Became Aware of Cyberattacks

- In laboratories within the state, including our own WSLH Proficiency Testing Division
- Started seeing more published articles

Some Times Square billboards went dark; ‘a handful’ remain offline

What is Crowdstrike?

Some US TV stations couldn’t air local news

About 1,500 US flights canceled by late morning, FlightAware says

A cancelled emergency heart surgery leaves a family scared and worried

Some U.S. states report 911 disruptions

July 19, 2024

Tech Outage Causes Worldwide Chaos and Disruptions to Airlines, Hospitals, Personal Computers

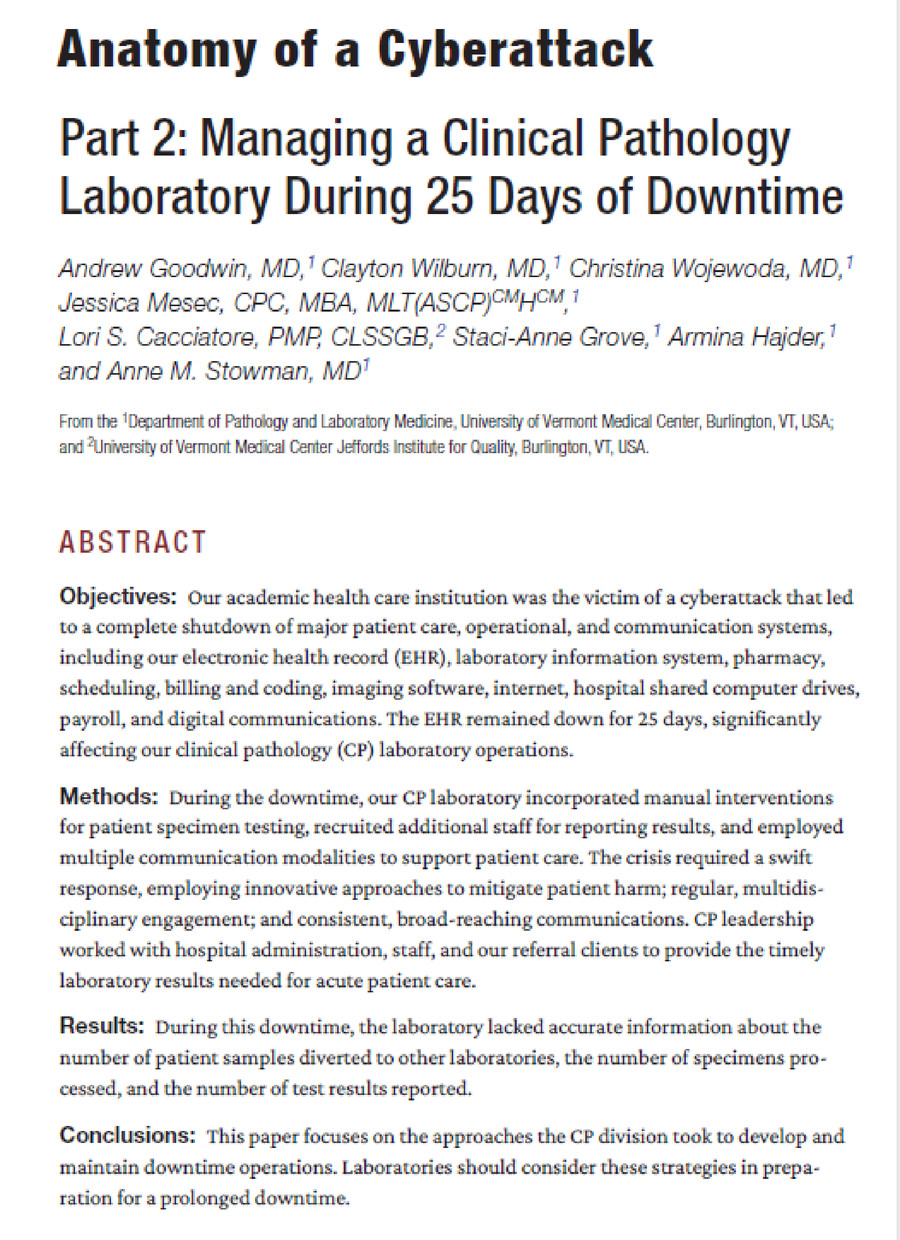
The New York Times

“The Downtime Menace” Cybersecurity Incident in the Clinical Pathology Laboratory

