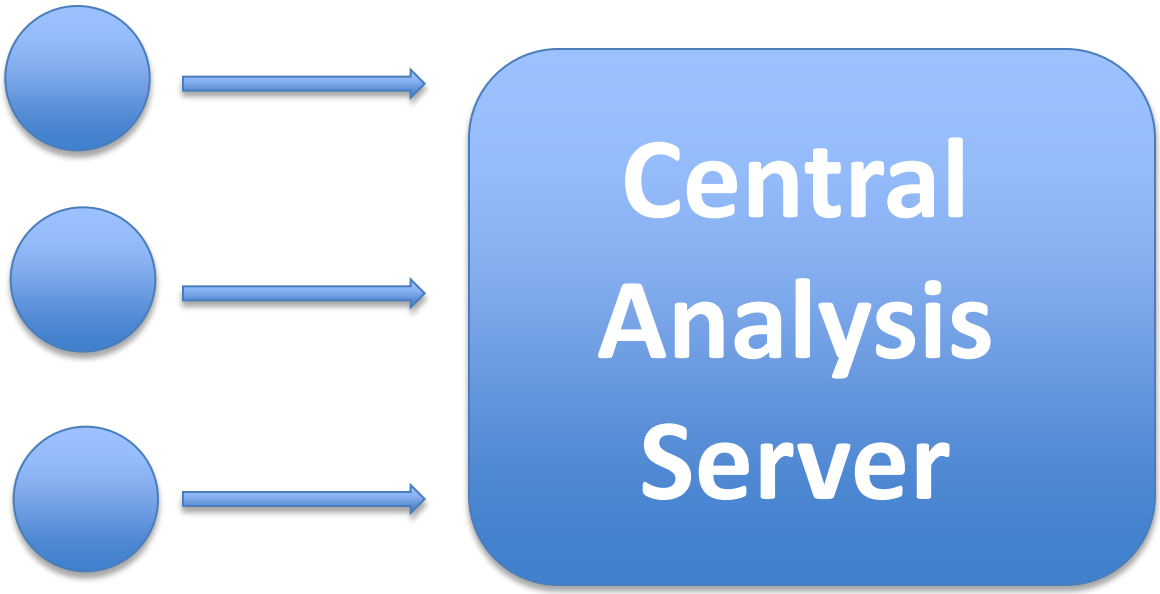
Central Analysis Server

ELSI Issues

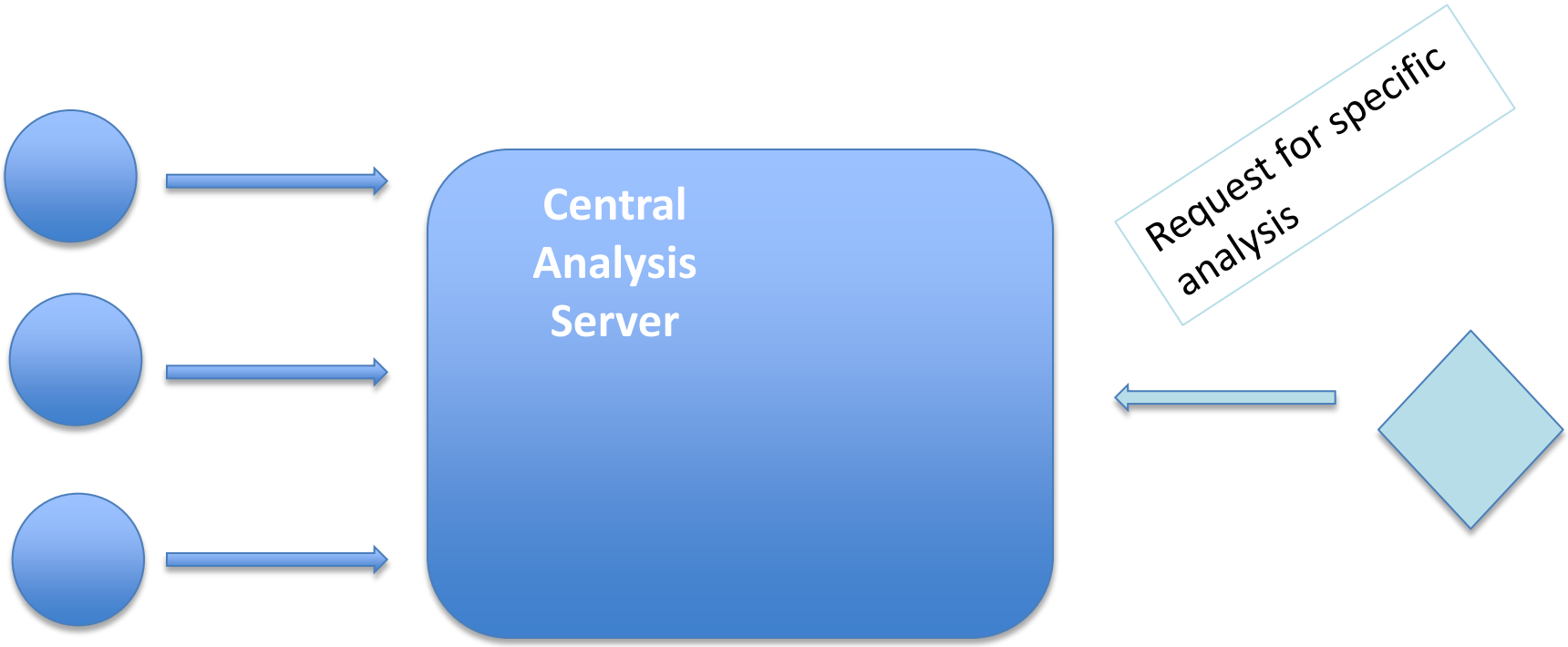
Pearl O'Rourke, Mark DePristo,
Lisa Brooks, Carlos Bustamante,
David Altshuler

