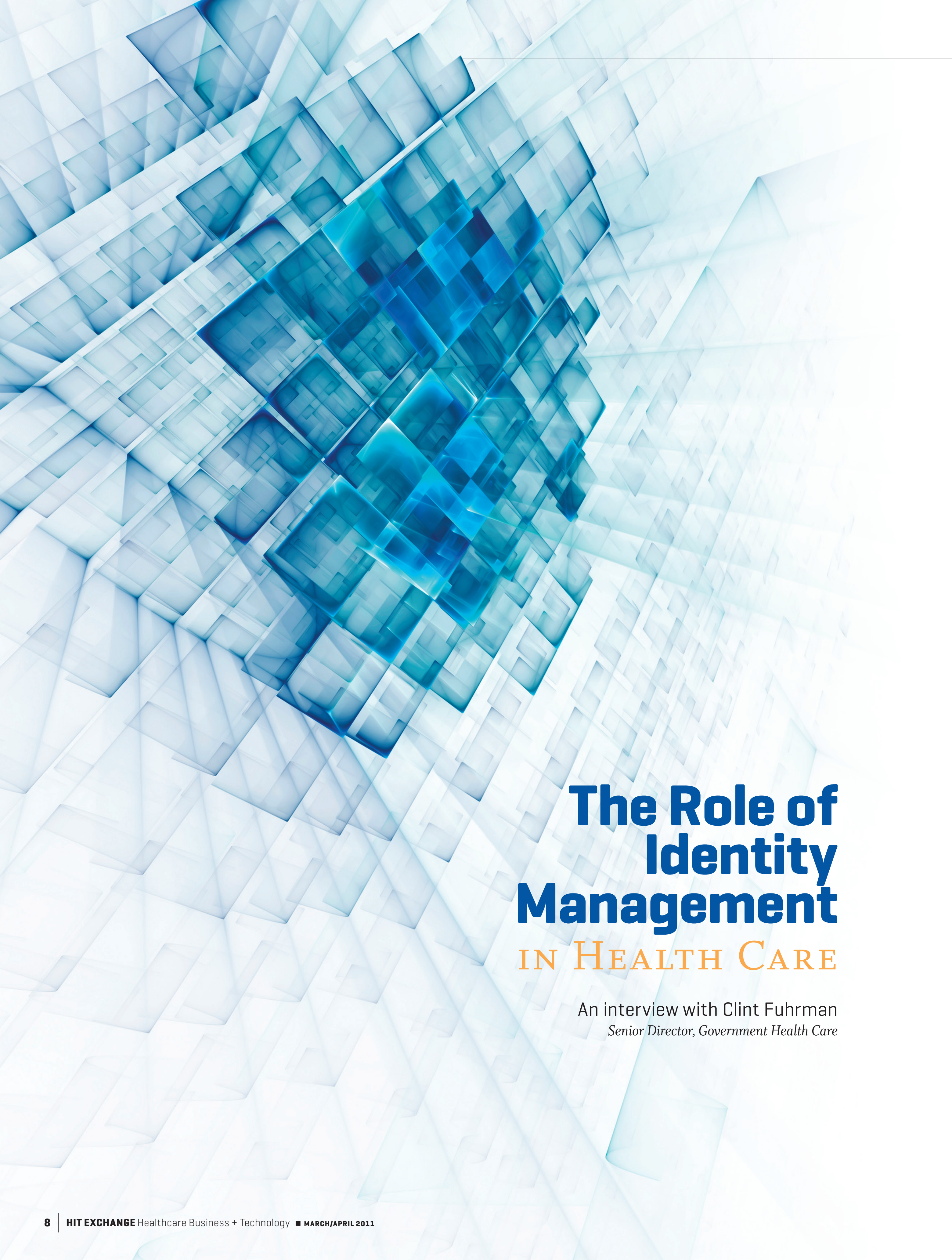

The Role of Identity Management in Health Care

An interview with Clint Fuhrman

Senior Director, Government Health Care

Q: How should the healthcare industry be thinking differently about identity management?

