

Research IT Clinic / Open House

Implementation of New Research Compliance and Security Policies: A Discussion with Legal, Compliance and Research IT

Nicholas Hunt, Biomedical Informatics

Joan Gates, Counsel, Legal Department

Jeremy Corsmo, Director, ORCRA

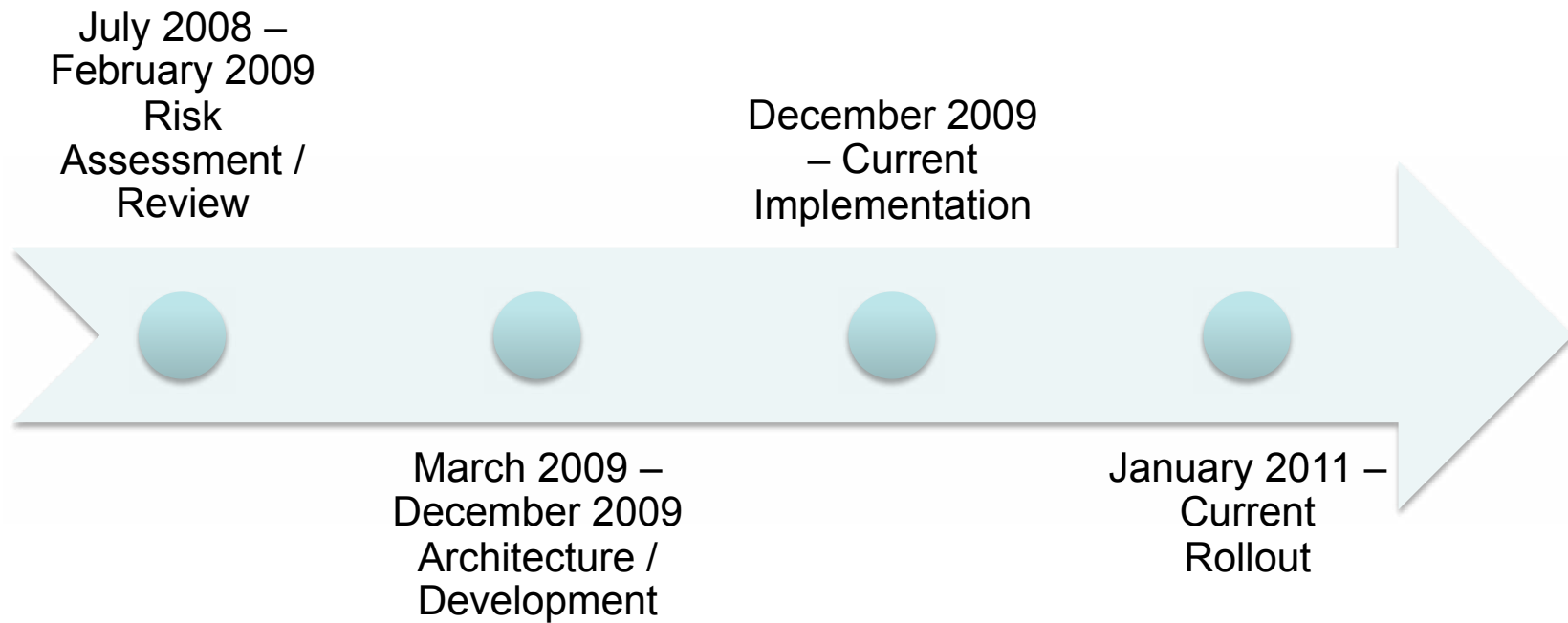
Agenda

- Introductions
- History
- New Processes / Automation
- Conclusion / Q&A

Introductions

- Nicholas Hunt (nicholas.hunt@cchmc.org)
 - Biomedical Informatics
- Joan Gates (joan.gates@cchmc.org)
 - Counsel, Legal Department
- Jeremy Corsmo (jeremy.corsmo@cchmc.org)
 - Director, ORCRA

