Global Alliance
for Genomics & Health

GA4GH Data Security Work Stream
Minutes and Actions 2017-2018

These are the minutes for the GA4GH … Work Stream. For further information, please visit the GA4GH Work Stream page (will link to the page on the website when it is ready) at ga4gh.org.

2019-2020 Minutes

Table of Contents:

Meeting Protocols

- Please note that by participating in meetings, attendees agree to adhere to the GA4GH Standards of Professional Conduct
- Meetings may be recorded for note-taking purposes. Recordings will be deleted within three months of the meeting taking place.

Sub-Group Minutes and Actions Documents

This Work Stream has meetings for the following sub groups.

List of Meetings

Next Meeting

Chair:

Attendees “Name (Affiliation)”:

	Actions Arising	Assigned To	Deadline

	Agenda Item	Speaker	Time
1.	Approve Previous Minutes and Agenda	Chair	
2.	Review of Actions		
	A.O.B.		

Minutes:

2018-10-04: 2018 6th Plenary

Chair:
Attendees “Name (Affiliation)”:

	Actions Arising	Assigned To	Deadline
	Speak to Julia about Security Hire	Paul	
	Talk to Peter about requiring DPs to report GA4GH related breaches	Melissa (done)	

	Agenda Item	Speaker	Time

1.	Approve Previous Minutes and Agenda	Chair	
2.	Review of Actions		
	A.O.B.		

Minutes:
Vulnerability reporting, and breach response/management deliverables are not standards but rather GA4GH internal processes and should go through a "light touch" review, focused on REWS. AAI will need the full GA4GH approval process.

Security contractor: objection by Paul, Dixie, and JP. Paul to follow up with Julia
Having an outside contractor complicates breach and vulnerability reporting
JP: The person needs to be FTE GA4GH, even as a contractor

Dixie: require new driver projects to report GA4GH related breaches back to GA4GH. Melissa to follow up with Peter. (done).

Rishi: updates to Security review process presentation
Dixie: we need to get rid of the term "penetration testing" use "assurance testing" instead
JP: Artificial time pressure to get products released in time is a cause of the problem
Dixie: No live server testing, but the implementers may test their own server and let us know if they find an issue on our end

Dixie: Do security questionnaire for AAI.

2018-08-16 Driver Project Engagement Meeting

Chair: Dixie Baker, Paul Flicek
Attendees "Name (Affiliation)": Juan Troncoso-Pastoriza (EPFL), Rishi Nag (GA4GH), Knox Carey, Dave Bernick (Broad) David Lloyd (ELIXIR, Beacon Project), Dusan Andric (OICR, ICGC-ARGO)

	Actions Arising	Assigned To	Deadline
	Set up proposal for new standards from the Breach Response split	Melissa	

	Email driver projects to get a second Breach Response implementation	Melissa	
	Determine who will turn the Breach Response Slide deck into a written spec	Melissa to follow up with the team	
	Request feedback from Driver Projects on AAI	Melissa	
	Decide if we want to fill out a security form for each of the products	Dixie + team	

	Agenda Item	Speaker	Time
1.	Update and DP input for Authorization and Authentication Infrastructure (AAI)	Dave Bernick	
2.	Breach Response Protocol: test implementations	Kate Birch	
3.	Product Approval Process	Melissa Konopko	
	A.O.B.		

Minutes:
The proposed division of the breach response protocol into three standards still needs to be presented to the steering committee. [ACTION] Melissa to follow up with Dixie, Paul, Kate, and Snehit on the next steps.

Kate: Discussed the **Breach Response protocol**. Slides here:
https://docs.google.com/presentation/d/1JJa5hbpnfxuuXGd_XncOVNT4FLs_uDvQ0-qtkA8cwYg/edit#slide=id.p1
Said that there would be an AGHA trial run of the protocol. Discussed how GA4GH should be notified and if the contact should be secure.

- Kate: including barriers, such as the requirement of a complex, secure protocol for sending information to GA4GH will reduce uptake. Sending this information is not required, so using simple email is the best solution.
- Dixie: Breaches are not usually widely reported early on, and details about the breach are highly sensitive. So the projects will want to control when this information gets out, it should be secure. That is, the transmission needs to be secured to protect the confidentiality and integrity of the information, and the source of the information needs to be authenticated so that GA4GH knows the source is trustworthy.

- David B: Suggests creating a simple secure website for reporting. Transmission could be secured using Transport Layer Security (TLS), and source can be authenticated through a user credential, such as a password.
- For now, Driver Projects needing to report a breach can use unsecured email to security-notifications@ga4gh.org, as set on the Contact Us page on the GA4GH website.

Driver projects approved of the protocol at the Toronto meeting. However, we still need a second implementation outside of AGHA with interoperability. [ACTION] Melissa to email driver projects to see if we can get another volunteer for implementation.

David L: Beacon would consider automating this breach response process.

