# Clinical Quality Metrics Registry (CQMR) Subject Matter Expert Workgroup

August 8, 2018

Oregon Health Authority

# Agenda

- Welcome and agenda review
- Status update
- CQMR roles refresher
- OneHealthPort – account registrations and affiliations
- CQMR Policies and Procedures
- CQMR security overview
- Communications materials
- Wrap up and next steps

Oregon Health Authority

# CQMR Status Update

- CQMR System Test (initial run F/NF Test Scripts) started 7/25
- CQMR Security Testing – Security Scan occurred 8/3; results coming by 8/10

**Coming up:**

- Training materials in review process; next version of materials to OHA by 8/8
- Pre-prod environment available on 8/20
- Performance Testing targeted start on 8/21
- System Test Maintenance Release targeted 8/20

Oregon Health Authority

# Role Mapping: Reference Table

| OneHealthPort Role Name | Example user(s) | CQMR Permission Sets |
|---|---|---|
| Quality Report and Data Entry + OHP Administrator | • OHA Administrator<br>• CCO Master User | • **Submit/View** Individual Practitioner Aggregated Data, Individual Practitioner Patient Data, Practice/Clinic Aggregated Data, Practice/Clinic Patient Data, CCO Aggregated Data, CCO Patient Data and All Aggregated Data.<br>• Create Sub accounts and Submission Capability. |
| Quality Report and Data Entry | • Provider, Informaticist, Quality Manager at clinic | • **Submit/View** Individual Practitioner Aggregated Data, Individual Practitioner Patient Data, Practice/Clinic Aggregated Data, Practice/Clinic Patient Data, CCO Aggregated Data, CCO Patient Data and All Aggregated Data.<br>• Submission Capability. |
| Quality Manager | • Quality Manager at clinic | • **View** Individual Practitioner Aggregated Data, Individual Practitioner Patient Data |
| Quality Reports (View Only) | • Data Analyst at clinic | • **View** Individual Practitioner Aggregated Data, Practice/Clinic Aggregated Data, CCO Aggregated Data and All Aggregated Data. |

