires clinical wisdom. Technology can organize and display data, but it cannot assume full responsibility for the meaning of the patient's condition.

Electronic Health Records

EHRs allow authorized professionals to review histories, medications, laboratory results, imaging, allergies, plans, and prior encounters. They can reduce illegible handwriting and make information available across locations. They can also produce excessive documentation, confusing templates, duplicate records, and copied statements that no longer describe the patient. Nurses should verify imported information, document changes promptly, and avoid selecting default answers without assessment. The record is a communication tool, not merely proof that a task was completed.

Documentation Quality

Good documentation is accurate, timely, objective, relevant, and patient-specific. A statement such as “patient fine” gives little information. A stronger entry describes observable status, intervention, response, and communication. Nurses should avoid stigmatizing labels, unsupported conclusions, or unnecessary details about a patient’s private life. Corrections must preserve the audit trail according to policy. Delayed documentation should be identified honestly rather than entered as if it occurred in real time.

Professional Judgment and Technology

Nursing judgment and informatics are complementary. A decision-support alert may warn about an allergy, but the nurse must confirm the patient, drug, reaction, and current order. A risk score may identify deterioration, but a bedside observation can reveal urgent change before the score updates. Conversely, a nurse’s impression can be strengthened or corrected by trends that are difficult to remember. Safe practice uses technology as an additional source of evidence while preserving assessment, critical thinking, and escalation.

Clinical Decision Support

Clinical decision-support systems provide alerts, reminders, predictive scores, care pathways, and evidence links. They can support vaccination, fall prevention, medication safety, and early recognition of sepsis or deterioration. Too many low-value alerts can create alert fatigue. Staff may override important warnings because irrelevant alerts have trained them to click automatically. Organizations should monitor alert performance, false positives, overrides, workflow burden, and patient outcomes. Nurses should report unsafe alerts rather than silently work around them.

Barcode Medication Administration

Barcode systems can help verify patient identity and medication details. Their protection depends on accurate wristbands, pharmacy data, scanners, and workflow. Scanning another patient's band, carrying duplicate labels, or bypassing a damaged barcode can defeat the system. A successful scan also does not answer whether the medication is clinically appropriate given blood pressure, laboratory values, symptoms, allergies, or recent changes. The nurse must still perform required clinical checks.

Smart Pumps and Connected Devices

Smart infusion pumps use drug libraries and dose limits to reduce programming errors. Bedside monitors, glucose devices, ventilators, and other equipment may transmit information to the EHR. Connectivity saves time but can create mismatched patients, delayed transmission, duplicate values, or cybersecurity vulnerabilities. Nurses need to understand which information transfers automatically, which requires validation, and what to do when device data conflict with the patient's condition.

Interoperability

Interoperability means that systems can exchange and meaningfully use information. A scanned document may be visible but not searchable or available to decision support. Standardized terminology and data formats improve exchange across hospitals, clinics, pharmacies, laboratories, and public-health agencies. Nurses encounter interoperability failures during admission, transfer, medication reconciliation, and discharge. Reporting these failures contributes to system improvement because frontline work reveals where information stops following the patient.

Health Information Exchange

Health information exchanges can provide data from other organizations, reducing duplicate tests and incomplete histories. External records may be outdated, duplicated, or associated with the wrong person. Critical information should be verified with the patient, current provider, or source where appropriate. Access must follow authorization and privacy rules. The existence of a regional exchange does not mean every clinician may search any person out of curiosity.

Patient Portals

Portals allow patients to view results, request appointments, communicate, and review instructions. They can strengthen engagement and allow patients to identify errors. Some results may appear before a clinician has provided context, causing confusion. Not every patient has broadband, a device,

language access, disability accommodation, or digital confidence. Nurses can teach portal use while ensuring that patients have alternative communication methods. Messages describing urgent symptoms should be redirected to timely care rather than left in a routine inbox.

Telehealth

Telehealth can support follow-up, chronic-disease care, education, triage, and access for remote patients. Nurses need skills in identity verification, privacy, consent, camera use, remote assessment, documentation, and emergency planning. A virtual encounter cannot reproduce every physical assessment. The nurse must recognize when symptoms require in-person or emergency evaluation. Telehealth quality should be measured through outcomes and access, not the number of completed video calls.

