

Compliance Update

Corporate Integrity Agreement

Reporting Period 3

- Annual Report filed 9/30/2019
- No comments received to date

Reporting Period 4

- Training Modules are live and staff are in process of completing
- Developing proposal for training plan changes for RP5
- Claims Review facility list and selection will occur in spring 2020

Compliance: Work Plan YTD

FY2020 Work Plan

- 102 current efforts
 - 35 planned efforts
 - 67 additions
- 15 monitoring efforts (ongoing)

Improvement Items planned

- Refine compliance communication methods
- Adopt additional functionality from Healthicity

FY20 Work Plan Completion Percentage

64%

- Audits

56%

- Investigations

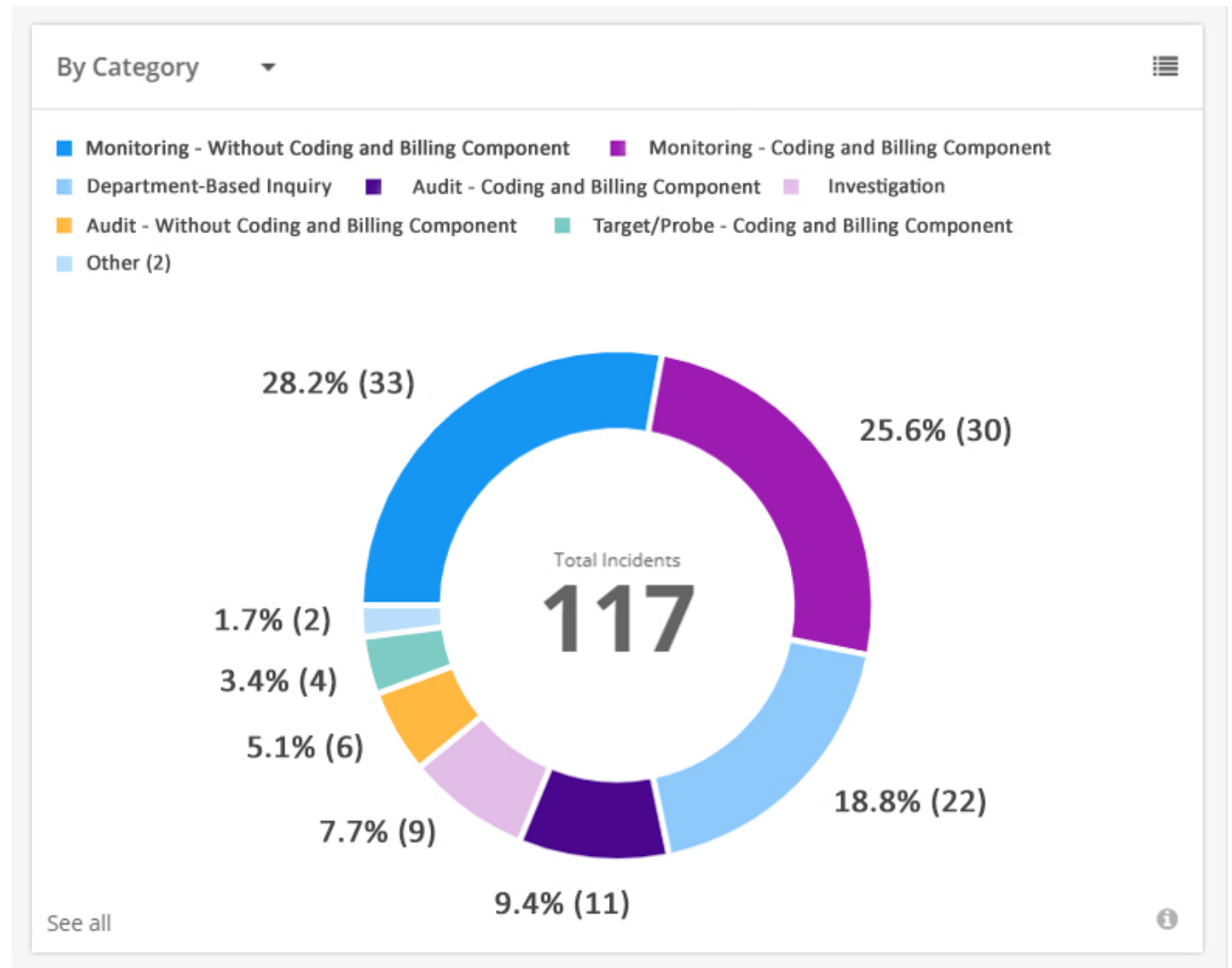
66%

- Probes/Targets

Compliance: Healthicity

Incident Management, Tracking and Reporting Software Tool

- Implemented Q2 FY20
- Includes privacy, information security and corporate compliance activities
 - Assign
 - Track
 - Collaborate
- Reporting Tools
 - Automated
 - Granular