Lisa Buchinger

Renee Pelch

HSHS Laboratories



Anatomy of a Cyberattack

Part 2: Managing a Clinical Pathology Laboratory During 25 Days of Downtime

Andrew Goodwin, MD,[1] Clayton Wilburn, MD,[1] Christina Wojewoda, MD,[1] Jessica Mesec, CPC, MBA, MLT(ASCP)^{CM}H^{CM},[1] Lori S. Cacciatore, PMP, CLSSGB,[2] Staci-Anne Grove,[1] Armina Hajder,[1] and Anne M. Stowman, MD[1]

From the [1]Department of Pathology and Laboratory Medicine, University of Vermont Medical Center, Burlington, VT, USA; and [2]University of Vermont Medical Center Jeffords Institute for Quality, Burlington, VT, USA.

ABSTRACT

Objectives: Our academic health care institution was the victim of a cyberattack that led to a complete shutdown of major patient care, operational, and communication systems, including our electronic health record (EHR), laboratory information system, pharmacy, scheduling, billing and coding, imaging software, internet, hospital shared computer drives, payroll, and digital communications. The EHR remained down for 25 days, significantly affecting our clinical pathology (CP) laboratory operations.

Methods: During the downtime, our CP laboratory incorporated manual interventions for patient specimen testing, recruited additional staff for reporting results, and employed multiple communication modalities to support patient care. The crisis required a swift response, employing innovative approaches to mitigate patient harm; regular, multidisciplinary engagement; and consistent, broad-reaching communications. CP leadership worked with hospital administration, staff, and our referral clients to provide the timely laboratory results needed for acute patient care.

Results: During this downtime, the laboratory lacked accurate information about the number of patient samples diverted to other laboratories, the number of specimens processed, and the number of test results reported.

Conclusions: This paper focuses on the approaches the CP division took to develop and maintain downtime operations. Laboratories should consider these strategies in preparation for a prolonged downtime.

Am J Clin Pathol 157:653-663; 2022

CYBERATTACKS IN HEALTHCARE

- Large southern California healthcare network in May 2021

- Global co$t exceeding $20 billion

- Literature has discussed:

  Impact on entire healthcare organizations
  Recommendations to improve cybersecurity
  Development of risk inventory (Erin's risk assessment)

  Medical oncology, radiation oncology, perioperative

Am J Clin Pathol 157:653-663; 2022

UNIVERSITY of VERMONT MED CTR

- Regional referral center for Vermont and northern New York (~1 million residents)
- Six partner hospitals; 17 regional laboratories
- 1.2 million annual patient care encounters
- 3.2 million test results reported annually

Am J Clin Pathol 157:653-663; 2022

OCTOBER 2020; → 25-day downtime

- Electronic health record
- Laboratory information system
- Other health information & administrative systems

  Internet access
  Paging
  Pharmacy
  Radiology
  Supply Chain Ordering

  Hospital shared drives
  Billing/coding
  Digital communications
  (many phones, FAX)

- Attack cost $40-50 million (mostly in lost revenue)

Am J Clin Pathol 157:653-663; 2022

IN A NUTSHELL…

Pre-analytic	significantly affected
Analytic	relatively limited impact
Post-analytic	significantly affected