The Model



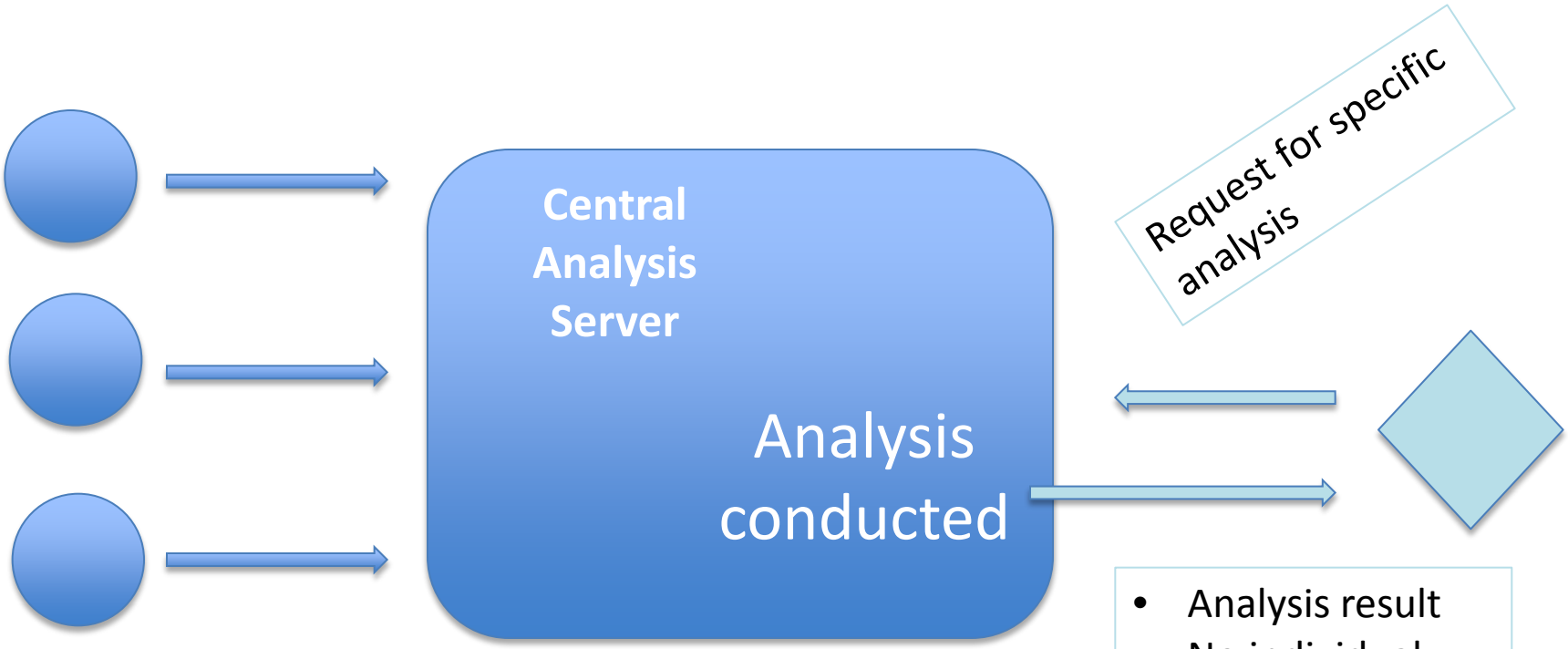
- Data collected pursuant to informed consent
- Coded - no HIPAA identifiers

The Model



- Data collected pursuant to informed consent
- Coded - no HIPAA identifiers

The Model



- Data collected pursuant to informed consent
- Coded - no HIPAA identifiers

- Analysis result
- No individual level data

Central Analysis Server:
dbGaP-lite? Or heavy?