History



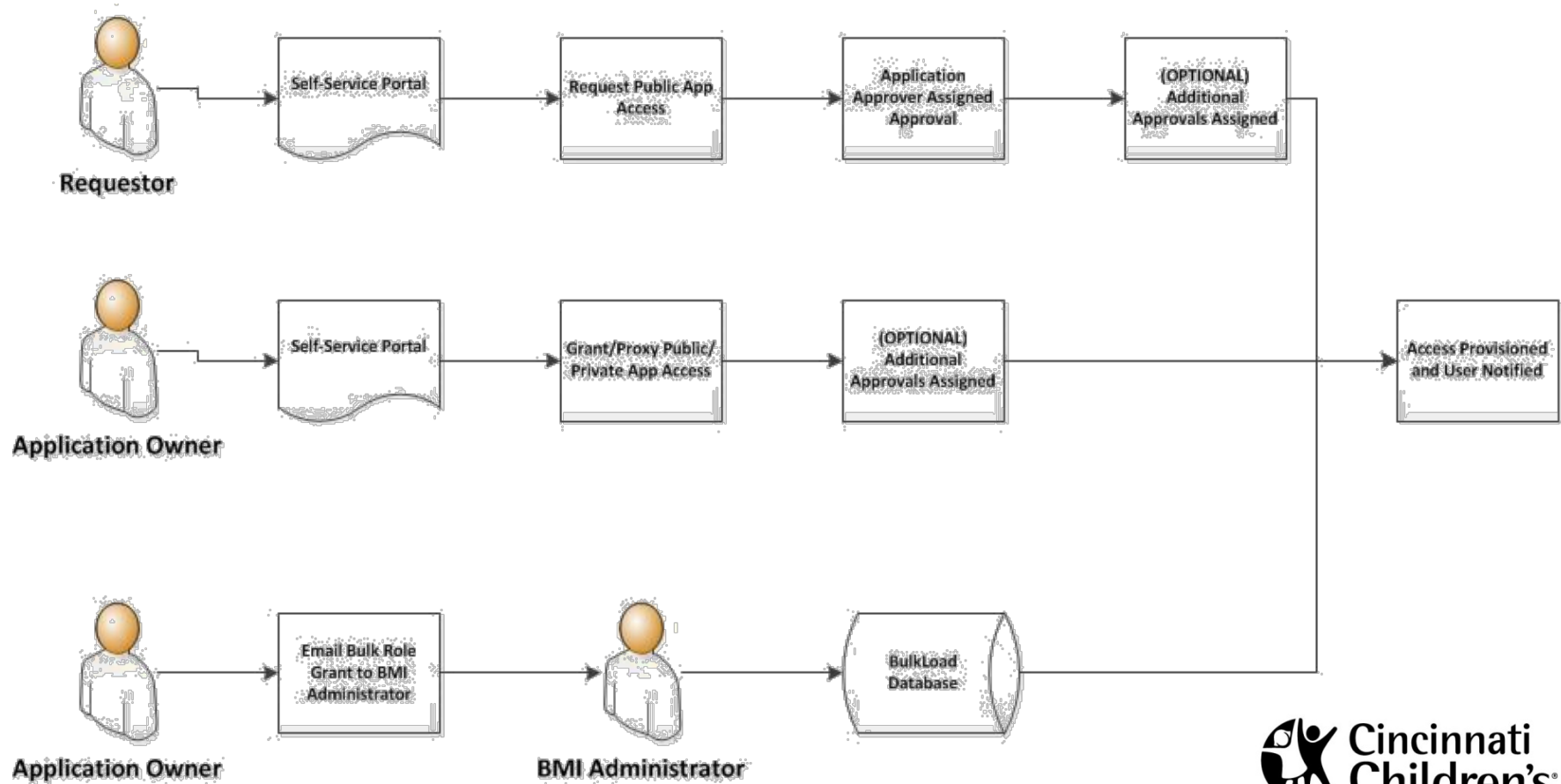
History (cont.)