Am J Clin Pathol 157:653-663; 2022

Pre-analytic Nuts and Bolts

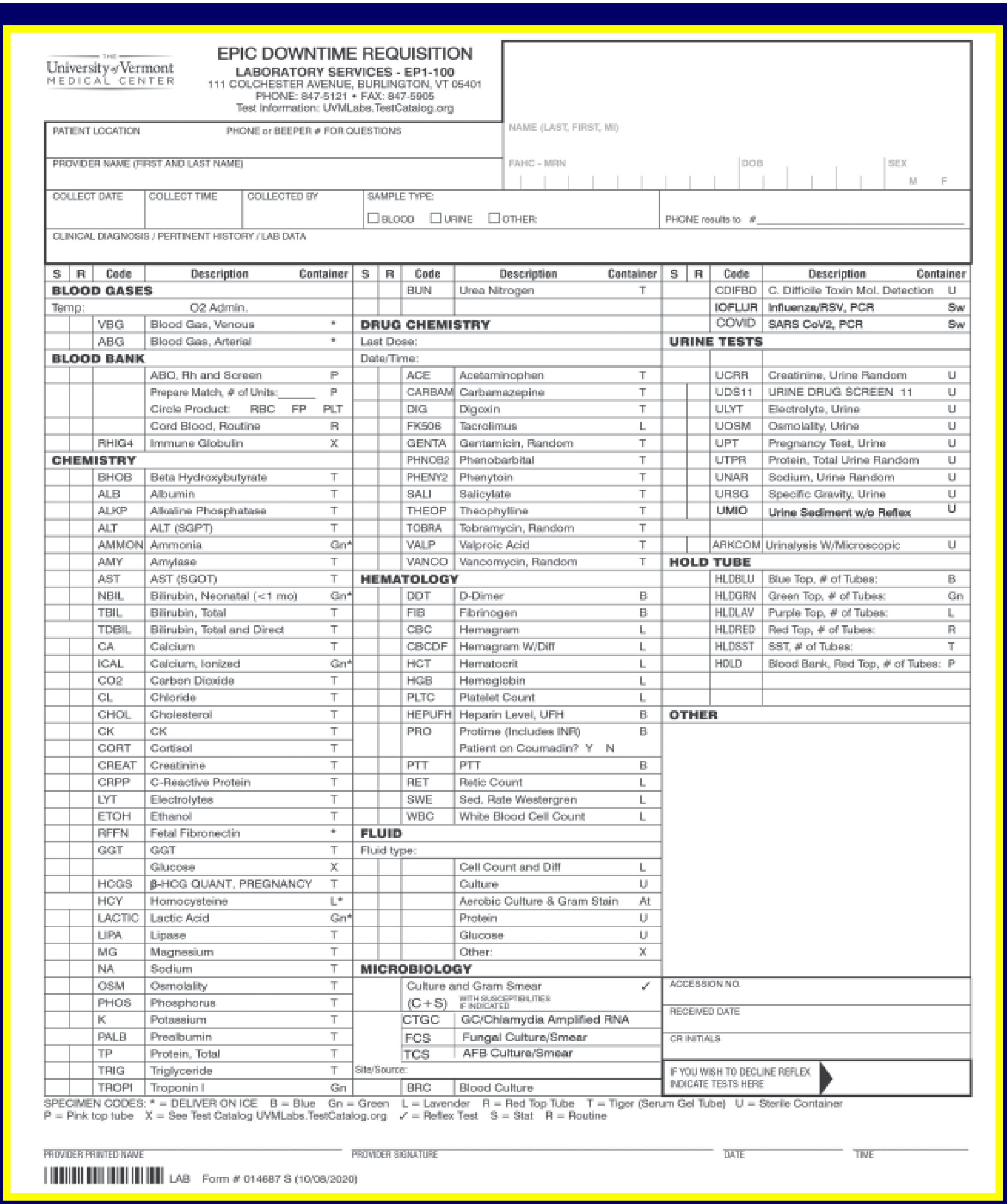
ORDERING, LABELING

- Providers unable to place electronic orders
  Laboratory unable to view new, existing orders
  Outpatient clients "new to the game"

- Laboratory tried to get providers to use pre-printed barcode labels; eventually ran out

- "Wild West" with respect to downtime requisitions

Am J Clin Pathol 157:653-663; 2022



THE University of Vermont MEDICAL CENTER

EPIC DOWNTIME REQUISITION

LABORATORY SERVICES - EP1-100
111 COLCHESTER AVENUE, BURLINGTON, VT 05401
PHONE: 847-5121 • FAX: 847-5905
Test Information: UVMLabs.TestCatalog.org

NAME (LAST, FIRST, MI)

FAHC - MRN

DOB

SEX M F

PATIENT LOCATION

PHONE or BEEPER # FOR QUESTIONS

PROVIDER NAME (FIRST AND LAST NAME)

COLLECT DATE

COLLECT TIME

COLLECTED BY

SAMPLE TYPE: □ BLOOD □ URINE □ OTHER:

