Healthcare

VANTAGE POINT®

A Healthcare Risk Management Resource | 2024 Issue 2

Telemedicine Update: Coordinating Remote and In-person Care

The delivery of remote healthcare services via telecommunications technology has grown exponentially in recent years. According to the Centers for Disease Control and Prevention, about 23 percent of patients/residents/clients utilized some form of telemedical service by late 2022, up from 5 percent prior to the pandemic. As remote care gains acceptance, the telemedicine market – valued at $87 billion in 2022 – is predicted to reach $286 billion by 2030. (See "A Snapshot of User Demographics and Service Characteristics" on page 2 for additional insights into market patterns and trends.)

As the technology evolves, so too does the language used to describe digitally enabled care, with different settings and providers using their own distinct terminology to describe the various services available. This article divides the wide range of remote healthcare options into the following three categories:

- **Telemedicine** refers to systems that enable the virtual exchange of medical information and/or delivery of clinical care, generally between the patient/resident/client and medical providers. Common telemedical services include specialty consultation, diagnostic testing, and various types of treatment or therapy.
- **Telehealth** encompasses a range of remote healthcare services outside of direct consultation or communication with healthcare providers. One common telehealth technology entails the use of body sensors or wearables to monitor a patient's/resident's/client's health status, while other applications provide compliance reminders, offer educational support or troubleshoot issues associated with chronic care maintenance.

In this issue…

- **Telecare,** also referred to as eHealth, extends beyond the patient/resident/client-provider relationship, encompassing certain direct-to-consumer technologies – such as home testing kits, novel mental health tools and software platforms – that enable individuals to address health concerns while circumventing traditional healthcare providers, organizations and intermediaries. While eHealth is a burgeoning field, it is not without attendant risks, some of which are discussed on page 7.

…about **23 percent of patients/residents/clients utilized** some form of **telemedical service by late 2022**, up from 5 percent prior to the pandemic.

Although remote care offers many advantages in terms of convenience, efficiency and expanded access, it does have its limitations and risks. If misused, telemedicine can lead to fragmented care delivery, weakening of the patient/resident/client-provider relationship, lack of follow-up and increased liability exposure. (See "Remote Care: A Balancing Act" on page 3.) In order to help organizational leaders and providers offset these hazards and realize the full potential of these technologies, this edition of *Vantage Point*® offers a basic guide to common uses and associated risks of remote care, along with guidance and information on a variety of issues, ranging from standard of care, clinical assessment, mental health treatment and provider accountability to recordkeeping and communication practices. Also included are suggestions for safeguarding the transfer of protected health information (PHI), as well as updates on regulatory, legal and policy matters.

Please note that this edition is intended to serve as a companion piece to two earlier CNA publications:

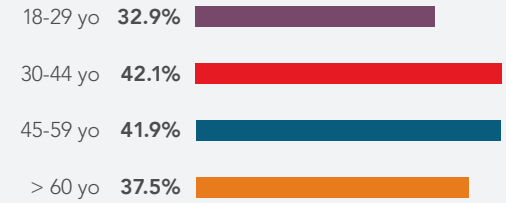
- *Vantage Point*® 2021-Issue 2, "Telemedicine: A Brief Guide to the Emerging Risks of Remote Care" and
- *AlertBulletin*® 2023-Issue 4, "Remote Patient Monitoring: Five Basic Risk-reduction Strategies."

Readers are encouraged to consult both publications for a thorough review of relevant risk exposures and countermeasures.

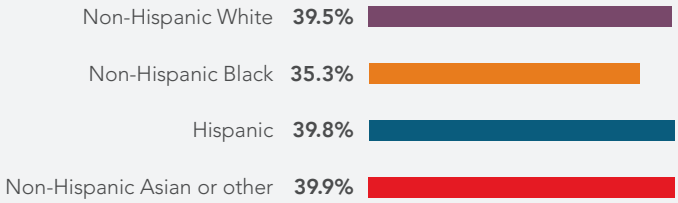
A Snapshot of User Demographics and Service Characteristics

The following graphics present data from a cross-sectional secondary analysis of the 2022 Health Information National Trends Survey, which was conducted by the National Cancer Institute between March and November 2022, and involved 5,317 respondents. (See Raj. M. and Iott, B. "Characterizing Telehealth Use in the US: Analysis of the 2022 Health Information National Trends Survey." *The American Journal of Managed Care*, January 12, 2024, volume 30:1.)