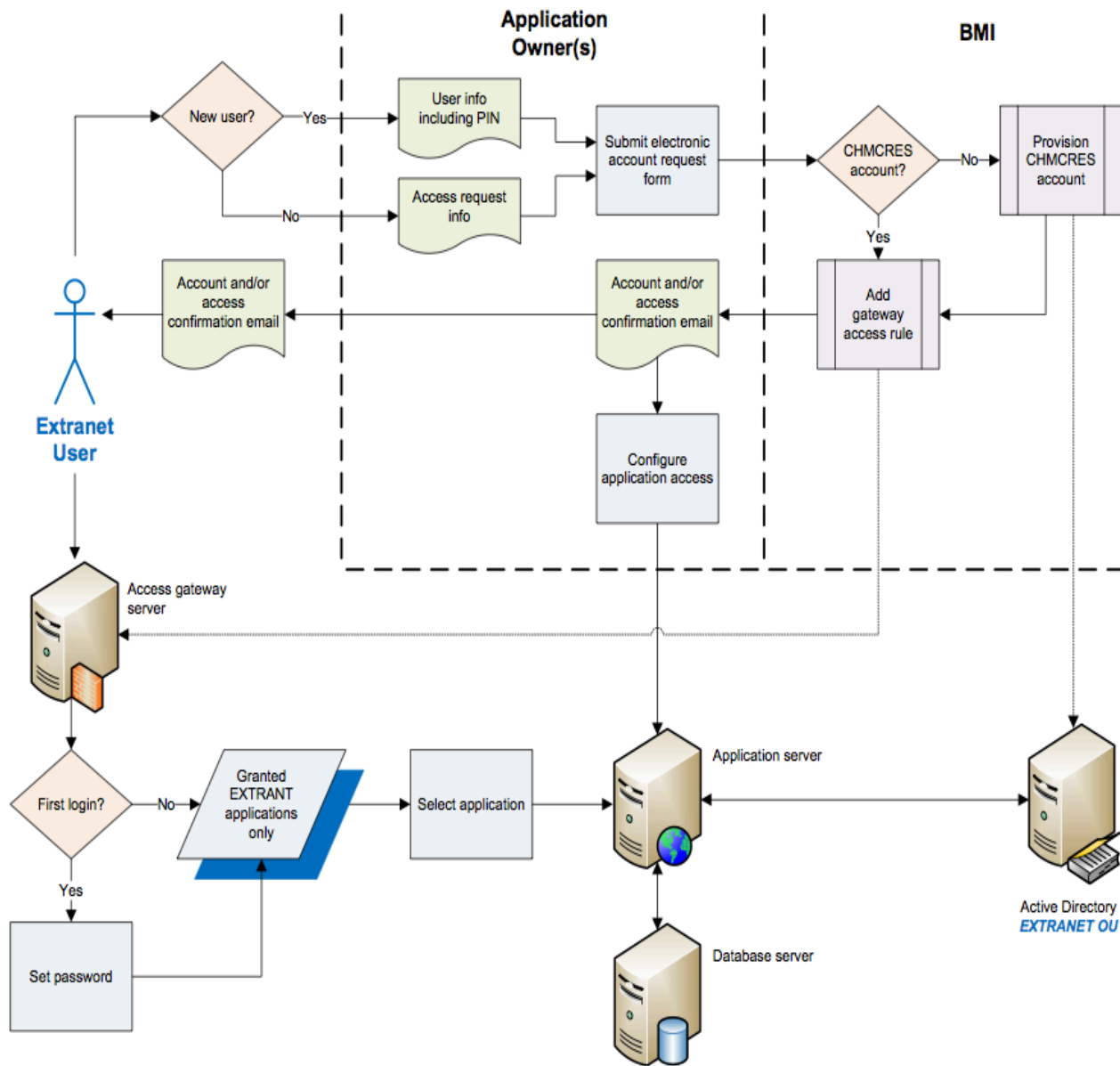
- Perform Security Review of the Current Research Environment / Application
- Designed New Network / Central Identity Store
- Implemented New Network / Central Identity Portal for Self-Service Capabilities

New Processes / Automation

- User Account Provisioning / Access
 - Central portal to handle user registration / requesting access to applications / password management
 - Application registration / setup to allow application owner to manage their own users
 - Central point of contact for all users

New Process / Automation (cont.)





New Processes / Automation (cont.)

Cincinnati Children's

CCHMC Research ID Login
Division of Biomedical Informatics

Home Login Help Policies

Welcome

Welcome to the Cincinnati Children's Hospital Medical Center (CCHMC) Research ID Login page. To access the requested research application, please login via the appropriate login button from the links on the right or via the [Login](#) page from the menu above. For any one that does not have an account, please click on the External Users link and register for a login to the environment. If you have any problems logging into your application, or need additional help, please contact BMI at the contact information located on the [Help](#) page.