# Get your cell phones out!

**Instructions to join the poll:**

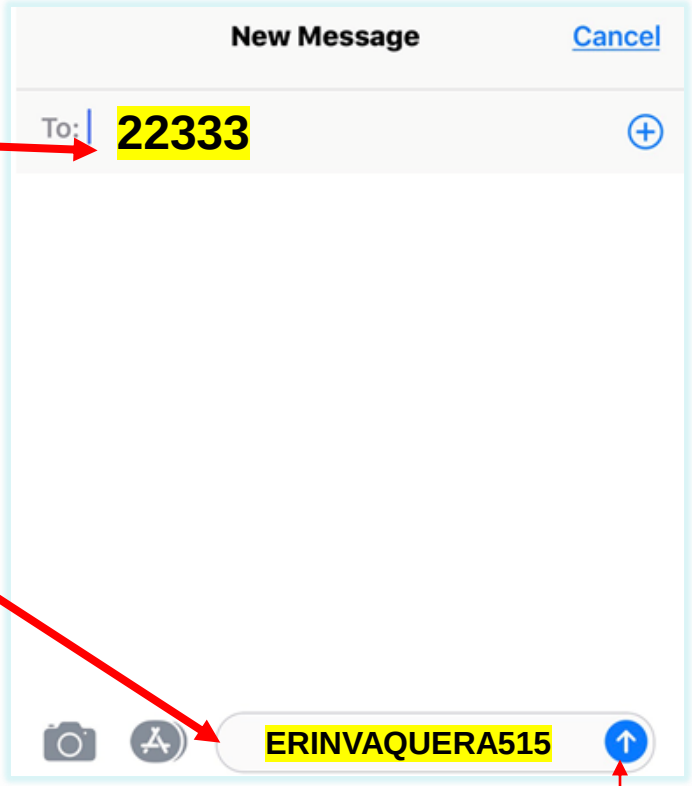
1. Type 22333 in the To: field

2. Type ERINVAQUERA515 in the message field

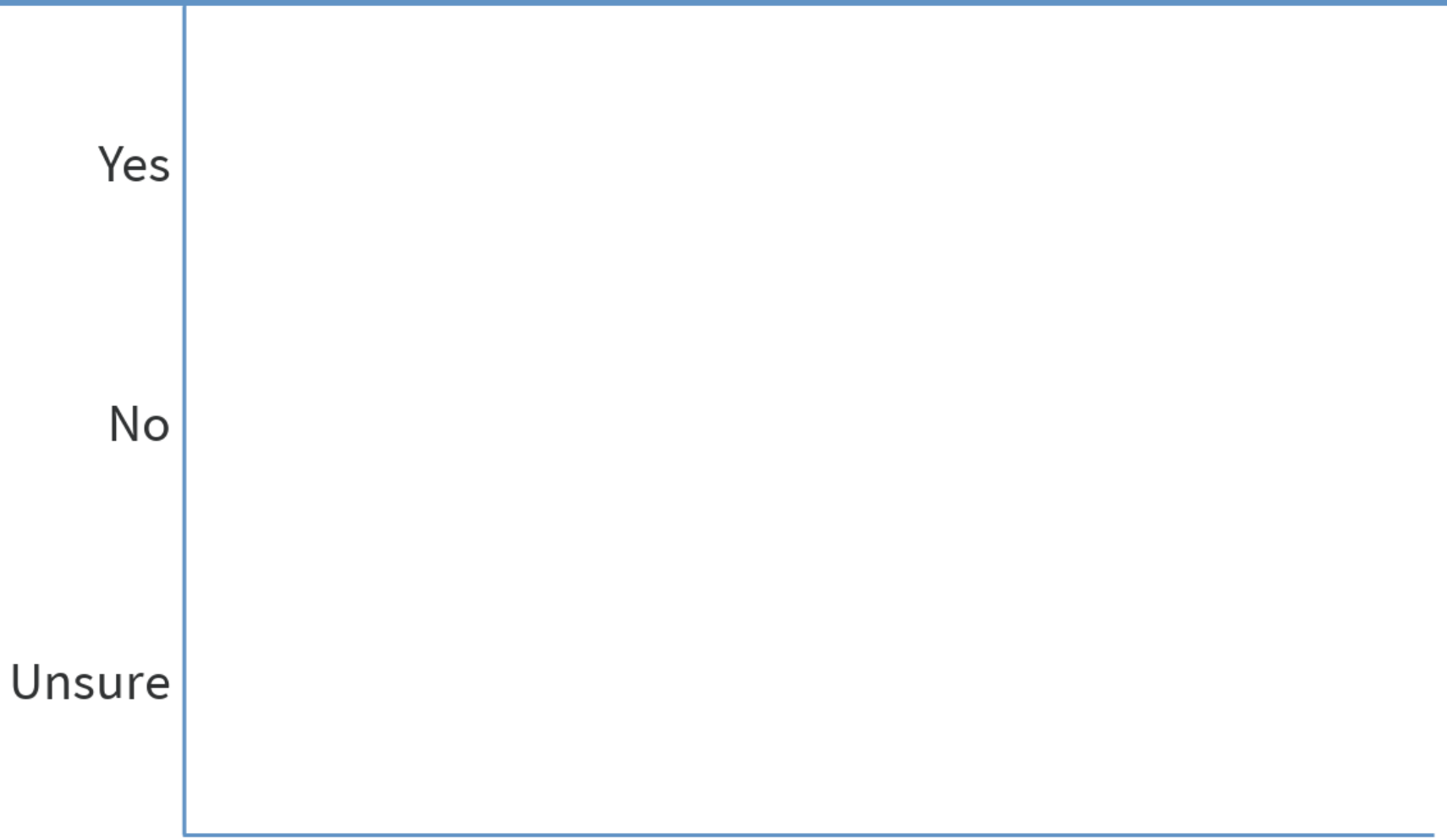
3. Click send

4. Wait for a response message to confirm you have joined the poll:

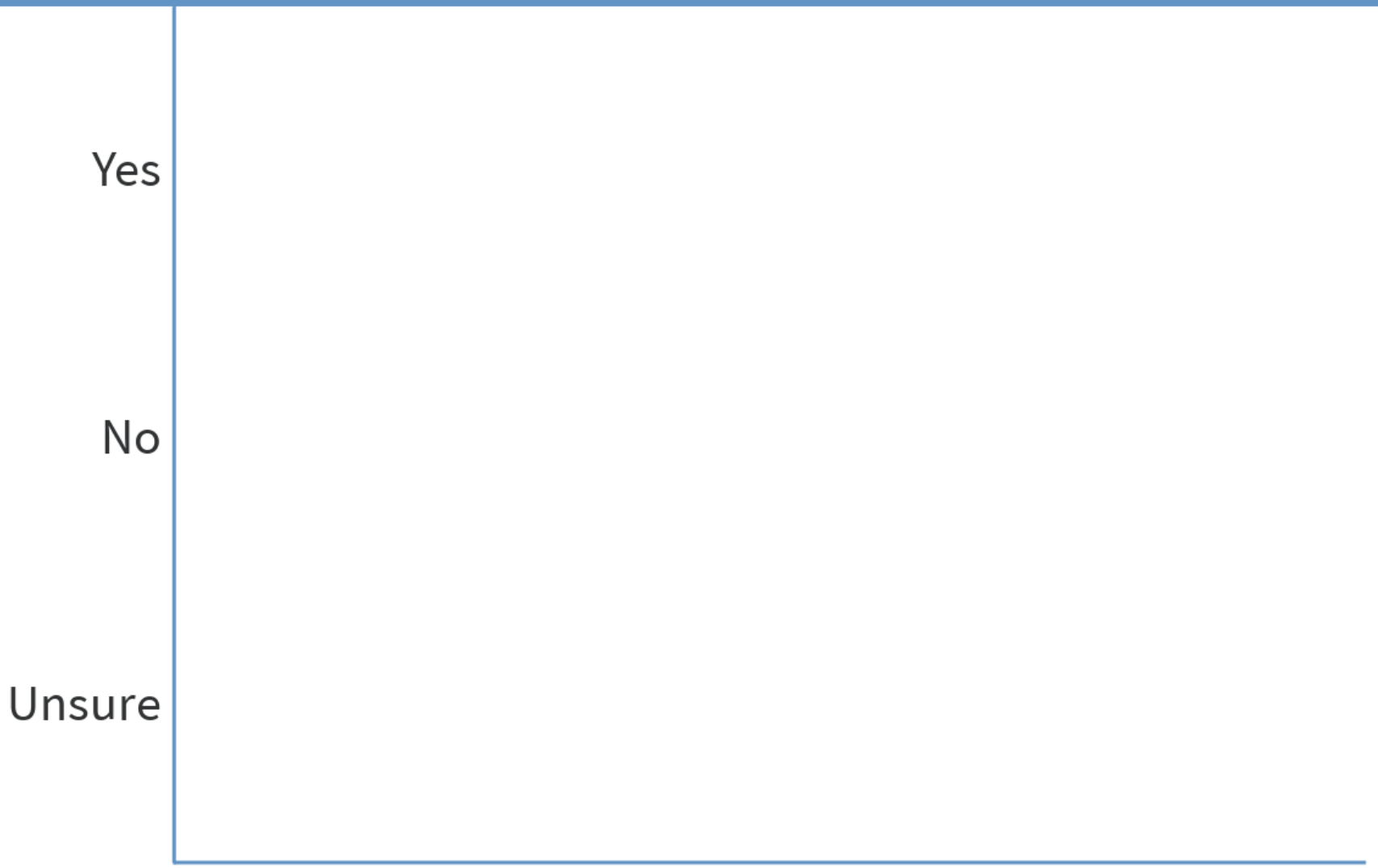
**You've joined Erin Vaquera's session (ERINVAQUERA515). When you're done, reply LEAVE**



# Does your managing organization currently use OneHealthPort (OHP)?



# Do you have a personal OneHealthPort (OHP) account?



# OneHealthPort Demo

Teresa Davis, OneHealthPort

# CQMR Policies and Procedures

Kate Lonborg, OHA

# CQMR Policies and Procedures

- Policies and Procedures will be part of a larger framework of legal agreements
  - Policies and Procedures will be harmonized with legal agreements – for example, consistent definition of terms
- All users (organizations and individual end users) will need to follow the Policies and Procedures

# Policies and Procedures Contents

- Definitions
- Permissible Uses
- Who Must Comply with the Policies and Procedures
- Process for Amending the Policies and Procedures
- Quality Reporting Programs
- Authentication
- Training
- Access
- Audit
- Adverse Security Events

# Permissible Uses

- Uses permitted under HIPAA and other applicable laws
- Operations of OHA quality reporting programs
- Reporting to other programs (e.g., to CMS for MIPS)
- Quality assessment and improvement activities, including combining clinical with other data sets
- Research as allowed under HIPAA, with request and review process
- Archiving for audit, trending and quality control
- Enrichment of data to standardize and enhance usability
- Extract of authorized user affiliations to Oregon Provider Directory

# Quality Reporting Programs

- Programs supported initially: CCO incentive, Medicaid EHR Incentive Program, CPC+, MIPS
- Support quality improvement efforts and decrease administrative burdens by
  - enabling reporting clinical quality measures data to the CQMR,
  - collecting supplemental data from health plans and potentially additional sources,
  - providing functionality to filter by fields such as payer and practice location,
  - offering the ability to send reports meet quality reporting obligations, for example, submitting data to the CMS Quality Payment Program (QPP) portal