Virtual Learning Environments

A virtual learning environment can provide simulations, discussion, case analysis, quizzes, and collaborative projects. It supports flexible learning but requires organization, accessibility, and active participation. Online completion does not prove competence in clinical work. Students need opportunities to practice documentation, communication, device use, and safety decisions in realistic scenarios. Faculty feedback should connect virtual exercises with actual nursing responsibilities.

TIGER and Informatics Competencies

The TIGER initiative helped articulate informatics competencies for nurses, including basic computer skill, information literacy, and clinical information management. Its lasting contribution is the view that informatics belongs throughout nursing education. A graduate should be able to locate evidence, use systems safely, communicate through approved channels, protect information, and participate in improvement. Digital familiarity from social media does not automatically create clinical competence. (American Association of Colleges of Nursing, 2021; Collins, 2016)

TANIC Self-Assessment

The TANIC tool can help nurses assess perceived informatics competence. It may reveal confidence in documentation but uncertainty about data analysis, privacy, or system implementation. Self-assessment is useful for setting goals, but confidence can differ from performance. A person may feel highly skilled while using unsafe workarounds. TANIC results should be combined with simulation, observation, feedback, and evidence of practice. Reassessment can show change after education.

Information Literacy

Nurses need to identify an information need, search effectively, judge source quality, and apply evidence to a patient. A search-engine result, promotional site, and clinical guideline do not carry equal authority. The nurse should consider date, population, study design, conflicts, and fit with patient values. Generative AI can produce fluent but incorrect summaries and invented citations. Every clinical claim must be checked against reliable sources before use.

Data Quality

Quality reports are only as reliable as the data collected. Inconsistent definitions, missing fields, duplicate patients, and copy-forward errors can distort performance. A dashboard may show fewer falls because events were not documented. Organizations should explain why data matter, reduce unnecessary fields, and validate measures. Nurses should be able to report when a required option does not represent the patient rather than choosing an inaccurate category merely to close the screen.

Analytics and Quality Improvement

Data can reveal patterns in infections, pressure injuries, readmissions, delays, and medication errors. A pattern does not explain its cause. Teams need chart review, process observation, staff input, and patient experience. Results should be stratified carefully to identify disparities without stigmatizing groups. Quality improvement uses data to test changes, but research and operational improvement have different oversight requirements. Nurses should understand when additional ethical review is required.

Artificial Intelligence

AI tools may support documentation, imaging, risk prediction, scheduling, and patient communication. They can reproduce bias, hallucinate facts, or perform poorly in populations absent from training data. A generated note may contain a plausible event that never occurred. Nurses should use only approved tools, protect patient information, and review output before it enters a record. Automation should not make responsibility disappear. Organizations need governance for validation, monitoring, consent, and correction.

Project Management in Nursing

Project management supports implementation of EHR modules, clinical pathways, device programs, and quality initiatives. The process includes defining scope, stakeholders, requirements, risks, timeline, resources, communication, testing, training, deployment, and evaluation. The original essay identifies planning, monitoring, implementation, and evaluation. These stages should be connected with change management and frontline participation. A project delivered on schedule can still fail if staff cannot use it safely.

The Advanced Practice Nurse as Project Leader

Advanced practice nurses understand clinical problems and can translate between patients, clinicians, administrators, analysts, and vendors. They may sponsor changes, define requirements, test workflows, interpret data, and evaluate outcomes. Leadership does not mean making every technical decision alone. Effective APNs build interdisciplinary teams, clarify authority, manage conflict, and keep patient outcomes at the center. They also know when legal, cybersecurity, informatics, or engineering expertise is required.

Stakeholder Engagement

Technology projects often fail when designers consult users only after purchase. Nurses, physicians, pharmacists, patients, registration staff, privacy officers, and technical teams may experience the same system differently. Early engagement identifies unintended consequences. Staff should be able to test prototypes and report problems without being labeled resistant to change. Resistance may reveal legitimate safety, workload, or ethical concerns.

Change Management

Implementation changes roles and identity, not only software. Staff need a clear reason for change, training, practice time, local support, and feedback. Leaders should identify super-users without making them responsible for every problem. Training must reflect real tasks and continue after launch. Evaluation should examine workarounds, time, errors, user experience, and patient outcomes. A “successful go-live” is the beginning of improvement, not its end.