CCHMC Users

CCHMC users click [here](#) to login to the environment or click on CCHMC Users image above.

External Users

External users click [here](#) to login to the environment or click on External Users image above. If you have not registered for a Research ID, go to the External Users login page and click to register for a new account.

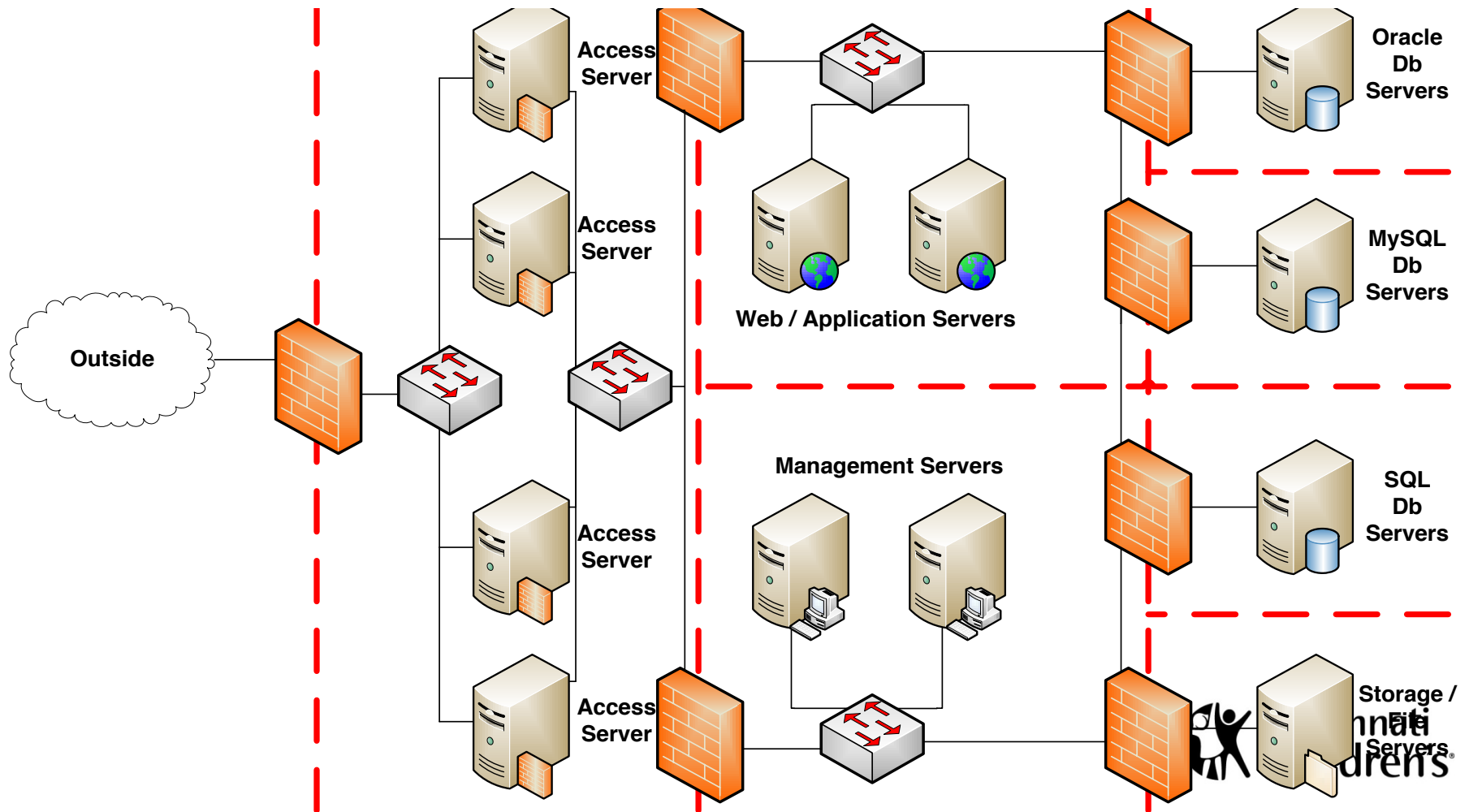
Federated Users

COMING SOON!
BMI is currently working on implementing federated access to the environment. Check back to see when federated identities can be used to access the environment.