PHONE results to #____________________

CLINICAL DIAGNOSIS / PERTINENT HISTORY / LAB DATA

S	R	Code	Description	Container
BLOOD GASES				
Temp:			O2 Admin.	
		VBG	Blood Gas, Venous	*
		ABG	Blood Gas, Arterial	*
BLOOD BANK				
			ABO, Rh and Screen	P
			Prepare Match, # of Units:______	P
			Circle Product: RBC FP	PLT
			Cord Blood, Routine	R
		RHIG4	Immune Globulin	X
CHEMISTRY				
		BHOB	Beta Hydroxybutyrate	T
		ALB	Albumin	T
		ALKP	Alkaline Phosphatase	T
		ALT	ALT (SGPT)	T
		AMMON	Ammonia	Gn*
		AMY	Amylase	T
		AST	AST (SGOT)	T
		NBIL	Bilirubin, Neonatal (<1 mo)	Gn*
		TBIL	Bilirubin, Total	T
		TDBIL	Bilirubin, Total and Direct	T
		CA	Calcium	T
		ICAL	Calcium, Ionized	Gn*
		CO2	Carbon Dioxide	T
		CL	Chloride	T
		CHOL	Cholesterol	T
		CK	CK	T
		CORT	Cortisol	T
		CREAT	Creatinine	T
		CRPP	C-Reactive Protein	T
		LYT	Electrolytes	T
		ETOH	Ethanol	T
		RFFN	Fetal Fibronectin	*
		GGT	GGT	T
			Glucose	X
		HCGS	β-HCG QUANT, PREGNANCY	T
		HCY	Homocysteine	L*
		LACTIC	Lactic Acid	Gn*
		LIPA	Lipase	T
		MG	Magnesium	T
		NA	Sodium	T
		OSM	Osmolality	T
		PHOS	Phosphorus	T
		K	Potassium	T
		PALB	Prealbumin	T
		TP	Protein, Total	T
		TRIG	Triglyceride	T
		TROPI	Troponin I	Gn

S	R	Code	Description	Container
		BUN	Urea Nitrogen	T
DRUG CHEMISTRY				
Last Dose:				
Date/Time:				
		ACE	Acetaminophen	T
		CARBAM	Carbamazepine	T
		DIG	Digoxin	T
		FK506	Tacrolimus	L
		GENTA	Gentamicin, Random	T
		PHNOB2	Phenobarbital	T
		PHENY2	Phenytoin	T
		SALI	Salicylate	T
		THEOP	Theophylline	T
		TOBRA	Tobramycin, Random	T
		VALP	Valproic Acid	T
		VANCO	Vancomycin, Random	T
HEMATOLOGY				
		DDT	D-Dimer	B
		FIB	Fibrinogen	B
		CBC	Hemagram	L
		CBCDF	Hemagram W/Diff	L
		HCT	Hematocrit	L
		HGB	Hemoglobin	L
		PLTC	Platelet Count	L
		HEPUFH	Heparin Level, UFH	B
		PRO	Protime (Includes INR) Patient on Coumadin? Y N	B
		PTT	PTT	B
		RET	Retic Count	L
		SWE	Sed. Rate Westergren	L
		WBC	White Blood Cell Count	L
FLUID				
Fluid type:				
			Cell Count and Diff	L
			Culture	U
			Aerobic Culture & Gram Stain	At
			Protein	U
			Glucose	U
			Other:	X
MICROBIOLOGY				
		Culture and Gram Smear (C+S)	WITH SUSCEPTIBILITIES IF INDICATED	✓
		CTGC	GC/Chlamydia Amplified RNA	
		FCS	Fungal Culture/Smear	
		TCS	AFB Culture/Smear	
Site/Source:				
		BRC	Blood Culture	

S	R	Code	Description	Container
		CDIFBD	C. Difficile Toxin Mol. Detection	U
		IOFLUR	Influenza/RSV, PCR	Sw
		COVID	SARS CoV2, PCR	Sw
URINE TESTS				
		UCRR	Creatinine, Urine Random	U
		UDS11	URINE DRUG SCREEN 11	U
		ULYT	Electrolyte, Urine	U
		UOSM	Osmolality, Urine	U
		UPT	Pregnancy Test, Urine	U
		UTPR	Protein, Total Urine Random	U
		UNAR	Sodium, Urine Random	U
		URSG	Specific Gravity, Urine	U
		UMIO	Urine Sediment w/o Reflex	U
		ARKCOM	Urinalysis W/Microscopic	U
HOLD TUBE				
		HLDBLU	Blue Top, # of Tubes:	B
		HLDGRN	Green Top, # of Tubes:	Gn
		HLDLAV	Purple Top, # of Tubes:	L
		HLDRED	Red Top, # of Tubes:	R
		HLDSST	SST, # of Tubes:	T
		HOLD	Blood Bank, Red Top, # of Tubes:	P
OTHER				

ACCESSION NO.