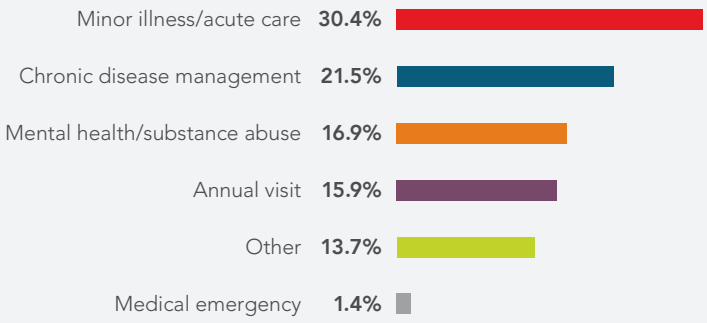
Age Category by User Percentage



Race and Ethnicity by User Percentage

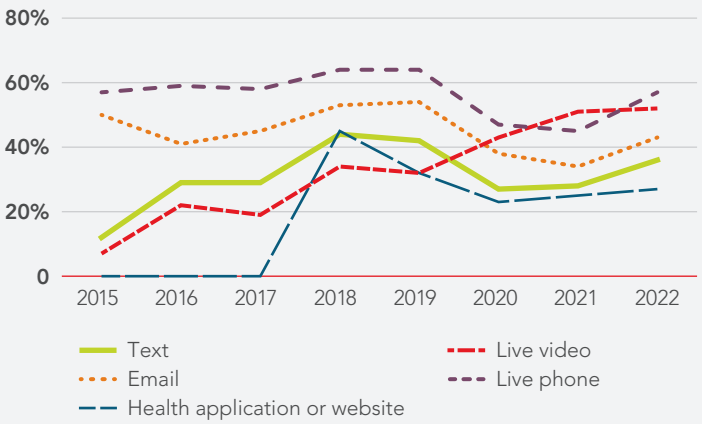


Reason for Service by Percentage



Modality Choice from 2015-2022

Source: Stewart, C. "Use of Telemedicine in the U.S. 2015-2022, by Channel." Posted on the Statista website, March 14, 2023.



Remote Care: A Balancing Act

Advantages	Disadvantages
• Improved levels of satisfaction among patients/residents/clients, due to greater convenience and flexibility. • Greater continuity of care with respect to chronic conditions. • Enhanced access to primary and secondary care. • Broader access to specialists in rural areas. • Diminished exposure to healthcare-related airborne infections. • Lower healthcare costs overall.	• Reduced patient/resident/client-provider connection, rapport and trust. • Diagnostic lapses due to lack of hands-on examinations, insufficient laboratory data and/or low-quality images. • Privacy concerns associated with data security breaches. • Challenges in safely accessing electronic healthcare records. • Expense of upgrading IT infrastructure and training staff. • Patients'/residents'/clients' potential lack of access to high-speed Internet, a prerequisite for many telehealth services.

Maintaining Quality of Care

If mishandled, remote care may disrupt traditional patient/resident/client-centric delivery models, potentially resulting in less safe and effective care. To ensure that providers adhere to the same standard of care for both remote and in-person encounters, it is essential to create sound policies governing virtual care processes and to communicate these policies to all providers and staff. Protocols should encompass the following key areas, among others:

Standard of care. The same performance expectations apply whether the patient/resident/client is in the presence of the provider or is attended to remotely. Regardless of advances in technology, providers should be mindful of the fact that telemedicine is merely an extension of traditional forms of care and does not alter professional or ethical standards or duties. Failure to uphold these standards may endanger patients/residents/clients, potentially resulting in liability exposure.

Patient selection. Providers must determine whether telemedicine is appropriate for the encounter or if an in-person visit is needed, based upon the patient's/resident's/client's history, acuity and clinical presentation. Formal selection criteria should be established, taking into consideration not only medical factors, but also Internet access and computer skills. Once the decision is made to proceed with remote care, according to the American Telemedicine Association, "It should be the responsibility of the provider to escalate to a higher level of care (or otherwise initiate appropriate recommendations) when medically indicated or necessary for patient safety."