New Processes / Automation (cont.)

- Network Access to Applications
 - Central gateways to control access to applications
 - Unified access to applications from any location
 - Same URL / access method no matter the location of the user
 - Virtual Desktop Environment (VDI) for client / server applications and continuous access

New Processes / Automation (cont.)



New Processes / Automation (cont.)

- Confidentiality / Application Owner Agreements
 - Replace current extranet / 3rd party agreements for VPN access
 - Applied to all users who access applications in the research network environment
 - Annually, all users will be required to review and accept the agreement
 - All application owners will be required to review and agree to requirements

New Processes / Automation (cont.)

- Confidentiality / Application Owner Agreements
 - For CCHMC employees, reminds users/owners of existing policies and legal requirements related to confidentiality/security
 - For non-employees, informs network users of CCHMC and legal requirements

New Processes / Automation (cont.)



CCHMC Research ID Login
Division of Biomedical Informatics

Home

CINCINNATI CHILDREN'S HOSPITAL MEDICAL CENTER ("CCHMC") CONFIDENTIALITY AND NETWORK ACCESS AGREEMENT

STATEMENT OF POLICY

It is the legal and ethical responsibility of all CCHMC Information System Users to use personal and confidential patient, employee and CCHMC business information (referred to here collectively as "confidential information") in accordance with the law, CCHMC policies including the Code of Conduct, and to preserve and protect the privacy rights of the subject of the information.

Laws controlling the use, disclosure and maintenance of confidential information include, but are not limited to, the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA). This and other laws apply whether the information is maintained in electronic or any other form, and whether the information is used or disclosed orally or in writing. CCHMC policies that control the way confidential information may be used are located at [insert location]. It is your responsibility to review and assure your compliance with these requirements.

Confidential information includes Protected Health Information, Employment Information, Business Information and Education Information. Please review CCHMC policy E-100 "Confidentiality and Management of Information" for examples of confidential information.



ACKNOWLEDGEMENT OF RESPONSIBILITY

I understand and acknowledge that:

- It is my legal and ethical responsibility as an authorized user to preserve and protect the privacy, confidentiality and security of all confidential information collected, created or maintained by CCHMC, in accordance with the law and CCHMC policy.
- It is my legal and ethical responsibility to ensure that all confidential information I access is required for the particular purpose for which I am accessing, disclosing or using it. This includes assuring that research activities involving human subjects has a valid protocol approved by CCHMC's Institutional Review Board before accessing, disclosing or using such confidential information.



New Processes / Automation (cont.)



Home

CINCINNATI CHILDREN'S HOSPITAL MEDICAL CENTER ("CCHMC") RESEARCH NETWORK APPLICATION OWNER ACCEPTANCE OF RESPONSIBILITY

STATEMENT OF POLICY

It is the legal and ethical responsibility of all CCHMC Information System Users to use personal and confidential patient, employee and CCHMC business information (referred to here collectively as "confidential information") in accordance with the law, CCHMC policies including the Code of Conduct, and to preserve and protect the privacy rights of the subject of the information.

Laws controlling the use, disclosure and maintenance of confidential information include, but are not limited to, the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA). This and other laws apply whether the information is maintained in electronic or any other form, and whether the information is used or disclosed orally or in writing. CCHMC policies that control the way confidential information may be used are located at [insert location]. It is your responsibility to review and assure your compliance with these requirements.

As an Application Owner, it is your responsibility to protect access to data which has been entrusted to you within CCHMC applications and systems (referred to here collectively as "environment"). When you review, grant, and approve access to the environment, you are responsible to assure that only those people with the right and a need-to-know are given access to the environment and the information contained within it.

When receiving requests for access, it is important to ensure that requests are for the proper type of access (full, limited, read, read/write, etc.) based on the needs of the individual user and limited to job-related purposes. This will ensure that when you approve an access request, the individual you approve will have appropriate access without additional rights that could lead to increased exposure and potential compromise of the environment and information.

ACKNOWLEDGEMENT OF RESPONSIBILITY



CONCLUSION / Q&A