RECEIVED DATE

CR INITIALS

IF YOU WISH TO DECLINE REFLEX INDICATE TESTS HERE ▶

SPECIMEN CODES: * = DELIVER ON ICE B = Blue Gn = Green L = Lavender R = Red Top Tube T = Tiger (Serum Gel Tube) U = Sterile Container
P = Pink top tube X = See Test Catalog UVMLabs.TestCatalog.org ✓ = Reflex Test S = Stat R = Routine

PROVIDER PRINTED NAME PROVIDER SIGNATURE DATE TIME

LAB Form # 014687 S (10/08/2020)

No collect date/time

No unique patient identifiers

No patient location

Illegible penmanship

Delivery of results (where)?

Providers had to call

Am J Clin Pathol 157:653-663; 2022

SPECIMEN TRANSPORT/ACCESSION

- Networked server drives pneumatic tube system
- Couriers unable to enter facility
- Accessioning at instrument level by technologists
  - Standardization
  - What do you do with all of the paperwork?

Am J Clin Pathol 157:653-663; 2022

FOR THOSE WHO HAVE AUTOMATION

- Extreme level of manual effort to deliver correct specimen type to correct area

  Additional local servers were shut down to prevent the spread of malware through system

- Aliquot, centrifugation process no longer available on automation line

- QC ranges and rules no longer available

Am J Clin Pathol 157:653-663; 2022

VOLUME, VOLUME, VOLUME

“Volume of incoming specimens far exceeded the laboratory’s ability to perform testing because of reduced efficiency with manual workflows”

Am J Clin Pathol 157:653-663; 2022

WHAT DID THEY DO?

- Ordering, labeling

  Bouncers 24/7 (within first 24h)

- Specimen transport/accession

  Runners for inpatient 24/7
  Staff an identified entry point for couriers
  Standardized process for entry into analyzer
  (what information and how it would be entered)

Am J Clin Pathol 157:653-663; 2022

WHAT DID THEY DO?

- Automation
  - Each discipline came up with own plan
  - Adequate staffing to manually process specimens
  - Program QC into analyzers (rather than LIS)
- Volume, volume, volume
  - Encourage testing for urgent needs only
  - Limit outpatient phlebotomy locations
  - Communicate laboratory status and current TAT
  - Referral locations divert specimens to reference labs

