EXECUTIVE SUMMARY

INTRODUCTION:
The increased use of health information technology (health IT) is a common element of nearly every health reform proposal because it has the potential to decrease costs, improve health outcomes, coordinate care, and improve public health. However, it raises concerns about security and privacy of medical information. This paper examines some of the “gaps” in privacy protections that arise out of the current federal health privacy standard, the Health Insurance Portability and Accountability (HIPAA) Privacy Rule, the main federal law which governs the use and disclosure of health information. Additionally, it puts forth a range of possible solutions, accompanied by arguments for and against each. The solutions provide some options for strengthening the current legal framework of privacy protections in order to build public trust in health IT and facilitate its use for health reform. The American Recovery and Reinvestment Act (ARRA) enacted in February 2009 includes a number of changes to HIPAA and its regulations, and those changes are clearly noted among the list of solutions (and ARRA is indicated below where the Act has a relevant provision).

LAW IN EFFECT PRE-ARRA AND PERCEIVED “GAPS”:
The Health Insurance Portability and Accountability Act (HIPAA): The use of health information is currently covered by HIPAA and its implementing regulations. The Department of Health and Human Services (HHS) issued final regulations in 2002, which became effective for most entities covered by HIPAA in 2003. The HIPAA privacy regulations set forth rules governing the access, use, and disclosure of personal health information by most traditional health care entities. The goal of the regulations is to ensure that health information is rapidly accessible to those authorized, but kept confidential and protected from inappropriate use.

- **Who is covered:** The Privacy Rule only applies to entities expressly defined in the HIPAA statute, which places unmentioned, new, and emerging entities outside the direct coverage of the rule.
- **What is covered:** The Privacy Rule regulates the type of health information that can be shared by covered entities and for what purposes. But individuals are concerned that their personal health information will not be protected in the emerging e-health environment. For example, privacy may be at risk due to the lack of federal notification standards for breaches; the possibility that developments in technology may make “de-identified” data (not covered under the Privacy Rule) re-identifiable; and the lack of strong prohibition on the use of personal health information for marketing purposes.
- **State law variation:** The Privacy Rule is only a minimum standard, which gives states the power to enact more stringent protections for health privacy. The resulting variations in state privacy laws may pose an obstacle to health information exchange across state lines and/or to a national health information system.
- **Insufficient comprehension of and compliance with the Privacy Rule and enforcement:** Entities covered by the Privacy Rule and individuals/patients do not adequately comprehend the Privacy Rule’s provisions, leading health care entities to either over- or under-interpret the Rule and leaving individuals unaware of their privacy rights. In addition, there has been debate among policymakers and stakeholders over 1) whether the Rule to date has been appropriately enforced; 2) whether or not the current mechanisms are adequate to ensure compliance; and 3) what the limits of the enforcement mechanisms should be.
POTENTIAL SOLUTIONS:
The perceived “gaps” in federal legal protections for health information can be grouped into four categories: 1) who is covered; 2) what is covered; 3) state law variation; and 4) insufficient comprehension of and compliance with privacy protections. The solutions range from amending existing law or regulation to encouraging private action through market or other incentives.

- **Who is covered:** Amend HIPAA to create new categories of covered entities and require the federal agencies to issue new privacy regulations to cover activities of new entities; revise regulations and expand recent guidance on business associate agreements to include all health information exchanges in existence or development (ARRA); require all entities handling health information to adopt policies consistent with fair information practices; and/or keep the law in its current state and encourage adoption of good privacy practices through voluntary business agreements.

- **What is covered:** Enact federal legislation prohibiting the use of personal health information to determine the terms and conditions of employment or health insurance; establish a federal breach notification law applicable to identifiable health information (ARRA); seek the input of experts and public to examine the de-identification safe harbor exception (ARRA); create more options for the use of health data stripped of some individual identifiers (ARRA) and require data use agreements for all data disclosures; require those obtaining data stripped of patient identifiers to commit to keeping data de-identified except in certain circumstances; strengthen, establish, and increase compliance with HIPAA rules regarding the use of personal information for marketing (ARRA); adopt rules governing marketing uses by non-covered entities such as Internet health sites; issue more guidance on how to comply with the Privacy Rule (ARRA); issue new regulations regarding terms of access to health information exchanges.

- **State law variation:** “Wipe the slate clean” and have Congress could establish a new federal privacy law that preempts existing state laws but allows states to pass new stronger privacy provisions; and/or keep the status quo with the federal standard as a floor.

- **Improving comprehension of and compliance with the Privacy Rule and enforcement:** Revise the Privacy Rule to make it less complex; provide more guidance and better education on the requirements of the rules (ARRA); improve consumer education on HIPAA rights by requiring entities to provide a summary notice; ensure a proper enforcement regime for entities not covered by HIPAA that handle personal health information; amend HIPAA enforcement to clarify enforcement authority and also direct the Secretary to pursue civil actions (ARRA); amend HIPAA to allow the Secretary to directly enforce HIPAA regulations against business associates (ARRA); and/or amend HIPAA to allow a private right of action (ARRA).

**CONCLUSION:**
Generally, there is consensus that efforts to facilitate widespread adoption and use of health information technology must move forward with appropriate protections for privacy and security. However, achieving consensus on the details of what privacy and security measures need to be put in place continues to be a challenge. The new Administration and Congress are moving forward to increase the use of health IT. Any efforts to reform the nation’s health systems and to increase the adoption of health IT will need to address the concerns surrounding the privacy and security of personal health information.