The protocol is currently only in slide form. Needs to be turned into a written spec. [ACTION] Dixie, Paul, Kate, Snehit, and Melissa to follow up on how this will be done.

Work left to be done, need volunteers:

- Convert communications protocol into written specification built upon the strategy described in the slides
- Write guidance document
- Get another DP to implement the Breach Response protocol
- Write vulnerability reporting protocol

David B: Discussed the AAI profile. Document here:
https://docs.google.com/document/d/1zzsuNtbNY7agPRjfTe6gbWJ3BU6eX19JjWRKvkFg1ow/edit

Had been working closely with Ilia and Moran from DURI as well as someone from ELIXIR. Unknown if other driver projects have given feedback. [ACTION] Melissa to request feedback from other DPs.

Need to add examples regarding API. Current specification focuses primarily onauthentication, while providing foundation for adding authorization details. Addition authorization to the specification is the next big step, but is already in progress

Melissa: Discussed Product Approval Process. Slide deck here:
https://docs.google.com/presentation/d/1aOBJ4V4jug7s4rRUTFseqNwkMhqQZLP4Sic9KVID-Rk/edit#slide=id.p

[Action] Need to determine with each product if we want to fill out an initial security questionnaire.

2018-01-29 Data Security Intro Meeting

Chair:Dixie Baker & Paul Flicek
Attendees “Name (Affiliation)”: Dixie Baker, Paul Flicek, Rishi Nag (GA4GH), Melissa Konopko (Ga4GH), Dylan Spalding (EGA), Richard de Borja (CanDIG), Christian Bolliger (BRCA, ETH), David Bernick (Broad Institute/DataBiosphere), Heidi Sofia (NHGRI/NIH), Jean Louis Raisaro (EPFL), David Bernick (Broad Institute - first 25 minutes), Juan Ramón Troncoso-Pastoriza (EPFL), Stephanie Dyke (McGill), Knox Carey (self), Adrian Thorogood (McGill)

	Actions Arising	Assigned To	Deadline
	Follow up with D Bernick & Knox about the AAI project leadership	Melissa, Dixie, Paul	
	Breach Response Leadership to follow up with Adrian of REWS to connect those two groups	Snehit, Kate	
	Determine if Breach Response Protocol is ready for comment by the broader Breach Response team	Snehit, Kate	

	Agenda Item	Speaker	Time
1.	Approve Agenda	Chair	
2.	Introductions	All	
3	Data Security Roadmap	Dixie	
4	Breach Response plan	Kate & Snehit	
5	New security staff	Paul	
	A.O.B.		

Minutes:

Dixie: went over roadmap and structure, Snehit focused on the Breach Response project:
https://docs.google.com/presentation/d/1f6GXX4wvcTUrOPojneBlw4MwTRjqUuepTMfk0YwQCPA/edit?usp=sharing
David Bernick: from the Broad Institute. Taking on several leadership roles in AAI in the life sciences community. Volunteering to help lead the AAI project. Have a lot of open source software and infrastructure in place to help. OpenID Connect is the standard that they use including authorization APIs that can be leveraged. Recognize the difficulty in Authentication.
Knox: Will help by talking about what has been done thus far. **[Action]** Work stream leadership will follow up with Dave and Knox.

Snehit: Trying to design a breach response protocol that can be followed by a wide range of projects by creating a protocol with a "light touch"
Dixie: Plan to work with REWS to come up with a protocol for sharing breach data among the driver projects. **[Action]** Follow up with Adrian to move this part of the project forward.
Adrian: REWS will look at the legal layer for breach notification, whether it falls under privacy laws etc. Also check and see if there are legal reporting obligations and see if they are similar or different across jurisdictions and how we can keep track of those different obligations when information is shared across borders.

Dixie: We want to have a system where developers can proactively report vulnerabilities that they discover in GA4GH standards.   This is not breach response, but breach avoidance.
Rishi: If something is picked up by security by needing attention, then there is a fast track process to allow the certified standard to be secured. Security issues found by developers can be reported to the people who are associated with it or a GitHub pull request or issue being raised.

Dixie: Discussed roadmap:
https://docs.google.com/document/d/16WIo4siUIF88z1cbjyEx2X3mty6XIRZ022MKL_xYig8/edit?usp=sharing
Snehit: **[Action]** Will follow up with Kate to determine if the Breach Response protocol is ready to be viewed and edited by the rest of the GA4GH Breach Response team.

Paul: We will be bringing on a part time, dedicated security person to help work with work streams to evaluate GA4GH standards in terms of security to bring a standard from proposal to sign off. Hopefully, we will grow to 2 full time staff members in this area. At this point, they can provide regular security consulting support to the work streams and driver projects, and work directly with the REWS to make sure that legal issues are in sync with security.