	dbGaP	Central Server
ICF for source material	Yes	Yes
Limitations per ICF	Yes	Yes
Identifiable data	No	No
Disclose individual data	Yes	No

Central Analysis Server:
dbGaP-lite? Or heavy?

	dbGaP	Central Server
ICF for source material	Yes	Yes
Limitations per ICF	Yes	Yes
Identifiable data	No	No
Disclose individual data	Yes	No
Local certification	Yes	Presume yes
Review of uses	Yes	?
Return of research results	Unlikely	Even more unlikely

“Vulnerable” points

- The central analysis server
- Primary collection of tissue → data
- Analyses
- Return of analyses to requesting investigator

The Central Analysis Server*

- Research repository of de-identified data
- IRB review and approval of a biorepository including rules for:
  - Submission of data
  - Maintenance of data
  - Accepting analysis requests
  - Conducting analyses
  - Reporting analyses

* Note: dbGap is NOT IRB reviewed/approved. Strongly suggest that a Central Server should be IRB approved.

Primary data source

- Data from tissue collected under IRB-approved protocol and ICF
  - Under auspices of local IRB

The informed consent form

- From an ethical standpoint, the informed consent process and document should make it clear that participants' DNA will undergo genome-wide analysis and that genotype and phenotype data will be shared for research purposes through the NIH GWAS data repository.

http://gwas.nih.gov/pdf/PTC_for_IRBs_and_Institutions_revised5-31-11.pdf

The informed consent form

In order to allow researchers to share test results, the National Institutes of Health (NIH) and other central repositories have developed special data (information) banks that analyze data and collect the results of whole genome studies. These banks may also analyze and store DNA samples, as well. These central banks will store your genetic information and samples and give them to other researchers to do more studies. We do not think that there will be further risks to your privacy and confidentiality by sharing your samples and whole genome information with these banks. However, we cannot predict how genetic information will be used in the future. The samples and data will be sent with only your code number attached. Your name or other directly identifiable information will not be given to central banks. There are many safeguards in place to protect your information and samples while they are stored in repositories and used for research.

Primary data source

- Tissue → data collected under IRB-approved protocol and ICF
  - Under auspices of local IRB
- 'Certification' that data can be submitted to the central server
  - Local institution +/- local IRB involvement

Institutional Certification

- The NIH will only accept GWAS data into the NIH GWAS data repository after receiving appropriate certification by the responsible Institutional Official(s) of the submitting institution that they approve submission to the NIH GWAS data repository.

http://gwas.nih.gov/pdf/PTC_for_IRBs_and_Institutions_revised5-31-11.pdf

1. Certification should assure that:

- The data submission is consistent with all applicable laws and regulations as well as institutional policies;
- The appropriate research uses of the data and the uses that are specifically excluded by the informed consent documents are delineated;5
- The identities of research participants will not be disclosed to the NIH GWAS data repository; and

http://gwas.nih.gov/pdf/PTC_for_IRBs_and_Institutions_revised5-31-11.pdf

2. Certification should assure that:

- An IRB and/or Privacy Board, as applicable, reviewed and verified that:
  - The submission of data to the NIH GWAS data repository and subsequent sharing for research purposes are consistent with the informed consent of study participants from whom the data were obtained;
  - The investigator's plan for de-identifying datasets is consistent with the standards outlined in the policy;
  - It has considered the risks to individuals, their families, and groups or populations associated with data submitted to the NIH GWAS data repository; and
  - The genotype and phenotype data to be submitted were collected in a manner consistent with 45 C.F.R. Part 46.

http://gwas.nih.gov/pdf/PTC_for_IRBs_and_Institutions_revised5-31-11.pdf

Central Analysis Server analyses

- De-identified data, hence not human subjects research
  - No IRB review required
  - BUT – central server should consider some method of review
    - E.g., Consider community risk

Return of analyses to requester/s

- De-identified data, hence not human subjects research
  - No IRB review required

Return of Research Results

- **Return of Individual Research Results**. For reasons explained later in this document, the return of individual research results to participants from secondary GWAS is expected to be a rare occurrence. Nevertheless, as in all research, the return of individual research results to participants must be carefully considered because the information can have a psychological impact (e.g., stress and anxiety) and implications for the participant's health and well-being. While clinically valid and meaningful results may have a positive impact on an individual's health, harms can occur if unvalidated research results are provided back to participants or used for medical decision-making.

http://gwas.nih.gov/pdf/PTC_for_IRBs_and_Institutions_revised5-31-11.pdf

Central Analysis Server
Final ELSI Thoughts

- Can use lessons-learned from dbGaP
- Possibly more streamlined than dbGaP
- Must reassess if:
  - Relevant changes to Common rule via the ANPRM
  - Relevant changes to HIPAA/Privacy and Security Rules