Am J Clin Pathol 157:653-663; 2022

AFTERMATH

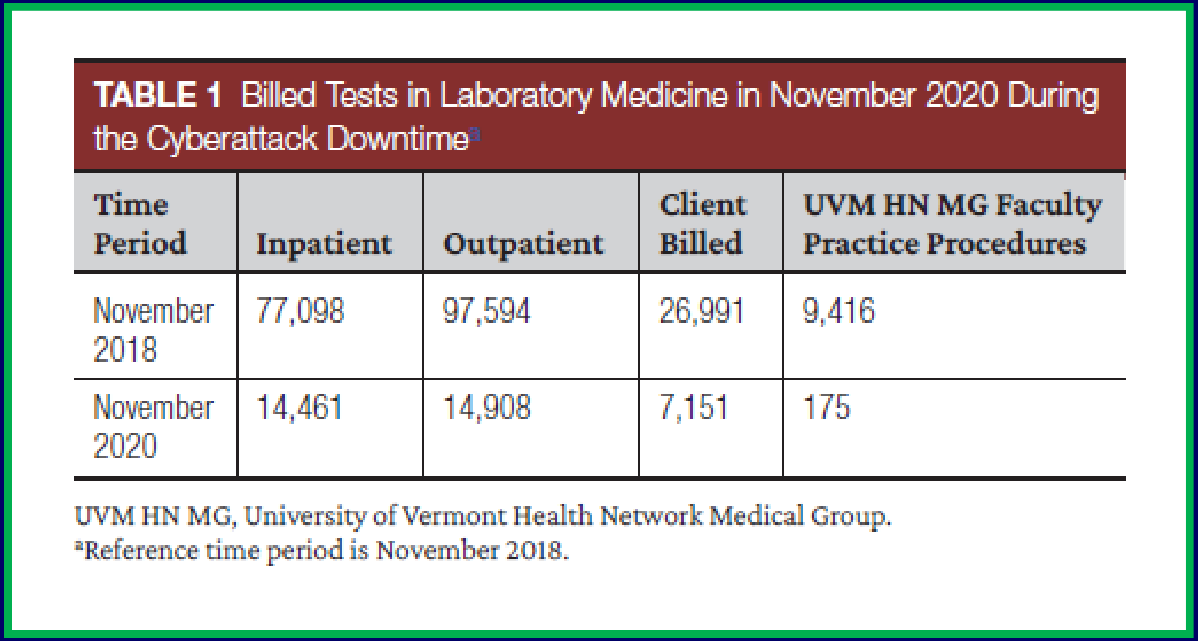


TABLE 1 Billed Tests in Laboratory Medicine in November 2020 During the Cyberattack Downtime[a]

Time Period	Inpatient	Outpatient	Client Billed	UVM HN MG Faculty Practice Procedures
November 2018	77,098	97,594	26,991	9,416
November 2020	14,461	14,908	7,151	175

UVM HN MG, University of Vermont Health Network Medical Group.
[a] Reference time period is November 2018.

Unable to capture data on total tests performed (too manual)

Am J Clin Pathol 157:653-663; 2022

Analytic Nuts and Bolts

- Instrumentation was fully functional
- Instruments had dedicated hardware (independent)

- Could not interface with LIS
- Temperature monitoring built into automation
- Lost remote troubleshooting with vendors

Am J Clin Pathol 157:653-663; 2022

Post-analytic Nuts and Bolts

REPORT GENERATION

- LIS gone; IT had to hook up printers to analyzers

  Patient demographics not showing up on reports
  Analyte names on instrument reports were not familiar to providers

  "Anti-Xa" rather than "Unfractionated heparin"

- Reports lacked critical information to help providers

  Reference ranges absent
  Comments or always text not present
  Disclaimers (laboratory-developed testing) gone

Am J Clin Pathol 157:653-663; 2022

PROGRAMMED ALGORITHMS

- No automatic flagging of critical values
- Chemistry calculations not available

  Estimated glomerular filtration rate
  Low-density lipoprotein
  Transferrin saturation

- Automatic add-ons not available (automated storage/inventory not available)
- Reflex testing (UA, syphilis serology, hepatitis C)

Am J Clin Pathol 157:653-663; 2022

CLIENT SERVICES

- First 48 hrs, FAXed results to inpatient locations, FAXed to outpatient provider office
- Access to 2 FAX machines, huge increase in phone call volume; no critical value notification
- Many recipient FAX machines on hospital servers
- Also responsible for filing hard copies

Initially, did so by date of laboratory service

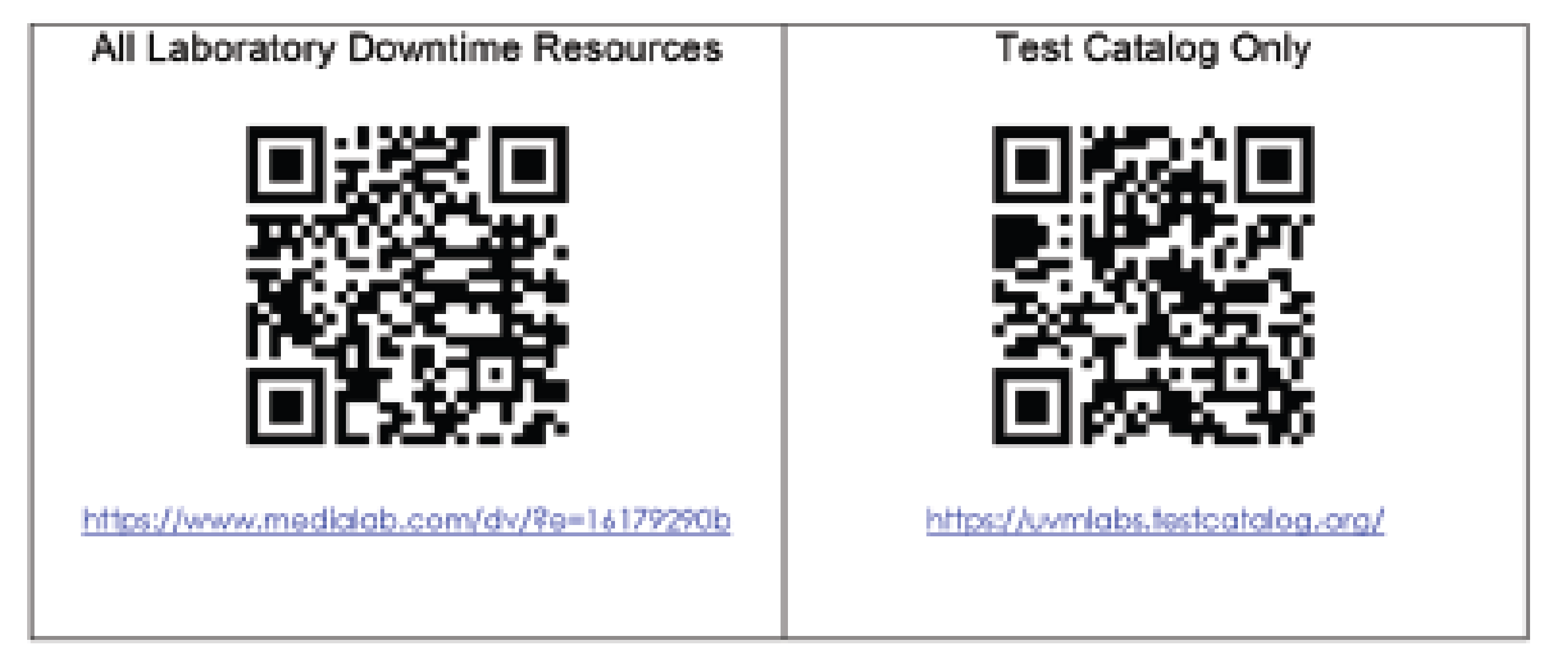
Provider requests often involved date of collection (per their records) that was not translated onto downtime requisition