The following guidelines are designed to help minimize risk by clarifying whether virtual care is an appropriate choice and communicating risks and limitations to patients/residents/clients:

- **Ask whether proposed remote care services comply with the legally expected standard of care** in the relevant field of practice.
- **Undertake a comprehensive risk-benefit analysis** of each proposed procedure or treatment before proceeding with any remote care activity.
- **Explain to patients/residents/clients why virtual services are a valid option,** note any inherent limitations, and document discussion in the healthcare information record.
- **When necessary, explain to patients/residents/clients why a face-to-face encounter is necessary,** in light of assessment findings and acuity level.
- **Acknowledge that certain clinical presentations may require referral to a specialist.** Convey to patients/residents/clients how the referral process works and explain why it is vital for them to see the specialist.
- **Emphasize that it may be necessary for the provider to end a virtual visit prematurely** and direct the patient/resident/client to seek in-person or emergency care.

Clinical assessment. Virtual physical assessments have innate limitations, obliging providers to consider what information they can and cannot accurately obtain from a remote examination, as well as whether the patients/residents/clients in question are capable of fully participating in the process. As traditional physical examination techniques, such as abdominal exams, are not possible, alternative methods must be used. Educational resources relating to remote physical examination are available from Stanford Medicine and the U.S Department of Health and Human Services, among other published resources.

The following measures can help strengthen the remote assessment process and reduce the risk of misdiagnosis:

- **Instruct patients/residents/clients to complete self-assessment questionnaires** specific to the presenting clinical condition, focusing on the history of the complaint and associated symptomatology.
- **Have medical assistants complete a pre-visit checklist** to ensure that patients/residents/clients are capable of using equipment needed to record vital signs and other baseline measurements.

- **Indicate that findings are "self-reported" whenever vital signs are relayed by patients/residents/clients,** or when subjective comments cannot be corroborated through virtual means.
- **Request that patients/residents/clients reveal affected body parts to the camera,** with the assistance of family members and/or caregivers, if needed.
- **Clearly identify which assessment steps were completed by the patient/resident/client,** such as palpation of the abdomen or lymph nodes.
- **If applicable, refer to any relevant pre-visit health data** gathered via a wearable device.

Mental health treatment. The COVID-19 pandemic prompted a dramatic shift to remote assessment in the behavioral health field, creating a need for guidance on detecting and managing suicidal ideation in the virtual environment. From a risk control perspective, consider implementing the following mental health assessment protocols, at a minimum:

- **Identify sources of support** – such as family members, friends or community organizations – in the virtual care record and obtain authorization to share information with these contacts, if needed.
- **Formulate a plan to re-establish contact** in the event telephone or on-screen connection is interrupted.
- **Using patient/resident/client portals, send online pre-visit questionnaires to screen for suicidal ideation and self-harm behaviors,** and require providers to administer questionnaires to those who cannot complete such a form online.
- **In the questionnaire, ask patients/residents/clients whether they have access to weapons** or have thought about harming themselves or others, and document the response.
- **Have a set response plan in place** – including automated alerts to staff and providers – should the screening questionnaire indicate possible suicide risk.
- **Review questionnaires promptly;** if they cannot be read immediately, issue a disclaimer statement to that effect to the patient/resident/client.
- **Provide patients/residents/clients with contact information for emergency resources,** including 988 for access to the national suicide prevention lifeline and 911 for urgent intervention, as well as the phone numbers for local mental health crisis lines and support services.

Protocols and training should also include guidelines for responding to online behavioral health emergencies. Common indicators include failure to keep a scheduled appointment, abrupt visit cutoffs, and urgent requests for in-person treatment or care. The organization's or practice's crisis prevention and response plan should direct providers and mental health workers to take the following actions, among others, in emergency situations:

- **Activate the telephone or instant messaging alert system** to notify other providers or consultants.
- **Determine the patient's/resident's/client's location** and document it in the healthcare information record.
- **Summon EMS providers,** law enforcement agencies or mobile crisis units to the location.
- **Maintain the remote link with the patient/resident/client** and continue to assess suicidal ideation and behaviors, documenting all interventions until crisis providers take over.

IT considerations. While virtual care platforms are designed to enable remote care, the inherent limitations of digital interactions can give rise to fragmentation of care, especially when providers rely upon limited information when making diagnostic- and treatment-related decisions. Therefore, when adopting a virtual care platform, consideration should be given to features that enable access to a wide range of clinical data, including laboratory and diagnostic imaging results, consultations and the clinical interpretations of other providers.