BYOD in Healthcare

[Bring-your-own-device](#) programs allow staff to use personally owned phones, tablets, or laptops for authorized work. Benefits may include familiarity, mobility, and reduced equipment purchase. Risks

include lost devices, shared family access, insecure applications, local storage, unpatched software, and mixing personal with clinical communication. BYOD is not safe simply because employees sign a policy. It requires technical controls, support, and a decision about which tasks should never occur on personal devices.

Mobile Device Management

Mobile device management can require encryption, screen lock, approved applications, security updates, separation of work data, remote removal of organizational data, and detection of compromised devices. The organization should explain what it can view or erase so employees understand privacy implications. Remote wipe should be designed carefully to avoid destroying personal data unnecessarily. Devices that cannot meet minimum controls should not connect to clinical systems. (National Institute of Standards and Technology, 2023)

Secure Communication

Ordinary text messages and personal email may lack required security, retention, identity, and audit features. Staff should use approved clinical messaging. A secure application still requires recipient verification and appropriate content. Photographs should be taken only for a legitimate purpose with authorization and stored in approved systems rather than personal galleries or cloud backups. Deleting a photo from the phone may not remove every copy.

HIPAA and the Minimum Necessary Principle

HIPAA protects identifiable health information held by covered entities and business associates, with rules for permitted use and disclosure. Nurses should access only information needed for their role. “I work at the hospital” is not permission to view the record of a relative, coworker, neighbor, or public figure. Emergencies and treatment create legitimate access, but curiosity does not. Organizations use audit logs to identify inappropriate viewing.

Cybersecurity Threats

Healthcare faces phishing, ransomware, credential theft, insecure devices, and supply-chain attacks. Nurses can reduce risk by using unique credentials, multifactor authentication, verified links, rapid reporting, and approved storage. Cybersecurity should not rely entirely on individual vigilance. Systems must be designed to reduce dangerous clicks, limit privileges, segment networks, maintain backups, and support rapid recovery. Staff who report a mistake promptly should be encouraged because delay increases harm.

Downtime Preparedness

Power loss, maintenance, cyberattack, or network failure can interrupt clinical systems. Nurses need accessible downtime procedures for identification, orders, medication administration, documentation, laboratory results, and communication. Paper records created during downtime must later be reconciled accurately. Drills reveal whether forms, contact numbers, labels, and roles are available. An organization dependent on technology must plan for safe care without it.

Privacy and Ethics

Informatics raises ethical questions about consent, secondary data use, surveillance, bias, and patient access. A technically legal data use may still damage trust if patients do not expect it. Nurses should participate in governance because they understand how information reflects vulnerable moments. Patient data should not be treated merely as a commercial resource. Benefit, risk, fairness, transparency, and confidentiality should guide decisions.

My Development Plan

I will improve my informatics competence through measurable activities. I will practice concise EHR documentation and request feedback, use approved databases for evidence, review privacy and downtime policy, and learn how decision support and medication technology are validated. I will complete cybersecurity training and avoid personal communication channels for patient information. I will participate in simulation or a quality project, then repeat TANIC and compare self-perception with observed performance. My goal is not just to use technology faster but to use it safely and critically.

Conclusion

Nursing informatics supports clinical communication, decision-making, education, project management, and quality improvement. EHRs, portals, telehealth, devices, analytics, and AI can improve care only when information is accurate and workflows are safe. Professional nursing judgment remains essential because technology can be incomplete or wrong. TIGER and TANIC provide useful competency frameworks, while BYOD requires policy, encryption, mobile management, secure messaging, and privacy protection. Advanced nurses can lead technology projects by connecting system design with patient care. Informatics is therefore not separate from nursing practice; it is one of the environments in which modern nursing responsibility is exercised.

References

American Association of Colleges of Nursing. (2021). *The essentials: Core competencies for professional nursing education*.

Collins, S. (2016). Nursing informatics competencies: Psychometric validation and dissemination of a self-assessment tool. In *Nursing informatics*.

McGonigle, D., & Mastrian, K. G. (2022). *Nursing informatics and the foundation of knowledge* (5th ed.). Jones & Bartlett Learning.

National Institute of Standards and Technology. (2023). *Guidelines for managing the security of mobile devices in the enterprise* (SP 800-124 Rev. 2).

U.S. Department of Health and Human Services. (2026). *Health information privacy and security guidance*.