Am J Clin Pathol 157:653-663; 2022

WHAT DID THEY DO?

- Report generation

  Pretty much at liberty of analyzer



All Laboratory Downtime Resources	Test Catalog Only
https://www.medialab.com/dv/?e=16179290b	https://uvmlabs.testcatalog.org/

Am J Clin Pathol 157:653-663; 2022

WHAT DID THEY DO?

- Programmed algorithms
  - Techs handled critical values
    - Cheat sheets
    - Lack of accurate provider contact information
  - Could not provide calculated values
    - Likely a function of instrument printout/report format
  - Could not provide add-on testing
    - Specimen storage/tracking functionality gone
  - Elected not to provide (some) reflex testing (↓ volume)

Am J Clin Pathol 157:653-663; 2022

WHAT DID CLIENT SERVICES DO?

- Dedicated results center (after 96 hours)

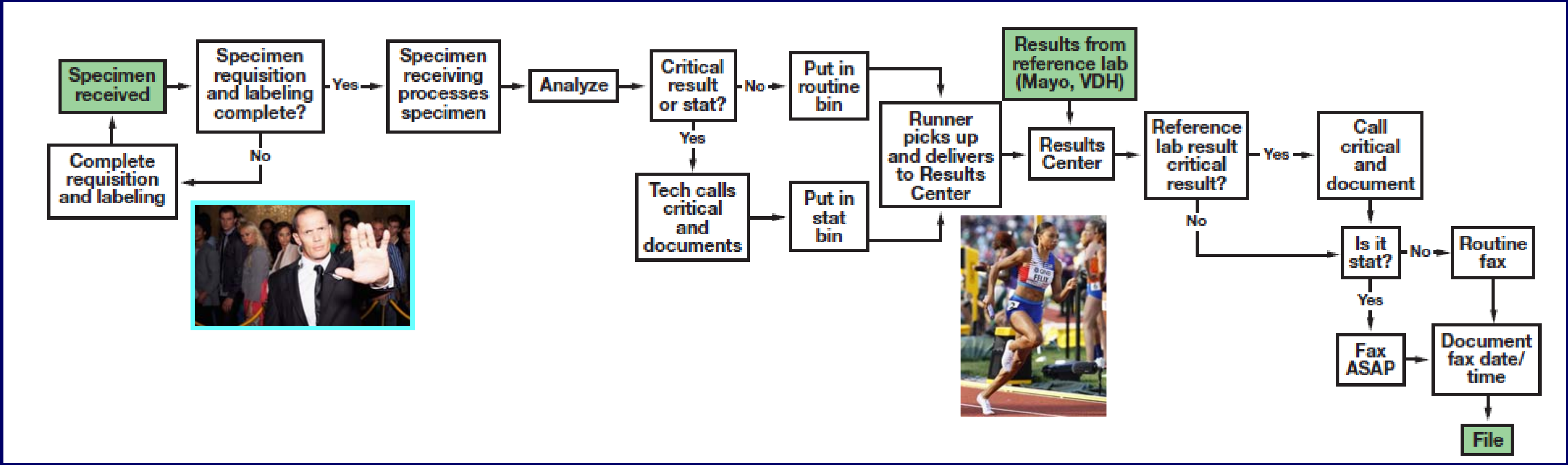
  Deployed in a laboratory conference room
  (5 analog FAX machines, 4 analog phones)
  This became an inpatient-only center by day 7
  Offsite (2nd center) deployed for outpatient results