# Quality Reporting Programs - Expansion

- Over time, additional programs may be supported in OHA's discretion
- OHA may consider factors such as
  - alignment of clinical quality measures and reporting parameters
  - availability of funding for development or operational costs
  - any approvals needed from CMS as a consequence of federal financial participation in the CQMR or other necessary approvals
  - consistency with the purposes of the CQMR
  - timing considerations for implementation

# Training

- OHA shall provide CQMR training materials
- Participating Entity shall ensure that its Authorized Users review training materials and CQMR Policies and Procedures
- Participating Entity shall ensure that its Authorized Users are trained on their obligations regarding privacy and security under HIPAA and other applicable laws

# Authentication

- OHA through its vendor OneHealthPort, is responsible for authorizing and authenticating a Participating Entity and its designated Administrator(s)
- OneHealthPort's Policies and Procedures are set forth in its Legal Notices and Terms, which can be found on its website: http://www.onehealthport.com/

# Access

- Each Participating Entity must enter into a Participation Agreement and shall be responsible for facilitating Authorized Users' access
- Participating Entity will identify its Administrator(s)
  - Responsible for granting access to all other Authorized Users
  - Point of contact for other Authorized Users for questions and reports of any potential unauthorized access
- Participating Entity shall maintain records of Authorized Users' access and training

# Access – Termination

- Participating Entity shall ensure that an Authorized User's access to the System is terminated
  - Termination of a Participating Entity's Participation Agreement with the OHA
  - Authorized User's failure to comply with the Authorized User Agreement
  - Termination of an Authorized User's employment or affiliation with the Participating Entity
- Participating Entity shall notify OHA immediately upon termination of an Authorized User's access to the System due to an Adverse Security Event

# Adverse Security Events

- "Adverse Security Event" means the unauthorized acquisition, access, disclosure, or use of unencrypted CQM Data by anyone who is not an Authorized User or by an Authorized User in any manner that is not permitted
- Processes in the event of an Adverse Security Event:
  - Notification
  - Investigation
  - Mitigation
- Nothing in Policies and Procedures supersedes any obligations under HIPAA or other laws

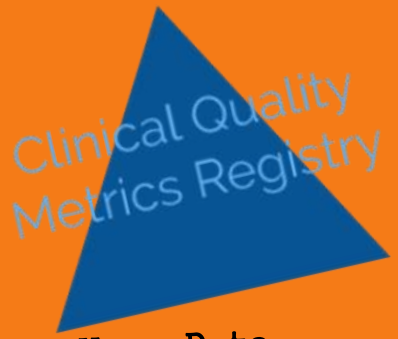
# Audit

- OHA may audit use of CQMR
  - Periodic audits for proper use of the CQMR and compliance with agreements and Policies and Procedures
  - Audits to be done at OHA's expense and designed to reasonably minimize interference with day-to-day operations
- Policies and Procedures do not alter or displace any program's audit standards, such as standards related to data quality and completeness

# Security Overview

Jason Miranda, OHA

Clinical Quality
Metrics Registry




## CQMR: Protecting Your Data

The Oregon Health Authority (OHA) and its vendors are committed to the privacy and security of the CQMR. OHA worked with internal privacy and security staff as well as with external stakeholders to develop program and operational requirements and guidelines that serve to safeguard all private information in the CQMR.

Collection of personally identifiable information (PII) and personal health information (PHI)

- Causes for Concern - Programs can create risks through development of poor user privacy provisions, exposure of data to unintended recipients, failure to properly classify.

- CQMR Risk/Mitigation - The CQMR is a closed system where access is provided only to authorized users who are vetted and verified. Before being granted access to the CQMR, authorized users must complete training and must review and agree to follow the CQMR Policies and Procedures. Users and their organizations are monitored for suspicious behavior and access to data follows the "least necessary access to perform business function" methodology recommended by industry professionals. Particularly sensitive data is restricted to only certain roles. Each organization must identify an administrator who is responsible for identifying the individuals within the organization who should have access and the role that each individual should have.


Bad Security Decisions

What not to do

How we do it right

Oregon Health Authority

Hackers/Malware penetrating and accessing customer data including names, addresses, health information, and other PII and PHI.

That's more like it!


- Causes for Concern - Hackers and Malware infection can take advantage of a solution's access to protected health information, financial data or other private data.