It is not unusual for individuals living in aging services settings or undergoing chronic care management to have multiple virtual care providers who are not in direct communication with each other. To enhance coordination of care, select vendors who offer user-friendly solutions that facilitate information exchange among disparate providers and settings, as well as accommodate both digital and in-person visits.

Recordkeeping. A well-documented record of virtual care can be the single most effective means of integrating remote services and maintaining continuity. While documentation requirements vary, the following items, among others, should be included in any record of remote care:

- **The patient's/resident's/client's identity,** as verified through a valid ID.
- **Pertinent history** and information used to make treatment decisions.
- **The patient's/resident's/client's geographic location**, as well as the provider's setting, e.g., "in the office."

- **An evaluation of the patient's/resident's/client's suitability for remote interaction,** e.g., "patient displays adequate digital literacy skills and can connect via a personal laptop."
- **The telemedicine modality used,** e.g., "secure interactive audio-visual visit via the resident portal."
- **The names of other individuals present on both sides of the remote contact,** as well as interpreters.
- **A signed informed consent form,** which is adapted to telehealth services.
- **Instructions regarding follow-up and referral,** as well as any discussion with the supervising physician.

(For a comprehensive checklist of virtual care record requirements, see *Vantage Point*® 2021-Issue 2, "Telemedicine: A Brief Guide to the Emerging Risks of Remote Care.")

Service disclaimers. A telehealth-specific service disclaimer can help mitigate the risks associated with remote care. Such a statement, read and signed by the patient/resident/client, should include the following notifications, among others:

- The standard of care rendered is equal to an in-person visit.
- The provider reserves the right to request an in-person appointment.
- Medical advice, diagnosis and treatment decisions may be affected by factors not within the provider's control, such as incomplete or inaccurate data supplied by the patient/resident/client, and/or poor transmission of diagnostic images.
- Any urgent medical symptoms or conditions that arise before, during or after a session should be treated in the nearest urgent care or emergency setting.

Staying Abreast of Telehealth Regulation, Law and Policy

As telehealth guidance and regulation are in a state of flux post-pandemic, it is important to check regularly for changes in state and federal laws governing remote healthcare provision. The diagram below summarizes certain key areas of remote care-related regulation at both the state and federal level. It includes links to relevant resources to help providers and administrators stay current on the latest directives in this rapidly evolving field.

Federal

CMS Medicare Waivers
The COVID-19 public health emergency officially ended in May 2023. The Consolidated Appropriations Act of 2023 (i.e., Act) extends some pandemic-era waivers related to remote-based care for Medicare beneficiaries through December 31, 2024. The Act also ensures that some pandemic-related flexibilities will be made permanent for Medicare patients/residents/clients.

Controlled Substances
In regard to online prescription of controlled substances (CS), see "Second Temporary Extension of COVID-19 Telemedicine Flexibilities for Prescription of Controlled Medications," in the *Federal Register*. See also 42 CFR Part 8 Final Rule with respect to online prescription of CS in opioid treatment programs.

Data Privacy
HIPAA does not specifically address telemedical services. For guidance on data privacy and telehealth, visit the U.S. Department of Health and Human Services webpage.

Data Tracking
For the latest directives concerning impermissible disclosures of PHI to tracking technology vendors, see FTC and OCR Stress (Again) the Importance of How Health Data is Handled, issued by the Center for Connected Health Policy, September 2023.

State

Medicaid and Private Pay
The termination of the public health emergency in 2023 resulted in a flurry of legislative activity at the state level regarding Medicaid reimbursement, the status of private payer reimbursement and coverage parity laws, which require payers to cover any telehealth service if it meets the standard of care and would be covered if delivered in person. To monitor ongoing legislative updates, visit the website of the Center for Connected Health Policy.

Licensure
Licensure regulation continues to evolve at the state level. For an interactive map of specific state licensing conditions, see Cross-State Licensing issued by the Center for Connected Health Policy.

Prescribing
Individual states regulate the prescribing of uncontrolled substances. For specific state requirements, see Online Prescribing, an interactive map from the Center for Connected Health Policy.

A Review of Delivery Modes, Uses and Safeguards

Organizations can significantly minimize their exposure to remote care-related risks by understanding the basic delivery modes, their uses and safeguards.