- Finding patient reports took too much time

  Began filing by alphabetical order (last name)
  Stratified by inpatient (runner) versus outpatient
  Consulting providers were still calling

Am J Clin Pathol 157:653-663; 2022

SUMMARY/RESULTS DISSEMINATION



Specimen received

Specimen requisition and labeling complete?

Yes

Specimen receiving processes specimen

Analyze

Critical result or stat?

No

Put in routine bin

No

Complete requisition and labeling

Yes

Tech calls critical and documents

Put in stat bin

Runner picks up and delivers to Results Center

Results from reference lab (Mayo, VDH)

Results Center

Reference lab result critical result?

Yes

Call critical and document

No

Is it stat?

No

Routine fax

Yes

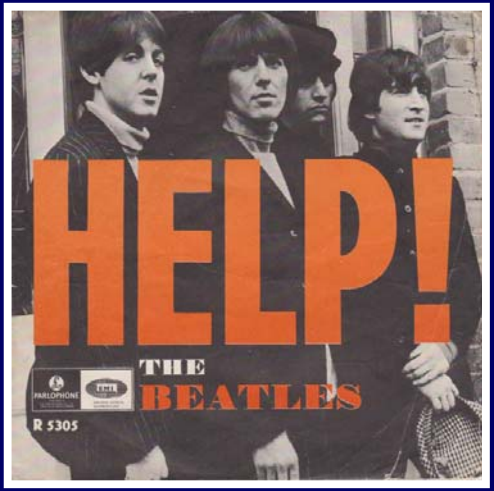
Fax ASAP

Document fax date/ time

File

Am J Clin Pathol 157:653-663; 2022

HELP



- Staffing requirements said to have doubled (including residents, fellows)
- Were able to bring in “volunteers”

  Furloughed or displaced and retired workers
  Learning curve/training

- Third-party scheduling system was software-based
- When manual processing systems adequately established, provided at least 1 day off per week

Am J Clin Pathol 157:653-663; 2022

Their 35,000-foot Summary

TAKE HOMES I

- Control incoming test requests/volume
- Standardize data entry process (analyzers)
- Plan for loss of automated specimen processing
- Analyzers reliable; connectivity is the issue
- Have up-to-date, easy paper requisition process
- Get a bouncer and result runners

Am J Clin Pathol 157:653-663; 2022

TAKE HOMES II

- Program reference ranges/critical values in instruments when possible
- Have enough people/techs to go manual
- Don’t forget about proficiency testing due dates
- Re-set turnaround time expectations
- Access to office supplies, space, copy machines
- Maintain instrument QC; conduct periodic QA, and second checks

Am J Clin Pathol 157:653-663; 2022

TAKE HOMES III

- Encourage organization to have access to hotspots
- Access to whiteboard for communication to team
- Keep up with back up data from EMR
- Manual log to track Blood Product unit activity
- Standard downtime result form for Microbiology
- Standard downtime result form for manual result testing

Am J Clin Pathol 157:653-663; 2022

TAKE HOMES IV

- File results by patient name/patient chart
- Be prepared for new processes daily
- Access to a computer not on the network to create patient labels.
- Prioritize patient registrations for recovery
- Be involved in the recovery plan

Am J Clin Pathol 157:653-663; 2022

IF YOU WANT TO LEARN MORE…

- Managing an anatomic pathology laboratory during 25 days of downtime
- Managing a clinical pathology laboratory during 25 days of downtime
- Coordination in crisis, development of an incident command team, and resident education during downtime
- Quality assurance and error reduction, billing and compliance, transition to uptime