Nope

- CQMR Risk/Mitigation - OHA mandates that vendor staff is trained not to expose the platform to threats via phishing, instant messaging, or other external stimulus. Our CQMR vendor uses real-time intrusion and Malware prevention measures to monitor for 3rd parties attempting to infect the platform. OHA does not collect fees for this program. If fees were collected as part of an expanded use case in the future, OHA mandates that vendors do not retain payment information after the transaction has been processed and only the minimum information necessary to process the transaction is provided to the vendor as OHA policy.

Oregon Health Authority


Publicly Accessible Data

Boo!

Yay!

Unpatched vulnerabilities, administration tools access, and data encryption.

- Causes for Concern - With web-based solutions, unauthorized access to internal tools and interfaces with access to consumer data is a concern. Reports of web control and supporting application vulnerabilities for web applications surface frequently. Solutions may store data in unencrypted or partially unencrypted formats.

- CQMR Risk/Mitigation - Users cannot access any components of the CQMR over unauthenticated or public interfaces. Additionally, access to data is protected using industry standard access and security protocols and practices. Finally, CQMR data is always encrypted in motion and at rest, so even if someone were able to access the information illegally or attempt to access it during transfer, the data is protected via encryption.

Oregon Health Authority

## CQMR Security Approach In Review

- Access to the CQMR is available only through the latest HTTPS encrypted and TLS 1.2 compliant web browser interfaces
- Single Sign On Solution for users provides security and convenience as well as enforcement of Security Assertion Markup Language (SAML) tokens for authentication and Multi-Factor Authentication
- All organizations are reviewed and vetted prior to being granted access to the solution and are able to self-manage user populations
- All data for Oregon customers are segregated from other platform customers and are always encrypted in motion and at rest

- Vendor is compliant with all state identity and theft protection requirements, data retention policies, and federal and state privacy and security requirements and administrative rules
- All security related technology, training, and policies are verified by an independent 3rd party evaluator yearly and by OHA and or their designees per release and quarterly
- OWASP Top 10 Compliant App Scans are performed and assessed before each new release of the solution
- Strong Service Level Agreement (SLA) provisions are in place related to data protection, breach reaction, and resolutions to ensure compliance



Oregon Health Authority

# MiHIN and Salesforce Security and Compliance Certifications











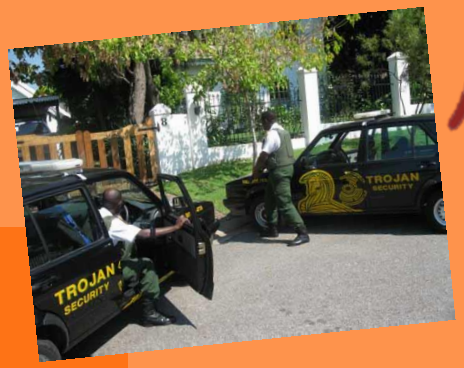
Oregon Health Authority

## How does OSPD respond in the unlikely scenario of a security event?

**Alert** - Vendor notifies OHA within one hour of discovery, and consult with the OHA regarding procedures for providing the required notice(s)

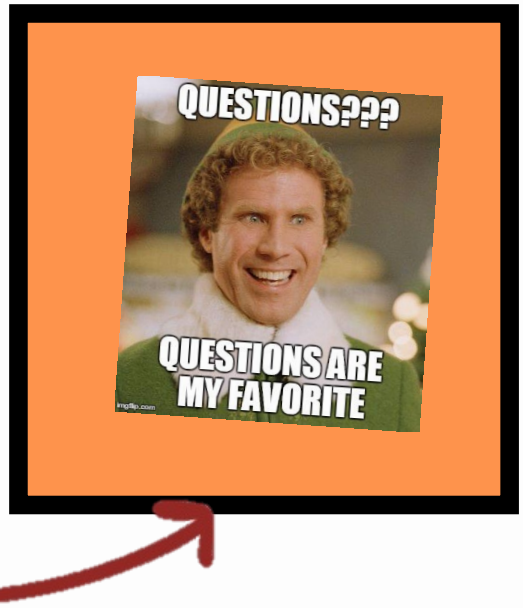

**Stop** - Vendor terminates or restricts the access of any users, user accounts, or user services and interfaces associated with the breach (within 24 hours)

**Notify** - OHA begins the established state process of analyzing the breach, determining and correcting the fault, and notifying those effected




Oregon Health Authority

Questions? Comments?
Applause?




Oregon Health Authority

# Communications

- Feedback on draft CCO toolkit?
  - Something you would use?
  - Ways to make it more useful?

# Next Steps

- Next meeting: September 12, 2018 10-noon
  - Focus on planning and preparation for User Acceptance Testing
- Feedback and suggestions for future meetings: katrina.m.lonborg@state.or.us

Oregon Health Authority