Basic Delivery Modes

Real-time Audio and Video
Live exchange between patients/residents/clients and healthcare providers via a mobile device or computer that enables virtual care visits, case collaboration and remote education.

Remote Monitoring
Collection and delivery of physiological data via wireless wearable or implantable devices, in order to monitor and evaluate chronic conditions, acute presentations and higher-risk patients/residents/clients.

Store and Forward
Asynchronous delivery of health information via video, email, text or portal messaging. This mode is particularly useful when diagnostic images, photos, healthcare records and lab results are used in remote diagnosis, or to facilitate collaboration of care.

Common Telehealth Uses

Types of Services
- Conducting real-time visits between providers and patients/residents/clients for consultative, diagnostic or treatment purposes.
- Linking patients/residents/clients to providers for non-acute conditions.
- Providing virtual bedside nursing.
- Taking and sharing photos, images or videos of physical conditions or diagnostic work up.
- Direct messaging with a provider on inquiries.
- Receiving digital reminders about screenings, appointments and prescription refills.
- Maintaining care for chronic conditions.
- Providing patient/resident/client education, such as how to use medical devices.
- Monitoring of vital signs and clinical data.
- Facilitating patient/resident/client access to electronic health records.

Types of Visits
- Interactions in which patients/residents/clients obtain referrals, prescriptions or diagnostic test results.
- Physical or occupational therapy.
- Individual or group psychotherapy.
- Some urgent or emergent care.
- Wellness visits and preventive education.
- Nutrition counseling.
- Fertility counseling.
- Prescription management.
- Wound observation.
- Post-surgical follow-up.
- Follow-up appointments.

Common Conditions
- Headaches or migraines.
- Recurring conditions, such as urinary tract infections, colds and influenza.
- Chronic pain.
- Diabetes, COPD and other chronic conditions.
- Colds and influenza.
- Skin conditions, such as acne, rashes and pressure injuries.
- Musculoskeletal conditions and injuries.
- Mental health disorders, such as anxiety or depression.
- Gastrointestinal symptoms, such as nausea, vomiting, diarrhea and constipation.

Safety Measures

Data Privacy
- Maintain compliance with HIPAA requirements regarding data security and protection.
- Outline vendor roles and responsibilities in business associate agreements, including appropriate uses and disclosures of PHI.
- Discuss the potential for privacy and security risks during patient/resident/client encounters, and include risk disclosure as part of the informed consent process.
- At the outset of every session, confirm the identities of patients/residents/clients and any other person present.
- Periodically delete files from all mobile devices after information has been transferred to healthcare information records.
- Utilize data backup and recovery processes in case of a known breach.

Cyber Security
- Conduct routine security assessments of the telehealth platform, including the presence of security features, e.g., user authentication, data encryption, data management controls.
- Minimize unauthorized access by creating unique user identification numbers, designing password-protected platforms and establishing automatic log-off times.
- Educate providers about remote work policies, including permitted forms of access and personal device security measures.
- Train providers to detect common cyberattack techniques, such as phishing.
- Regularly maintain operating systems and stay current with antivirus security updates.
- Audit data activities to identify unauthorized users and detect careless behaviors.
- Remotely disable IT devices in the event of loss or theft.

Vendor Due Diligence
- Develop vendor evaluation criteria. (See Selecting a Vendor Guide from the American Medical Association.)
- Thoroughly research vendors and schedule live or virtual demonstrations of the product.
- Test platforms with select user groups.
- Evaluate the strength of platforms' privacy and encryption capabilities prior to purchase.
- Install a virtual private network with software patches and security configurations.
- Review consumer feedback for existing platforms and network with providers and organizations that currently use the platform.
- Conduct periodic testing to ensure adequate bandwidth.
- Execute written contracts that align provider and vendor expectations, hold each party accountable for the delivery of care and indemnify parties, where appropriate.

eHealth Exposures and Risk Management Considerations

eHealth Exposures

When vendors, providers and organizations fail to mutually monitor eHealth platforms for quality control and safety features, they open themselves to a wide range of allegations, including the following:

- **Inaccurate patient/resident/client identification** with potential for fraud.
- **Data breaches** from unprotected recordkeeping practices.
- **Inadequate oversight** of providers.
- **Over-reliance on patient/resident/client input** for historical data.
- **Clinical limitations** in digital diagnosis and treatment.
- **Treatment plans that are inadequate** or not current.
- **Poor follow-up,** including missed encounters.
- **Unlawful prescription** of addictive medications.
- **Antibiotic misuse** or overuse.
- **Infection transmission** via touch screens in multi-user kiosks.
- **Lack of digital literacy** and skills on the part of users.
- **False advertising,** i.e., misleading claims.