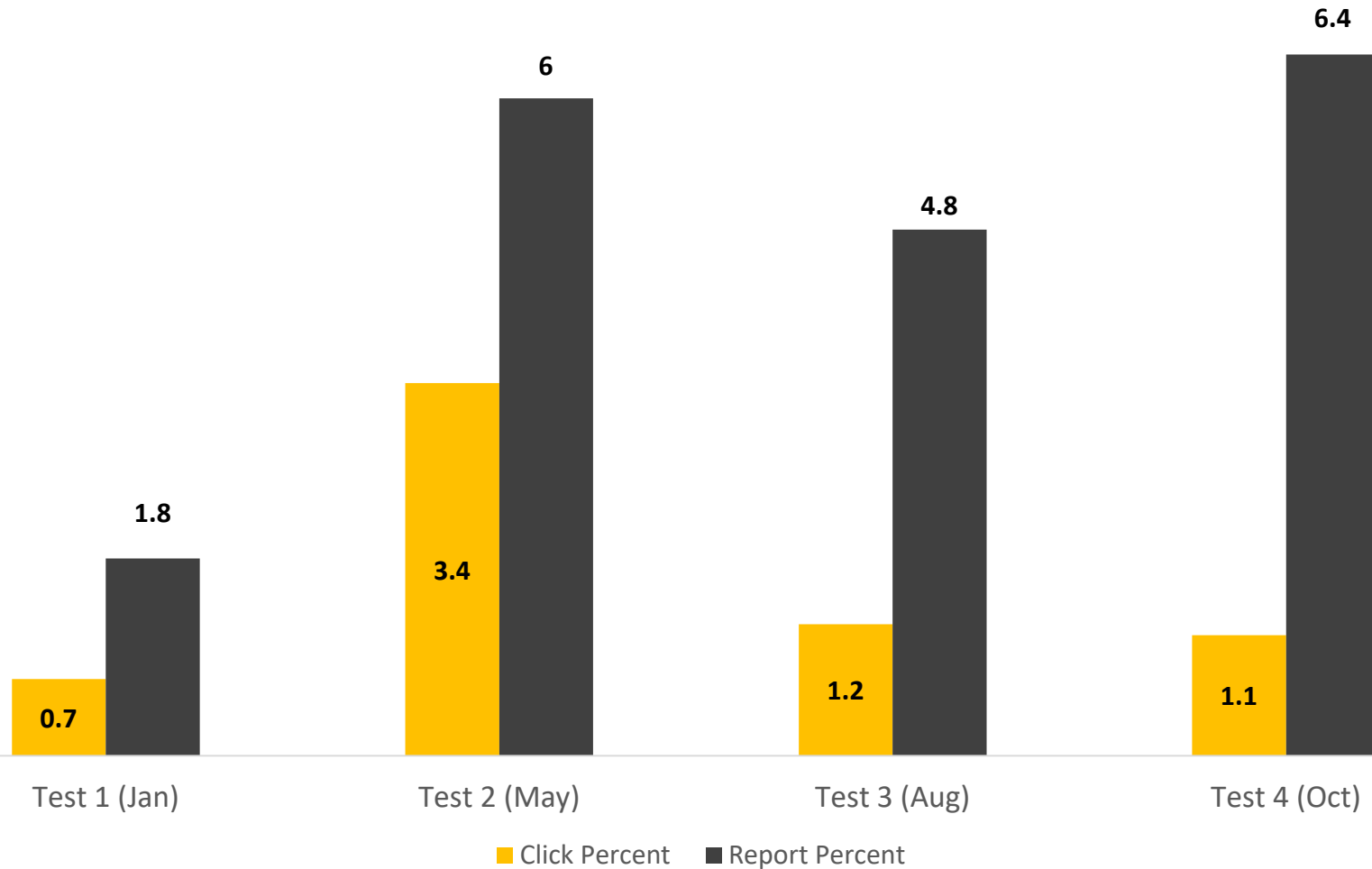


Information Security: Pen Testing

- Penetration, or “Pen”, Test
 - Simulated cyber attack against a computer system to check for exploitable vulnerabilities
- Tested MU Health’s network that communicates with the Internet between August and November 2019
- Preliminary findings:
 - Unable to gain access or place malicious code
 - Identified opportunities to improve security across all systems reviewed
 - 9 “critical” and 23 “high” areas to address identified
 - Examples were out-of-date software or missing security patches

Information Security: Phishing Tests

PHISHING TEST TRENDED FOR MU HEALTH



From the 2019 HIMSS Cybersecurity Survey:

