FOR IMMEDIATE RELEASE

New Report Calls for Enhanced Security to Safeguard Protected Health Information

5-Step Method Provides Health Care Organizations
with Tool to Estimate the Overall Potential Costs of a Data Breach

ANSI, The Santa Fe Group/Shared Assessments Program Healthcare Working Group,
and the Internet Security Alliance to Host Congressional Briefing Today; White House Cybersecurity
Coordinator Howard Schmidt Invited to Speak at Press Conference

Washington, DC, March 5, 2012: With the release today of *The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security*, health care organizations now have a new method to evaluate the "at risk" value of protected health information (PHI) that will enable them to make a business case for appropriate investments to better protect PHI. This report was created through the "PHI Project" – a collaboration of the American National Standards Institute (ANSI), via its Identity Theft Prevention and Identity Management Standards Panel (IDSP), in partnership with The Santa Fe Group/Shared Assessments Program Healthcare Working Group, and the Internet Security Alliance (ISA) – that involved a cross-section of more than 100 health care industry leaders from over 70 organizations. The report is available for free download at webstore.ansi.org/phi.

Health Care System Depends on Patient Trust in Confidentiality and Security
The health care delivery system is founded upon trust – a trust that those receiving health information will keep it confidential and secure. This trust is now being tested as the health care industry moves to adopt electronic health records (EHR), access federal incentives, and facilitate better patient care. PHI is now more susceptible than ever to accidental or impermissible disclosure, loss, or theft. Health care organizations (providers, payers, and business associates) are not keeping pace with the growing risks of exposure as a result of EHR adoption, the increasing number of organizations handling PHI, and the growing rewards of PHI theft.

PHI Breaches Increasing with Far-Reaching Repercussions
PHI data breaches are growing in frequency and in magnitude with huge financial, legal/regulatory, operational, clinical, and reputational repercussions on the breached organization. The report provides CISOs, CIOs, IT security, privacy, and compliance personnel with information to help them better understand the potential risks and liabilities resulting from data breaches.

The 5-Step Method to Estimate Breach Costs and Needed Investments in PHI Security
Health care organizations reading this report can take immediate action using PHIve – the PHI Value Estimator – a 5-step method for assessing security risks and evaluating the "at risk" value of an organization's PHI. This tool estimates overall potential data breach costs, and provides a methodology for determining an appropriate level of investment needed to strengthen privacy and security programs and reduce the probability of a breach occurrence.

"No organization can afford to ignore the potential consequences of a data breach," said Rick Kam, president and co-founder of ID Experts, and chair of the PHI Project. "We assembled this working group to drive a meaningful dialogue on appropriate levels of investment to better protect healthcare organizations and PHI."

"Health care is one of the most-breached industries," said Dr. Larry Ponemon, chairman and founder, Ponemon Institute. "Health care providers and supporting organizations don't currently have sufficient security and privacy budgets, including adequate processes and resources, to protect sensitive patient data. This report will help them understand what they need to do to augment their efforts."

(continued)

Report Launch Events on March 5 and Free Webinar on March 21

Leaders from the PHI Project will host events on Monday, March 5, 2012, for Congressional representatives, staff, and the press to present the report and its findings. The first event will be held at the National Press Club in Washington, DC, at 10:00 a.m. ET. White House cybersecurity coordinator Howard A. Schmidt has been invited to open the press conference. The second event will be held on Capitol Hill in Rayburn B-340, at 12:30 p.m. ET. A free webinar with the authors will be held on Wednesday, March 21, 2012, at 2:00 p.m. ET to discuss details of the report and walk through immediate actions organizations can take. To register, please visit https://www1.gotomeeting.com/register/739954912.

Bringing Together a Cross-Section of Experts

The PHI Project brings together experts from across the industry: including health care providers, payers and insurers, other health care services organizations, data breach prevention and recovery firms, legal experts on privacy and security, and others, providing a range of perspectives. The initiative was made possible through the generous support of the following organizations: Clearwater Compliance LLC and DriveSavers Data Recovery, Inc. (premium sponsors); Affinion Security Center; Alvarez & Marsal; BKD, LLP; Booz Allen Hamilton; The Center for Identity Management and Information Protection at Utica College; Deluxe Corporation; Direct Computer Resources, Inc.; Europ Assistance USA; ID Experts; ManageEngine, a division of Zoho Corp; and Terra Verde Services (partner sponsors).

About ANSI

The American National Standards Institute (ANSI) is a private non-profit organization whose mission is to enhance U.S. global competitiveness and the American quality of life by promoting, facilitating, and safeguarding the integrity of the voluntary standardization and conformity assessment system. The ANSI Identity Theft Prevention and Identity Management Standards Panel (IDSP) is a cross-sector coordinating body that facilitates the timely development, promulgation, and use of voluntary consensus standards and guidelines that will equip and assist the private sector, government, and consumers in minimizing the scope and scale of identity theft and fraud.

About the Shared Assessments Program

The Shared Assessments Program was created by leading financial institutions, the Big Four accounting firms, and key service providers to inject standardization, consistency, speed, efficiency, and cost savings into the service provider assessment process. Through membership and use of the Shared Assessments tools (the Agreed Upon Procedures and the Standardized Information Gathering questionnaire), Shared Assessments offers outsourcers and their service providers a faster, more efficient, and less costly means of conducting rigorous assessments of controls for security, privacy, and business continuity. The Shared Assessments Program is managed by The Santa Fe Group, a strategic consulting company based in Santa Fe, New Mexico.

About the Internet Security Alliance (ISA)

The Internet Security Alliance is a multi-sector trade association established in collaboration with Carnegie Mellon University in 2000. ISA's mission is to combine advanced technology with the pragmatic business needs of its members and help create effective public policy leading to a sustainable system of worldwide cybersecurity. ISA advocates a modernized social contract between industry and government creating market-based incentives to motivate enhanced security of cyber systems. ISA provides its members with a range of technical, business, and public policy services to assist them in fulfilling their mission.

# # #

Media Contacts:

Kelly Stremel, MacKenzie Marketing Group
(503) 225-0725; kellys@mackenzie-marketing.com

Elizabeth Neiman, American National Standards Institute (ANSI)
(212) 642-4911; eneiman@ansi.org