A: The focus right now is on the apparatus of network security and access control: verifying and authenticating an IP address, issuing credentials, etc. This approach addresses the "what" of identity management—the technical side—but misses the critical question of "who?" How do we know who the person on the other end of the Internet connection truly is, and what risks they may pose for the environments and systems they are attempting to enter? LexisNexis® Risk Solutions takes a fundamentally different approach to establishing and monitoring identities. We believe that true identity management encompasses not just looking at the computer a person is using, or the issuance of a password, but determining from the beginning the true identity of the person behind the monitor. Is the individual trying to access the system a real person in the real world, are they the person they claim to be, and are they an appropriate individual to have access to this information? True identity management encompasses knowing who the person is, understanding their background, evaluating how what that means to the environment they're trying to access, and being alerted to critical changes after they are credentialed. We must begin thinking differently about these issues if we are going to ensure the privacy and security of health information.

Q: Why is identity management becoming increasingly important to consider when deploying health information technologies?

A: Comprehensive identity management must be a foundational concern for the health care industry. Government efforts in the health care space are driving much of the focus on identity management, including the activities of the Office of the National Coordinator for Health Information Technology (ONCHIT), various policy committees, federal legislation such as the High Tech Act, and continuing efforts to comply with the Health Insurance Portability and Accountability Act (HIPAA). Perhaps more importantly, adoption of these technologies by both providers and patients will require trust in their privacy and security. The fear of medical identity theft or improper access to sensitive records, as well as liability concerns, could halt the progress we've made. Patients want to know the steps that are being taken to ensure their privacy.

Comprehensive identity management is not merely a "nice to have" component of the health care system; it is a core function. You wouldn't build a house without locks and fill it with valuable possessions, and the same is true of creating an online health care system with EHRs, HIEs, and online enrollment. You cannot implement healthcare technologies into your workflow without properly securing your valuable possessions, which in this case is patient information.

Q: What are some of the key questions HIT stakeholders should keep front of mind when deploying technologies that give access to protected health information?

A: We suggest, when implementing any technology that provides access to protected health information, the following questions be asked:

» Have we identified everyone who will have access and are they included in the identity management process?

» How will identities be verified, ensuring they are who they claim to be, and evaluated for risk and access purposes?

» What level of authentication strength is required?

» Are there national or local regulatory requirements or technical standards that we need to comply with?

» How will we evaluate the person to ensure that they are a licensed practitioner in the areas of certification they claim, that they do not have significant criminal history or other troubling issues that would prevent access?

» After authentication, what is the process for credentialing these individuals?

» How often will credentialed individuals need to be re-authenticated, and how will we find out about critical changes in their identity?

Deploying a comprehensive identity management solution will naturally be more complex in a state-wide health information exchange vs. a small family practice. Regardless, stakeholders across the health care continuum must work together to protect patient data. Identity Management cannot be pushed down to end users in every case; those responsible for the establishment and operation of health information exchange networks must accept their role in implementing these solutions at a central level. Cost-effective, user-friendly tools exist to deliver these services, and companies such as LexisNexis® Risk Solutions are leading the way in providing comprehensive Identity Proofing for health care companies and the financial services, legal, insurance, and government sectors. ●

EXPERT: Clint Fuhrman
Senior Director, Government Health Care
LexisNexis®

Clint Fuhrman is the Director of Government Health Care for LexisNexis® Risk Solutions. Prior to joining LexisNexis®, he served in positions including Deputy Secretary of the Florida Agency for Health Care Administration, Special Assistant to Governor Jeb Bush, Director of Legislative Affairs for The Rubin Group, and President of Meridian Consulting Group. Mr. Fuhrman began his career with the Florida Institute of Government at Florida State University, and is an FSU graduate.