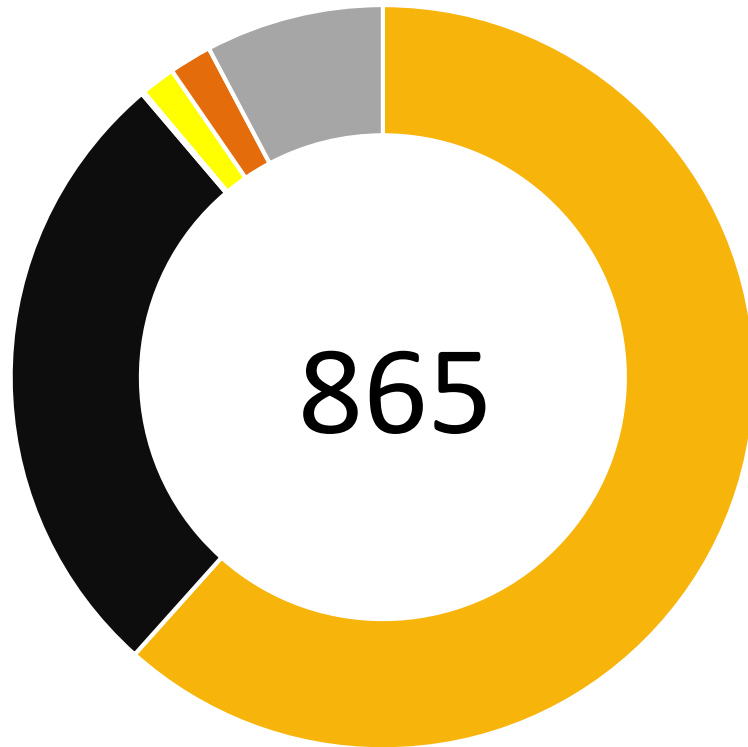
- 82% of survey respondents perform some level of phishing tests
- 40% of those have a click rate of 10% or lower
- Average click rate for health care phishing tests is 8%

Info Sec: Data Security Strategy

- **Multi-factor authentication**
 - Enabled on email web-portal; pending on email clients (Outlook)
- **Malware mitigation**
 - Removing administrative rights on end-user devices
 - Establishing approved software “app stores”
- **Data-loss prevention mechanisms**
 - Restricting USB drives on workstations
 - Options in Microsoft Office 365 and Azure
- **Email security**
- **Web-content filtering**

Privacy Program Update

Privacy/HIPAA Investigations and Findings



- Investigation, No Reportable Breach
- Reportable Breach, +500
- Subpoenas
- Reportable Breach, under 500
- AODs
- Walk throughs

Improvement Items Planned for CY20

- Revamp privacy education materials
- Create a central database in the EMR to track disclosures of PHI
- Expand monitoring functions through the addition of new audit reports

Organized Health Care Arrangement

Organized Health Care Arrangement, or “OHCA,” status provides expanded ability to share data among OHCA members for health care operations purposes, without the requirement that patients be in common.

- **Established with Lake Regional Health System in summer 2019**
 - Capital Region Medical Center reviewing documents now
- **Sharing of patient information in the common EMR platform**
- **Legal agreement with operational guidelines**
 - Common statement in Notices of Privacy Practices
 - OHCA members maintain their own HIPAA privacy and security policies and procedures, but harmonized through a review process

Organized Health Care Arrangement

HIPAA allows separate covered entities to designate themselves as an OHCA if they participate in one or more of the following activities:

- (i) provide a clinically integrated care setting in which individuals typically receive health care from more than one participant; and/or
- (ii) provide an organized system of health care in which the participants hold themselves out to the public as participating in a joint arrangement and participate in one or more of the following joint activities:
 - (a) utilization review;
 - (b) quality assessment and improvement activities; and/or
 - (c) payment activities.

- **Exception under the HIPAA Breach Notification Rule applies to inadvertent disclosures of PHI between OHCA partners**
- **Do not have joint and several liability for HIPAA violations**



Privacy Policy

MU Health Care OHCA Participants

MU Health Care currently participates in an organized health care arrangement (OHCA) with other health care providers in central Missouri. We do this to enhance the delivery of care and care coordination to improve patient experience as they are treated jointly by health care providers.

The OHCA participants share access to MU Health Care's electronic medical record and might, under certain circumstances, access your medical and billing information for treatment or health care operations purposes to improve, manage and coordinate your care without seeking your advance authorization, but only to the extent permitted by law.

The arrangement also enables participants to integrate patient portals into the MU Health Care portal, HEALTHConnect. The patient portal allows patients to securely message doctors, schedule appointments and access their health history across the shared electronic medical record system.

Current participants include:

- MU Health Care
- Lake Regional Health System

Organized Health Care Arrangement

Items planned for CY20

- Onboarding of Capital Region Medical Center
- Development of a Regional Governance Group
 - operations subcommittee to include:
 - health information management
 - compliance, privacy and information security
 - revenue cycle
 - quality
 - regulatory