2017-09-28: Breach Response Initial Call

Chair: Paul Flicek

Global Alliance
for Genomics & Health

Attendees “Name (Affiliation)”:

	Actions Arising	Assigned To	Deadline

	Agenda Item	Speaker	Time
1.	Welcome	Paul	
	Description of “Breach Response”	Paul	
	Current Breach Response Protocols in use by Driver Projects	All	

Minutes:

Paul: Definition of “Breach Response:

- A letter was sent to understand the role of GA4GH in identifying potential breaches, communicating these and responding.
- The goal is to have a coherent response.
- The more successful GA4GH is in having its standards adopted, the more likely these could be targeted.

Current Driver Project Breach Response Protocols

- **Genomics England** (Grant Stapleton): Treat security breach notifications similarly to IT issues. GeL also has to deal with clinical safety issues because they work with NHS participants. Plan is to take a holistic view on how breaches are dealt with in each case.
  - **Identify** that a breach has occurred and is reported to a central service desk.
  - Then the incident is brought to an investigation and recovery team to **limit the impacts** of the breach using incident management technologies. Outside groups may be brought in to assist.
  - Start working on **notification** procedure. The notification must comply with UK laws. This includes notifying other parts of the government and NHS stakeholders.

  - Carry out **evaluation and root cause analysis**.
  - **Make changes** based on evaluation for future prevention.
- **GDC** (Ray Powell): Breaches are considered a subset of standard incident response plan.
  - **Detection** of the problem, which is then reported to Ray, who notifies the head of the Center.
  - **Analyze** the **impacts** and determine if law enforcement or lawyers need to be informed.
  - **Mitigation:** fix the problem.
  - **Notification**: stakeholders are contacted, either immediately for major issues or at a weekly update for minor issues. This would also be discussed at the monthly security meeting. Template letters exist that are filled in with relevant info and the required people are notified. Ray and the head of the Center decide who needs to be notified within the organization. The user is the National Cancer Institute, so they would be notified. The NCI would notify third parties.
- **EGA** (Dylan Spalding)**:** EGA distributes data on behalf of other data access committees and is run by EBI and CRG
  - **Monitor** for breaches, when one is **detected**, the other internal partner is **notified** via set procedures
  - Further internal **notification** is followed to keep management up to date.
  - **Analysis**: what caused the issue and what data sets were affected?
  - **Report:** using a standard template, the breach would be reported
- **ELIXIR** (Ilkka): Works within an organization that is connected to the universities and provides data discovery services.
  - Team that **monitors** the physical and network security. When a breach is **detected**, they identify the incident and **report** it to management.
  - Depending on the type of breach, **reporting** may include governmental agencies.
  - Currently working on a more detailed, ELIXIR specific procedure with Dylan Spalding
- **BRCA** (Christian Bollinger): Working with Gunnar. Security breaches are handled by network security group, if necessary, it is escalated to the network provider who work with the governmental cert (?). Data breaches are handled differently:
  - **Identify** what data has been stolen, how much.
  - Determine which stakeholders need to be **notified** and how.
  - There are some possible legal changes that need to be addressed regarding EU law. This is in development.
- Also **BRCA** (Zack Fischmann): In the past, the group has only had publicly available information, so breach response was not an issue. This is something that needs to be determined now and the process is being developed.
  - Ways to make breaches less likely
  - Ways to make breaches less damaging (partitioning data so patient data is separate from variant data, limiting amount of information stored)

- **CanDIG** (Richard): No breach policy for CanDIG because they are comprised by several institutes across Canada and the onus for breach response is on a per institute basis. The University Health Network has a policy in place based on Ontario law (these laws are all on a per province basis).
  - **Identification** of the level of data breached
  - Determine which incidence and security response **escalation procedures** need to be used
  - Coordination of these procedures is outside the scope unless other institutions are called in to help out
- **ClinGen** (Snehit Prabhu): Group of institutions across the US trying to standardize the ways in which genomics gets interpreted in clinical care. Dealing with many different domains, but the data sets currently used are all public, though they are starting to consider including case level data, which would need a breach response protocol. Current structure is mostly interfaces that lets users log into portals to collect data from various streams. The result of a breach would result in the reduction in quality of the data. The main security in place involves restricting non experts from usage of the system.
- **Summary** (Paul):
  - There is a lot of similarity, which is good
  - What is the comfort level of reporting breaches outside of one's own organization? This could be either anonymized or in a confidential forum. This is done in other industries to help with information sharing in best practices and issues.

    (Christian) There is a long standing tradition of community emergency response schemes. This would benefit the community and can help shape a model breach response
  - (Paul) One goal of this group is to set a general breach response plan that is broad enough to work with the variety of organizations involved, but would lay an effective framework for all groups. The procedure would be targeted to genomics and health data.
  - One major difference would be differences in the ways that the different types of data are linked to one another.
  - Plan is to use industry standards, not develop new structures.
  - This conversation will be continued at the Breach Response meeting in Orlando