Direct-to-consumer platforms are proliferating both online and in the form of kiosks located in emergency rooms, ambulatory care settings, pharmacies, retail establishments, schools and workplaces. Service offerings run the gamut from routine diagnostics and treatment, procedure follow-up and medication management to chronic disease maintenance and automation of routine services, including admission, discharge, appointment scheduling and check-in.

The quality of care and safety standards that govern vendor arrangements in brick-and-mortar settings also apply to eHealth platforms and interactive kiosks. However, eHealth encounters tend to be episodic in nature, leaving providers with little history of patients/residents/clients and no practical framework within which to work. Furthermore, many technology vendors view themselves as data aggregators, shifting the responsibility of care to partner organizations and providers.

It is vitally important that vendor agreements accurately reflect the obligations and expectations of all parties, delineating duties owed to the patient/resident/client by each partner and specifying the designated "provider of record." For example, the vendor may be responsible for processing and reporting intake forms and questionnaires, while the provider is obligated to schedule follow-up consultations or evaluations.

The following risk management suggestions are intended to improve the safety and quality of eHealth interfaces:

- **Install log-on controls,** such as user identification numbers and passcodes, since most eHealth platforms permit users to initiate interactions without first obtaining network privileges.
- **Via a screen disclaimer, disclose to patients/residents/clients whether a licensed provider is delivering services** or an unlicensed individual who is supervised by a licensed provider.
- **Obtain informed consent from the patient/resident/client,** including risks, benefits and alternatives to the proposed service, as well as the risk of data compromise due to cyber threats.
- **Ensure that eHealth platforms include a computer-administered history-taking system,** requiring the user to select a chief complaint and respond to multiple-choice questions regarding signs and symptoms.
- **Maintain up-to-date business associate agreements with technology vendors** and closely monitor the exchange of health information to ensure compliance with HIPAA privacy provisions.
- **Establish sound practices for data management,** e.g., *who* will manage the platform – the provider, healthcare organization or vendor; *what* data will be reviewed by *which* party to the contract; *when* are incoming data monitored; and *how* are licensed providers alerted to significant clinical findings.
- **Adhere to federal and state requirements for online prescription of controlled substances and other medications,** and document compliance actions in the virtual care record.
- **Negotiate contractual protections,** including indemnification clauses and provisions for limiting liability/damages.

With respect to healthcare kiosks...

- **Design a dedicated network for kiosks,** protected by firewalls and other intrusion-prevention systems.
- **Train facilitators on the use of kiosks** for teleconsultations.
- **Situate kiosks in well-lit areas,** in order to protect the equipment from rough use or deliberate vandalism.
- **Utilize touchscreens rather than keyboards,** as they offer more protection against spy devices used by data hackers.
- **Install privacy screens** to prevent outsiders from viewing protected health information.

Telemedicine use skyrocketed during the COVID-19 pandemic and has shown no sign of abating since then. At this point, healthcare administrators and providers should consider implementing policies that address the specific risks posed by remote care, as well as modifying their systems and procedures to better coordinate virtual and in-person modes of care. The information and recommendations presented here can help leadership prepare their organizations and practices to thrive in a world where a large and growing proportion of healthcare encounters and services are mediated by electronic technology.

Quick Links

- American Hospital Association - Telehealth
- American Medical Association - Telehealth Helpful Resources
- American Telemedicine Association
- Center for Connected Health Policy
- Centers for Medicare & Medicaid Services–Telehealth
- National Consortium of Telehealth Resource Centers
- Health Resources & Services Administration, Office for the Advancement of Telehealth
- Telehealth.HHS.gov

At this point, **healthcare administrators and providers** should **consider implementing policies** that address the **specific risks posed by remote care**, as well as modifying their systems and procedures to better **coordinate virtual and in-person modes of care.**

Did someone forward this newsletter to you? If you would like to receive future issues of *Vantage Point*® by email, please register for a complimentary subscription at go.cna.com/HCsubscribe.

For more information, please visit www.cna.com/healthcare.